(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 552 707**

(21) Número de solicitud: 201590098

(51) Int. Cl.:

H04L 29/08 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

07.03.2013

(43) Fecha de publicación de la solicitud:

01.12.2015

(88) Fecha de publicación diferida del informe sobre el estado de la técnica:
15.04.2016

Fecha de la concesión:

15.03.2017

(45) Fecha de publicación de la concesión:

23.03.2017

(73) Titular/es:

TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (50.0%)
164 83 Estocolmo SE y
UNIVERSIDAD CARLOS III DE MADRID (50.0%)

(72) Inventor/es:

JIMÉNEZ, Jaime;
CAMARILLO GONZALEZ, Gonzalo y
URUEÑA PASCUAL, Manuel

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

(54) Título: **Método y dispositivo para control de acceso de escritura a un recurso en una red RELOAD**

(57) Resumen:

Método y dispositivo para control de acceso de escritura a un recurso de una red de localización y descubrimiento de recursos, RELOAD por uno o más nodos de acceso configurados para: en un nodo que posee el recurso, obtener una clave pública de un par responsable del recurso, cifrar una clave de escritura usando la clave pública obtenida y enviar la clave de escritura cifrada al par responsable del recurso; en el par responsable del recurso, descifrar la clave de escritura; en un nodo de acceso, firmar datos a ser escritos en el recurso usando la clave de escritura y enviar una petición al par responsable del recurso para escribir los datos firmados en el recurso; y en el par responsable del recurso, controlar el acceso de escritura al recurso en base a la clave de escritura descifrada y los datos firmados.

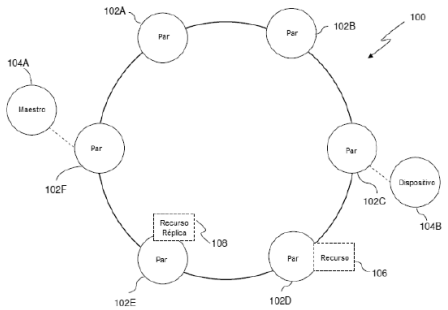

Figura 1

ES 2 552 707 B1

Aviso:Se puede realizar consulta prevista por el art. 37.3.8 LP.

DESCRIPCIÓN

Método y dispositivo para control de acceso de escritura a un recurso en una red RELOAD.

Campo técnico

La invención se refiere a métodos y un aparato para escribir datos en un recurso en una red Base de Localización Y Descubrimiento de Recursos (RELOAD). Más específicamente, la invención se refiere a métodos y un aparato para escribir datos en un recurso en una red RELOAD por un nodo distinto del propietario del recurso.

Antecedentes

El Grupo de Trabajo del Protocolo de Inicio de Sesiones (SIP) Entre Pares (P2P) (P2PSIP WG) del Grupo de Tareas de Ingeniería de Internet (IETF) está especificando el protocolo base RELOAD para construir sistemas distribuidos en base a tecnologías entre pares (P2P). En particular, una gran proporción del trabajo emprendido por el grupo de trabajo se centra en Tablas de Comprobación Aleatoria Distribuidas (DHT). Una DHT proporciona un servicio de almacenamiento distribuido, donde los recursos se almacenan en un par que, junto con otros pares, forma una red superpuesta.

Un recurso se almacena en base a un ID de Recurso, que es comúnmente un nombre de usuario de comprobación aleatoria de un nodo que posee el recurso. Un ID de Tipo especifica el tipo de datos que se pueden almacenar en un recurso.

En RELOAD, los recursos se pueden leer (por ejemplo, usando una Petición Fetch) por cualquier nodo que conoce el ID de Recurso del recurso. No obstante, por seguridad y a fin de limitar el volumen de información que un nodo puede almacenar en la red, RELOAD define un número de Políticas de Control de Acceso para controlar qué entidades pueden crear un recurso y escribir datos en un recurso.

Las políticas de control de acceso estándar definidas en RELOAD se basan en el ID de Usuario (por ejemplo, USER-MATCH) o el ID de Nodo (por ejemplo, NODE-MATCH). El ID de Usuario y el ID de Nodo de un nodo se incluyen en el certificado del nodo. Normalmente, se asigna al nodo uno o más ID de Nodo por una autoridad central de inscripción, aunque se podrían usar otros planteamientos, tales como un modelo de tipo Web de Confianza. Tanto el ID de Usuario como el ID de Nodo se colocan en un certificado de nodo, junto con la clave pública del nodo.

Con las políticas de control de acceso de RELOAD, normalmente un recurso solamente se puede crear, escribir o reescribir por un único nodo, llamado el "propietario" del recurso,

típicamente el nodo que creó el recurso.

Una política de control de acceso que permite a múltiples nodos escribir en el mismo recurso es la USER-NODE-MATCH, que permite a cualquier nodo escribir una única entrada a un recurso de Diccionario, el ID de Recurso del cual debe corresponder con el ID de Nodo. USER-NODE-MATCH solamente se puede usar con recursos de Diccionario.

En RELOAD-ACL, se define una nueva política de control de acceso, llamada USER-CHAIN-ACL, la cual permite al propietario del recurso compartir permisos de escritura con otros nodos. Esto se hace asociando una Lista de Control de Acceso (ACL) a un recurso compartido y enumerando explícitamente todos los usuarios y/o nodos que tienen permiso de escritura para el recurso.

Las dos políticas mencionadas anteriormente tienen algunos inconvenientes. USER-NODE-MATCH solamente se puede aplicar a recursos de Diccionario y permite a cualquier nodo de la red RELOAD con un certificado válido escribir una entrada en cualquier recurso de Diccionario. Por lo tanto, a fin de proteger sus propios recursos, los pares limitarán comúnmente el tamaño de tales recursos de Diccionario. Esto permite la posibilidad de ataques de Denegación de Servicio (DoS), en la medida que un nodo atacante con uno o más certificados válidos es capaz de almacenar un gran volumen de datos en un recurso de Diccionario, excediendo por ello su límite de tamaño. Esto impide a los usuarios legítimos almacenar datos. En USER-CHAIN-ACL, solamente usuarios autorizados explícitamente por el propietario del recurso (a través de la ACL) son capaces de escribir datos. No obstante esto requiere al nodo propietario conocer de antemano la lista de usuarios legítimos. Además, un recurso no se puede compartir por un número arbitrario de usuarios, debido a la carga colocada en el par responsable del recurso en la gestión de la ACL, así como todos los certificados asociados. Por lo tanto, el tamaño de la ACL se limitará por los pares que almacenan en ella, en particular, en la medida que el recurso de ACL se comparte por todos los recursos de USER-CHAIN-ACL dentro del mismo espacio de direcciones.

Compendio

A fin al menos de mitigar los problemas identificados anteriormente, se proporciona en la presente memoria métodos y un aparato para permitir a un nodo que no es el propietario original de un recurso escribir en un recurso.

Según un aspecto de la invención, se proporciona un dispositivo de red configurado como un par responsable de un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD. El dispositivo de red comprende un comunicador configurado para

recibir un mensaje que se origina desde un nodo propietario del recurso. El mensaje comprende una clave de escritura cifrada que usa una clave pública del dispositivo de red. El comunicador se configura además para recibir una petición para almacenar datos en el recurso. La petición que se origina desde uno o más nodos de acceso y que comprende datos firmados usando la clave de escritura, el uno o más nodos de acceso que es diferente al nodo propietario del recurso. El dispositivo de red comprende un descifrador configurado para descifrar la clave de escritura cifrada usando la clave privada del dispositivo de red. El dispositivo de red también comprende un controlador de acceso configurado para controlar el acceso de escritura al recurso por el uno o más nodos de acceso en base a la clave de escritura y los datos firmados recibidos.

Opcionalmente, el controlador de acceso se configura para escribir los datos recibidos en el recurso si los datos recibidos se han firmado usando la clave de escritura.

Opcionalmente, el mensaje que se origina desde el nodo que posee el recurso además comprende un algoritmo de firma a ser usado por el uno o más nodos de acceso cuando se firman los datos. El controlador de acceso se puede configurar además para escribir los datos recibidos en el recurso si los datos recibidos se han firmado usando el algoritmo de firma y la clave de escritura.

Opcionalmente, el dispositivo de red comprende además un replicador configurado para replicar el recurso en un par adicional de la red RELOAD enviando un mensaje de Petición de Almacenamiento al par adicional. El replicador se puede configurar para cifrar la clave de escritura con la clave pública obtenida del par adicional y enviar la clave de escritura cifrada al par adicional en el mensaje de Petición de Almacenamiento.

Según un aspecto de la invención, se proporciona un dispositivo de red configurado como un nodo que posee un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD. El dispositivo de red comprende un comunicador configurado para comunicar con uno o más nodos dentro de la red RELOAD para obtener una clave pública de un par responsable del recurso. El dispositivo de red comprende también un cifrador configurado para cifrar una clave de escritura usando la clave pública obtenida. El comunicador se configura además para enviar la clave de escritura cifrada al par responsable del recurso para controlar el acceso de escritura al recurso.

Opcionalmente, el comunicador se configura además para enviar un algoritmo de firma al par responsable del recurso que identifica el algoritmo de firma que se debería usar por uno o más nodos de acceso que soliciten acceso de escritura al recurso.

Opcionalmente, el comunicador se configura para enviar la clave de escritura cifrada y/o el algoritmo de firma en un mensaje de Petición de Almacenamiento que define una estructura StoreKindData.

Opcionalmente, el dispositivo de red está incrustado dentro de un sistema informático y comprende además un procesador de instrucciones configurado para recibir instrucciones desde uno o más nodos de acceso, a través del recurso.

Opcionalmente, el procesador de instrucciones se configura para sondear el recurso en diferentes momentos para recuperar instrucciones.

Opcionalmente, el dispositivo de red se configura además para cambiar la clave de escritura antes de se dé la vuelta a un contador de generación, el contador de generación que se asocia con valores almacenados en el recurso.

Según un aspecto de la invención, se proporciona un vehículo que comprende un dispositivo de red configurado como un nodo que posee un recurso, como se describió anteriormente.

Según un aspecto de la invención, se proporciona un dispositivo de red configurado como un nodo de acceso para escribir datos en un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD. El recurso se posee por un nodo diferente. El dispositivo de red comprende un firmante configurado para firmar datos a ser escritos en el recurso usando una clave de escritura. El dispositivo de red también comprende un comunicador configurado para generar una petición para escribir los datos firmados en el recurso no poseído por el dispositivo de red y enviar la petición a un par responsable del recurso.

Opcionalmente, el firmante se configura para firmar los datos usando la clave de escritura y un algoritmo de firma predeterminado.

Opcionalmente, el comunicador se configura para generar y enviar una Petición de Almacenamiento.

Opcionalmente, la Petición de Almacenamiento comprende un ID de Recurso del recurso.

Según un aspecto de la invención, se proporciona un método de control de un dispositivo de red configurado como un par responsable de un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD. El método comprende, en el dispositivo de red, recibir un mensaje que se origina desde un nodo que posee el recurso. El mensaje comprende una clave de escritura cifrada usando una clave pública del dispositivo de red. El método comprende además, en el dispositivo de red, recibir una petición para almacenar

datos en el recurso. La petición que se origina desde uno o más nodos de acceso y que comprende datos firmados usando la clave de escritura, el uno o más nodos de acceso que son diferentes al nodo que posee el recurso. El método comprende además, en el dispositivo de red, descifrar la clave de escritura cifrada usando la clave privada del dispositivo de red. El método comprende además, en el dispositivo de red, controlar el acceso de escritura al recurso por el uno o más nodos con el acceso en base a la clave de escritura y los datos recibidos.

Según un aspecto de la invención, se proporciona un método de control de un dispositivo de red configurado como un nodo que posee un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD. El método comprende, en el dispositivo de red, comunicar con uno o más nodos dentro de la red RELOAD para obtener una clave pública de un par responsable del recurso. El método comprende además, en el dispositivo de red, cifrar una clave de escritura usando la clave pública obtenida. El método comprende además, en el dispositivo de red, enviar la clave de escritura cifrada al par responsable del recurso para controlar el acceso de escritura al recurso.

Según un aspecto de la invención, se proporciona un método de control de un dispositivo de red configurado como un nodo de acceso para escribir datos a un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD, en donde el recurso se posee por un nodo diferente. El método comprende, en el dispositivo de red, firmar datos a ser escritos en el recurso usando una clave de escritura. El método comprende además, en el dispositivo de red, generar una petición para escribir los datos firmados en el recurso no poseído por el dispositivo de red. El método comprende además, en el dispositivo de red, enviar la petición a un par responsable del recurso.

Según un aspecto de la invención, se proporciona un sistema para controlar el acceso de escritura por uno o más nodos de acceso a un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD. El sistema comprende un nodo que posee el recurso y configurado para obtener una clave pública de un par responsable del recurso, para cifrar una clave de escritura usando la clave pública obtenida y para enviar la clave de escritura cifrada al par responsable del recurso. El par responsable del recurso se configura para descifrar la clave de escritura cifrada. El sistema comprende además un nodo de acceso configurado para firmar datos a ser escritos en el recurso usando la clave de escritura y para enviar una petición al par responsable del recurso para escribir los datos firmados en el recurso. El par responsable del recurso se configura además para controlar el acceso de escritura al recurso en base a la clave de escritura descifrada y los datos

firmados.

Según un aspecto de la invención, se proporciona un método de control de acceso de escritura por uno o más nodos de acceso a un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD. El método comprende, en un nodo que posee el recurso, obtener una clave pública de un par responsable del recurso, cifrar una clave de escritura usando la clave pública obtenida y enviar la clave de escritura cifrada al par responsable del recurso. El método comprende además, en el par responsable del recurso, descifrar la clave de escritura. El método comprende además, en un nodo de acceso, firmar datos a ser escritos en el recurso usando la clave de escritura y enviar una petición al par responsable del recurso para escribir los datos firmados en el recurso. El método comprende además, en el par responsable del recurso, controlar el acceso de escritura al recurso en base a la clave de escritura descifrada y los datos firmados.

Según un aspecto de la invención, se proporciona un medio legible por ordenador no transitorio que comprende código legible por ordenador configurado para llevar a cabo cualquiera de los métodos descritos anteriormente.

Breve descripción de los dibujos

La Figura 1 es una representación esquemática de una red RELOAD;

La Figura 2 es un diagrama de flujo de señalización que muestra un método de control de acceso a un recurso en una red RELOAD;

La Figura 3 es un diagrama de flujo de señalización que muestra un método de control de acceso a un recurso en una red RELOAD y que replica el recurso en un par de réplica;

La Figura 4 es una representación esquemática de un par responsable;

La Figura 5 es una representación esquemática de un nodo propietario;

La Figura 6 es una representación esquemática de un nodo de acceso;

La Figura 7 es una representación esquemática de un vehículo que comprende un nodo propietario;

La Figura 8 es un diagrama de flujo para un método de control de un dispositivo de red configurado como un par responsable de un recurso dentro de una red RELOAD;

La Figura 9 es un diagrama de flujo para un método de control de un dispositivo de red configurado como un nodo que posee un recurso dentro de una red RELOAD;

La Figura 10 es un diagrama de flujo para un método de control de un dispositivo de red configurado como un nodo de acceso para escribir datos en un recurso dentro de una red RELOAD; y

La Figura 11 es un diagrama de flujo para un método de control de acceso de escritura por uno o más nodos de acceso a un recurso dentro de una red RELOAD.

Descripción detallada

Los inventores han apreciado que todas las políticas de control de acceso RELOAD requieren la verificación de la identidad de un nodo que desea realizar una operación de almacenar. Es decir, se requiere obtener y validar un certificado de nodo, entonces comprobar las firmas de los valores a ser almacenados. Estas comprobaciones implican operaciones de criptografía de clave pública asimétrica, que generalmente son más complejas que las operaciones de criptografía simétrica.

Con referencia a la Figura 1, una red RELOAD 100 comprende una pluralidad de pares 102A-F que juntos forman una red superpuesta. Uno o más clientes 104A-B, que no forman parte de la red superpuesta, están en comunicación eléctrica con al menos un par 102. Cada par es responsable de uno o más recursos 106 guardados en el par. En la red RELOAD ejemplar 100 de la Figura 1, uno de los clientes 104 se muestra como un maestro 104A y otro se muestra como un dispositivo 104B. En los métodos y el aparato ejemplares, el maestro 104A puede almacenar instrucciones para el dispositivo 104B en el recurso 106, como se trata en más detalle más adelante. Se señala que el término "nodo" como se usa en la presente memoria abarca tanto los pares 102 como los clientes 104.

Cada recurso 106 tiene un "Tipo", como se define en el protocolo base RELOAD. Una política de control de acceso asociada al Tipo de recurso define qué usuarios y/o qué nodos son capaces de crear el recurso. Es decir, la política de control de acceso define qué usuarios y/o qué nodos son capaces de realizar la primera operación de Almacenar. Una vez que se crea un recurso 106, el nodo que lo creó se denomina el nodo "propietario". El recurso 106 se almacena a un par 102D de la red superpuesta en base a un ID de Recurso. El ID de Recurso se determina normalmente mediante comprobación aleatoria del ID de Usuario o el ID de Nodo del nodo propietario y define una dirección única para el recurso 106. Cada par 102 dentro de la red superpuesta es responsable de un intervalo de direcciones y el ID de Recurso especifica un par 102D en el que se almacena el recurso 106. Este par se denomina el "par responsable" y es el par responsable del recurso 106, en particular, para controlar qué nodos pueden almacenar datos en el recurso 106.

Como se trató anteriormente, generalmente, en una red RELOAD 100, solamente se permite al nodo 104B que posee un recurso 106 almacenar datos en el recurso 106. RELOAD usa, por ejemplo, políticas USER-MATCH y NODE-MATCH para limitar el acceso de escritura de un recurso 106 al propietario 104B. Una petición para almacenar datos en un recurso 106 (Petición de Almacenamiento) se envía desde un nodo 104B que posee el recurso 106 a un par 102C de la red superpuesta. La petición se transmite sobre la red superpuesta según sea necesario y alcanza el par 102D responsable del recurso 106. La Petición de Almacenamiento incluye el certificado del nodo propietario y los datos a ser almacenados. Los datos a ser almacenados se firman con la clave privada del nodo propietario. El certificado incluye la clave pública del nodo propietario, que permite al par 102D verificar que el nodo que envía la Petición de Almacenamiento es el nodo propietario 104B. El certificado incluye también el ID de USUARIO e ID de Nodo del nodo propietario, que permite al par responsable 102D comprobar que el ID de Recurso del recurso 106 corresponde a un ID de Usuario o ID de Nodo comprobado aleatoriamente. Bajo la USER-MATCH, si el nombre comprueba aleatoriamente el ID de Recurso, los datos se almacenan en el recurso 106. Bajo la política NODE-MATCH el ID de Nodo comprueba aleatoriamente el ID de Recurso, los datos se almacenan en el recurso 106. Como resultado, en USER-MATCH y NODE-MATCH, solamente el propietario 104B puede escribir en el recurso 106.

Generalmente, los métodos y el aparato descritos en la presente memoria permiten a nodos 104A que no poseen un recurso 106 almacenar datos en ese recurso 106. En los métodos y el aparato ejemplares, esto se hace asociando una clave de escritura secreta al recurso 106. Generalmente, el nodo propietario 104B obtiene la clave pública del par responsable 102D y cifra la clave de escritura con la clave pública del par. El nodo propietario 104B envía la clave de escritura cifrada al par 102D en una Petición de Almacenamiento. La Petición de Almacenamiento también puede incluir un algoritmo MAC que se debería usar por otros nodos de acceso 104A que desean almacenar datos en el recurso 106.

Los inconvenientes de USER-NODE-MATCH y USER-CHAIN-ACL se pueden demostrar con el siguiente ejemplo. Un dispositivo embebido puede emplear una tabla de comprobación aleatoria distribuida (DHT) RELOAD como un mecanismo para recibir comandos de uno o más maestros, dado que puede estar detrás de un cortafuegos/NAT o reposando la mayoría del tiempo. Una forma de recibir tales instrucciones es para el dispositivo para crear un recurso en la red RELOAD. El(los) maestro(s) puede(n) almacenar instrucciones en el recurso y el dispositivo puede sondear periódicamente el recurso para comprobar si se han almacenado cualesquiera instrucciones de los maestros. Si se han almacenado instrucciones, estas se pueden recuperar y emprender por el dispositivo. El(los)

maestro(s) solamente necesita(n) conocer el ID de Usuario o ID de Nodo del dispositivo a fin de determinar el ID de Recurso del recurso y almacenar instrucciones en él (ya que el recurso tiene un ID de Recurso = comprobación aleatoria (ID de Usuario) o comprobación aleatoria (ID de Nodo)). Los inventores han apreciado que, usar las políticas actuales en el protocolo base RELOAD tiene ciertos inconvenientes.

Si el recurso es un recurso de Diccionario con una política de control de acceso USER-NODE-MATCH, cada maestro solamente es capaz de almacenar un comando a la vez. Además, un nodo atacante con uno o más certificados válidos puede realizar fácilmente un ataque de DoS contra los dispositivos desbordando el recurso compartido, ya que el par responsable del recurso no conoce qué nodos son maestros válidos.

Si el recurso utiliza una política de control de acceso USER-CHAIN-ACL, el dispositivo debe conocer de antemano los ID de Usuario y/o los ID de Nodo de todos los maestros posibles antes de ser desplegados de manera que se puedan incluir en la ACL. Esto complica la gestión y el despliegue de dispositivos, especialmente en el caso de dispositivos embebidos que no tienen una interfaz de control dedicada (por ejemplo, un puerto USB), ya que tales dispositivos pueden no ser reconfigurables para actualizar la lista de nodos maestros. Por lo tanto sería beneficioso un mecanismo más simple para permitir a maestros inicialmente desconocidos escribir comandos en el recurso de un dispositivo embebido desplegado.

Se señala que el anterior es solamente un escenario ejemplo y los métodos y el aparato descritos en la presente memoria se pueden aplicar a otros escenarios. Por consiguiente, el ejemplo anterior no limita el alcance de la invención.

Descritos en la presente memoria están métodos y un aparato para compartir un recurso 106 de una red DHT basada en RELOAD 100 entre un número arbitrario de nodos, sin conocer por adelantado la lista completa de nodos permitidos. Es decir, los métodos y el aparato descritos en la presente memoria proporcionan acceso de escritura a uno o más nodos de acceso 104A que no son el nodo propietario 104B de un recurso 106 pero que desean almacenar datos en el recurso 106. El número de nodos de acceso 104A puede ser arbitrario y se puede aumentar o disminuir "sobre la marcha". En los métodos y el aparato ejemplares, la pertenencia al conjunto de nodos de acceso permitidos 104A se define demostrando la posesión de una clave secreta asociada con el recurso 106. La clave secreta es conocida por todos los miembros del conjunto. Los métodos y el aparato ejemplares descritos en la presente memoria se pueden aplicar a cualquiera de las políticas de control de acceso RELOAD ya definidas.

Un nodo 104B crea un recurso 106 en un par 102D. El nodo 104B se conoce como el nodo propietario y el par 102D se conoce como el par responsable. En los métodos y el aparato ejemplares, se puede escribir en el recurso por un nodo de acceso 104A, que no es el nodo propietario 104B. En la red ejemplar de la Figura 1, el nodo propietario 104B y el nodo de acceso 104A se muestran como clientes pero en otras redes ejemplares, el nodo propietario 104B y el nodo de acceso 104A pueden ser pares. En los métodos y el aparato ejemplares, el nodo propietario 104B puede ser un dispositivo embebido en un sistema separado. Por ejemplo, el dispositivo puede ser un sensor embebido en un sistema adaptado a un vehículo. El dispositivo se puede configurar para recibir instrucciones desde uno o más nodos maestros 104A, que pueden ser remotos del dispositivo por que están en una ubicación separada dentro de la red.

La Figura 2 muestra un diagrama de flujo de señalización que muestra métodos ejemplares implementados para permitir a un nodo de acceso 104A tener acceso de escritura a un recurso 106, en donde el nodo de acceso 104A no es el nodo propietario 104B. El nodo propietario 104B es capaz de crear un recurso de 106 y compartir sus permisos de escritura con otros nodos 104A por medio de un mecanismo de clave de escritura secreta compartida.

Las acciones emprendidas son:

A1 El propietario 104B obtiene la clave pública para el par responsable 102D. Esto se puede hacer enviando una Petición de Ping al par responsable 102D. La respuesta a la Petición de Ping incluye el certificado del par responsable 102D, que incluye la clave pública del par responsable.

A2 El propietario 104B crea un mensaje de Petición de Almacenamiento como se define en el protocolo base RELOAD, pero con una estructura StoreKindData específica. Para crear la estructura StoreKindData, el nodo propietario 104B cifra una clave de escritura secreta con la clave pública del par responsable y la incluye en la estructura StoreKindData. La estructura de datos también puede especificar un código de autenticación de mensaje (MAC), que especifica el algoritmo de autenticación que se debe usar por el nodo de acceso 104A cuando se escribe en el recurso 106. Se pueden usar otros tipos de algoritmo de autenticación.

Una estructura StoreKindData ejemplar se proporciona a continuación:

```
struct {
KindId          kind;
```

```
    uint64                generation_counter;
uint8            key_sign_type;
WriteKeySign write_key_sign;
StoredData     values<0..2^32-1>;
}StoreKindData;

struct {
select(key_sign_type) {
caseWRITE_KEY:
WriteKeywrite_key;
caseWRITE_SIGN:
     Signature write_sign;
    Case NONE:
     // Nothing
  }
} WriteKeySign;

struct {
MACAlgorithm          mac_algorithm; // From TLS
opaque                encrypted_key<0..255>;
} WriteKey;
```

Donde key_sign_type = WRITE_KEY, el campo mac_algorithm define el MAC a ser empleado por nodos de acceso 104A y el campo encrypted_key contiene la clave de escritura secreta asociada al recurso 106, cifrada con la clave pública del par responsable 102D que almacena el recurso (por ejemplo encrypted_key = cript{secret_key,

$Pub_{responsible_peer}$}). El algoritmo MAC puede ser, por ejemplo, HMAC-SHA256.

A3 El nodo propietario 104B envía la Petición de Almacenamiento hacia el par responsable 102D. La Petición de Almacenamiento se puede enviar directamente al par responsable 102D, si el nodo propietario 104B está en comunicación eléctrica directa con el par responsable 102D. La Petición de Almacenamiento se puede enviar a otro nodo, tal como un par separado (por ejemplo, 102C) en la red de superposición y pasar al par responsable 102D. Como la clave de escritura secreta se ha cifrado por la clave pública del par responsable 102D, solamente el par responsable 102D es capaz de descifrar la clave de escritura secreta. Por lo tanto, otros nodos en la red RELOAD 100 no son capaces de "fisgonear" la clave de escritura secreta.

Por lo tanto, en los métodos y el aparato ejemplares, el nodo propietario 104B y solamente el nodo propietario 104B, puede delegar el permiso para (re)escribir en el recurso 106 especificando una clave secreta en un campo definido recientemente, llamado write_key, de la operación Petición de Almacenamiento. La clave secreta se cifra usando la clave pública del par responsable 102D que almacena el recurso, de esta manera no se puede fisgonear por otros pares en la red RELOAD 100 reenviando el mensaje de Petición de Almacenamiento. El mismo mecanismo se puede emplear entonces cuando se almacena el recurso en las réplicas, como se trata más adelante.

A4 El par responsable 102D crea el recurso 106. El par responsable 102D descifra la clave de escritura secreta usando su clave privada y puede almacenar la clave de de escritura descifrada en una memoria. La clave de escritura secreta por ello se asocia con el recurso 106. Si el nodo propietario 104B también envió un MAC en la Petición de Almacenamiento, el par responsable 102D puede almacenar el MAC en una memoria y también asocia el MAC con el recurso 106.

A5 Un nodo de acceso 104A envía un mensaje de Petición de Almacenamiento al par responsable 102D. Los datos en el mensaje de Petición de Almacenamiento son los datos que el nodo de acceso 104A desea almacenar en el recurso 106. Los datos se firman por el nodo de acceso 104A usando la clave de escritura secreta, que es conocida para el nodo de acceso 104A. Si un MAC se asocia con el recurso 106, el nodo de acceso 104A firma los datos usando la clave de escritura secreta y el MAC.

Después de establecer una clave de escritura secreta y asociarla con el recurso 106, cualquier nodo que conoce la clave secreta es capaz de presentar operaciones Petición de Almacenamiento al par responsable 102D. En la estructura de datos ejemplar proporcionada

anteriormente, esto se hace ajustando key_sign_type = WRITE_SIGN y un campo write_sign (definido en el protocolo base RELOAD) que contiene el valor MAC de la estructura StoreKindData entera (es decir, sin el propio campo write_sign) concatenado con el ID de Recurso (por ejemplo, signature_value = hmac{StoreKindData|resourceID, secret_key}). Si un algoritmo de MAC se ha asociado con el recurso 106, el algoritmo usado por nodos de acceso debe ser el especificado en el campo mac_algorithm de la operación Petición de Almacenamiento enviada originalmente al par responsable 102D por el propietario 104B.

A6 El par responsable 102D recibe el mensaje de Petición de Almacenamiento desde el nodo de acceso 104B y controla el acceso al recurso 106 en base a la clave de escritura descifrada y los datos firmados. El par responsable 102D es capaz de usar su copia de la clave de escritura secreta descifrada para verificar que el nodo de acceso 104A tiene posesión de la clave secreta y por lo tanto está autorizado para almacenar datos en el recurso 106. Por lo tanto, si el par responsable verifica que el nodo de acceso 104A ha firmado los datos usando la clave de escritura secreta, permite a los datos ser almacenados en el recurso 106. Si un algoritmo de firma se ha asociado con el recurso 106, el par responsable también verifica que el algoritmo de firma correcto se ha usado por el nodo de acceso 104A cuando se firman los datos antes de permitir a los datos ser almacenados.

Usando el método descrito anteriormente, una política de control de acceso, que se puede denominar KEY-MATCH, permite a un recurso 106 ser compartido por un número arbitrario de nodos, sin requerir una lista explícita de dispositivos permitidos, como en, por ejemplo, la política de control de acceso USER-CHAIN-ACL. Por lo tanto, los métodos y el aparato descritos en la presente memoria no requieren al nodo propietario 104B del recurso 106 conocer de antemano la lista de nodos que comparten el recurso 106. Dado que los métodos y el aparato descritos en la presente memoria no permiten a nodos externos (es decir, que no conocen la clave compartida) escribir ningún dato en el recurso 106, no es vulnerable al ataque de Denegación de Servicio (DoS) tratado anteriormente.

Además, el par responsable 102D que almacena datos en el recurso 106 puede determinar fácilmente si se permite al nodo de acceso 104A escribir en el recurso 106, tan sólo comprobando los datos firmados en la Petición de Almacenamiento, en lugar de buscar el ID de Usuario y el ID de Nodo en la ACL y entonces comprobando la firma de clave pública del mensaje, que también requiere obtener y validar el certificado del solicitante.

Se señala que el nodo propietario 104B es capaz de almacenar datos en el recurso 106 enviando al par responsable 102D una Petición de Almacenamiento que no incluye un

campo write_key_sign (es decir key_sign_type = NONE).

En los métodos y el aparato ejemplares, el nodo propietario 104B puede cambiar la clave de escritura secreta y/o el algoritmo MAC enviando un nuevo mensaje de Petición de Almacenamiento. En base a la estructura ejemplar proporcionada anteriormente, la Petición de Almacenamiento debería incluir un campo key_sign_type fijado apropiadamente (es decir, key_sign_type = write_key) y debería identificar una nueva clave de escritura secreta cifrada con la clave pública del par responsable 102D y/o un nuevo algoritmo de firma, tal como un MAC.

Dado que el campo write_key_sign solamente aparece en mensajes de Petición de Almacenamiento dentro del protocolo base RELOAD, el resto de las operaciones de almacenamiento de datos de RELOAD (por ejemplo, Fetch, Stat) no se ven afectadas por los métodos y el aparato descritos en la presente memoria. Se señala que es importante para la clave de escritura secreta que no haya "fugas" en los metadatos del recurso (es decir, mediante una operación Stat).

Cualquier nodo que conoce la clave de escritura secreta es capaz de realizar una operación Almacenar firmando adicionalmente los datos a ser almacenados con el algoritmo de firma, tal como HMAC y usando la clave secreta asociada. Los datos almacenados en el recurso 106 tienen un campo generation_counter que se debería incrementar en cada mensaje. Por lo tanto, los ataques de repetición se pueden hacer menos probables si el nodo propietario 104B cambia la clave de escritura secreta asociada con el recurso antes de que se dé la vuelta al generation_counter. Es decir, antes de que el generation_counter exceda su valor máximo.

El par responsable 102D puede replicar el recurso 106 en una o más réplicas almacenadas en otros pares 102A-C y 102E-F. Esto se puede hacer enviando una Petición de Almacenamiento desde el par responsable 102D a un par réplica 102E.

La Figura 3 muestra un diagrama de flujo de señalización que muestra métodos ejemplares implementados para permitir al par responsable 102D crear un recurso réplica 108 en otro par 102E. En los métodos y el aparato ejemplares, las acciones emprendidas en la Figura 3 se pueden concatenar con las acciones mostradas en la Figura 2.

Las acciones emprendidas son:

B1-B4 El nodo propietario 104B obtiene la clave pública del par responsable 102D, crea una Petición de Almacenamiento y envía la Petición de Almacenamiento al par responsable 102D. El par responsable 102D crea el recurso 106. Las acciones B1-B4 son similares a las

acciones A1-A4 anteriores y no se explican en detalle de nuevo.

B5 El par responsable 102D crea y envía una Petición de Almacenamiento al par réplica 102E. La Petición de Almacenamiento incluye un campo wholewrite_key. La clave de escritura secreta cifrada recibida desde el nodo propietario 104B se descifra y entonces cifra con la clave pública del par réplica (por ejemplo, encrypted_key = cript{secret_key, $Pub_{replica_peer}$}. Cada par almacena en su caché los certificados de los otros pares en la red superpuesta y así cada par conoce la clave pública de todos los otros pares. Si no, la clave pública del par réplica 102E se puede obtener enviando una Petición de Ping de una manera similar al mecanismo descrito en A1/B1.

B6 El par réplica 102E crea un recurso réplica 108 de una manera similar al par responsable 102D. Es decir, el par réplica 102E descifra la clave de escritura secreta usando su clave privada y puede almacenar la clave de escritura descifrada en una memoria. La clave de escritura secreta se asocia por ello con el recurso réplica 108. Si el nodo propietario 104B también envió un algoritmo de firma, tal como un MAC, en la Petición de Almacenamiento al par responsable 102D, este se puede enviar al par réplica 102E, que puede almacenar el MAC en una memoria y también asociar el MAC con el recurso réplica 108.

B7-B8 Un nodo de acceso 104A envía una Petición de Almacenamiento al par responsable 102D y el par responsable 102D controla el acceso de escritura al recurso 106 de una manera similar a la descrita en las acciones A5-A6.

B9-B10 El par responsable envía una Petición de Almacenamiento al par réplica 102E. En este caso, el par responsable 102D no tiene que enviar el campo de Firma write_sign a las réplicas, dado que ya se ha verificado por el par responsable 102D. Es decir, el key_sign_type = NONE. El par réplica 102E escribe los datos en el recurso réplica 108 en base a la verificación emprendida por el par responsable 102D.

La Figura 4, muestra un dispositivo de red configurado como un par 102D responsable de un recurso 106 en una red RELOAD 100. El par responsable 102D comprende un comunicador 400, que comprende un receptor 401 y un transmisor 402. El par responsable 102D comprende además un descifrador 404, un controlador de acceso 405 y una memoria 406. Cada uno del receptor 401, el transmisor 402, el procesador 404 y la memoria 406 está en comunicación eléctrica con todos los otros rasgos 401, 402, 404, 406 en el par responsable 102D. Además, el comunicador 400 está en comunicación eléctrica con otros nodos en la red 100 y se configura para transmitir y recibir mensajes a/desde esos nodos. El par

responsable 102D se puede implementar como una combinación de hardware y software informático. En particular, el descifrador 404 y el controlador de acceso 405 se pueden implementar como software configurado para ejecutarse en un procesador. La memoria 406 almacena los diversos programas/archivos ejecutables que se pueden implementar por un procesador y también proporciona una unidad de almacenamiento para cualesquiera datos requeridos. Los programas/archivos ejecutables almacenados en la memoria 406 e implementados por el procesador, pueden incluir pero no están limitados a un comunicador, un descifrador y un controlador de acceso que están configurados para implementar los métodos descritos anteriormente.

En el aparato ejemplar, el comunicador 400 y específicamente el receptor 401, se configura para recibir un mensaje que se origina desde el nodo propietario 104B que comprende la clave de escritura secreta cifrada con la clave pública del par responsable 102D. Los comunicadores ejemplares 400 se configuran para recibir una Petición de Almacenamiento desde el nodo propietario 104B para crear el recurso 106. La Petición de Almacenamiento puede comprender una estructura StoreKindData como se expuso anteriormente. La Petición de Almacenamiento puede ser una Petición de Almacenamiento inicial y el par responsable se puede configurar para crear un recurso de 106 en la memoria 406. Alternativamente, la Petición de Almacenamiento puede relacionarse con un recurso existente 106.

El comunicador 400 se configura además para recibir una petición que se origina desde un nodo de acceso 104A para almacenar datos en el recurso 106. La petición comprende datos firmados por el nodo de acceso 104A usando la clave de escritura secreta. La petición puede ser una Petición de Almacenamiento como se expuso anteriormente.

El descifrador 404 se configura para descifrar la clave de escritura secreta cifrada usando la clave privada del par responsable 102D. En pares responsables ejemplares 102D, la clave de escritura secreta descifrada se puede almacenar en la memoria 406. El controlador de acceso 405 se configura para controlar el acceso de escritura al recurso 106 por el nodo de acceso 104A, en base a la clave de escritura y los datos recibidos. Si los datos recibidos se han firmado usando la clave de escritura secreta, el controlador de acceso se puede configurar para almacenar los datos en el recurso 106.

El mensaje que se origina desde el nodo propietario 104B puede comprender adicionalmente un algoritmo de firma, tal como un MAC, como se expuso anteriormente. En tales casos, el algoritmo de firma se debería usar por un nodo de acceso cuando se firman los datos. El controlador de acceso por lo tanto se puede configurar además para almacenar

los datos recibidos en el recurso 106 si los datos se han firmado usando la clave de escritura secreta y el algoritmo de firma.

Como se expuso anteriormente, el par responsable 102D se configura de manera que el controlador de acceso permita al nodo propietario 104B almacenar datos en el recurso 106. Es decir, el nodo propietario 104B puede almacenar datos en el recurso 106 sin la necesidad de firmar los datos usando la clave de escritura secreta.

Un replicador 407 también puede ser embebido en software ejecutado en un procesador y configurado para crear un recurso de réplica 108 en un par réplica 102E. El transmisor 402 se puede configurar para transmitir una Petición de Almacenamiento al par réplica 102E. Por lo tanto, el replicador de 407 se puede configurar para obtener la clave pública del par réplica 102E, cifrar la clave de escritura secreta con la clave pública obtenida y enviar la clave de escritura secreta cifrada al par réplica 102E.

La Figura 5 muestra un dispositivo de red configurado como un nodo 104B que posee un recurso 106 dentro de una red RELOAD 100. El nodo propietario 104B comprende un comunicador 500 que comprende un receptor 501 y un transmisor 502. El nodo propietario 104B comprende además un cifrador 504 y una memoria 506. Cada uno del receptor 501, el transmisor 502, el cifrador 504 y la memoria 506 está en comunicación eléctrica con todos los otros rasgos 501, 502, 504, 506 en el nodo propietario 104B. Además, el comunicador 500 está en comunicación eléctrica con otros nodos en la red 100 y configurado para transmitir y recibir mensajes a/desde esos nodos. El nodo propietario 104B se puede implementar como una combinación de hardware y software informático. En particular, el cifrador 404 y el controlador de acceso 405 se pueden implementar como software configurado para ejecutarse en un procesador. La memoria 506 almacena los diversos programas/archivos ejecutables que se implementan por un procesador y también proporciona una unidad de almacenamiento para cualesquiera datos requeridos. Los programas/archivos ejecutables almacenados en la memoria 506 e implementados por el procesador, pueden incluir pero no están limitados a un comunicador y un cifrador que se configuran para implementar los métodos descritos anteriormente.

Específicamente, el comunicador 500 se configura para comunicar con otros nodos en la red 100 para obtener la clave pública del par responsable 102D. El cifrador se configura para cifrar la clave de escritura usando la clave pública obtenida del par responsable 102D. El transmisor 502 del comunicador 500 se configura para enviar la clave de escritura cifrada al par responsable 102D para controlar el acceso de escritura al recurso 106.

El comunicador 500 puede comunicar con los otros nodos en la red 100 para obtener la clave pública usando una Petición de Ping.

El comunicador 500 se puede configurar además para enviar un algoritmo de firma con la clave de escritura cifrada. El algoritmo de firma debería identificar el algoritmo de firma a ser usado por un nodo de acceso 104A que desea escribir en el recurso 106. La clave de escritura cifrada y el algoritmo de firma se pueden enviar en una Petición de Almacenamiento que define una estructura StoreKindData. El algoritmo de firma puede ser un MAC.

El dispositivo de red configurado como un nodo propietario 104B se puede integrar en un sistema informático y puede comprender además un procesador de instrucciones 505 configurado para recibir instrucciones desde los nodos de acceso 104A. Como se muestra en la Figura 7, en un sistema informático embebido ejemplar, el nodo propietario 104B puede ser un dispositivo, tal como un sensor, embebido dentro del sistema informático de un vehículo 700. El dispositivo de red por lo tanto puede formar parte de un sistema remoto configurado para comunicar con una red superpuesta de una red RELOAD 100. El sensor se puede configurar para recibir instrucciones desde los nodos de acceso 104A a través del recurso 106. El sensor puede sondear el recurso 106 en diferentes momentos para recuperar instrucciones. El dispositivo embebido se puede desplegar sin preconfigurar la lista completa de maestros, pero tan sólo con una clave de escritura secreta generada aleatoriamente. Entonces un maestro solamente necesita conocer el identificador del dispositivo y su clave de escritura secreta. Estos datos se pueden imprimir en un manual o se pueden almacenar en el dispositivo en sí mismo. Por lo tanto un dispositivo se puede controlar fácilmente por un número arbitrario de maestros sin tener que gestionar una ACL explícita.

La Figura 6 muestra un dispositivo de red configurado como un nodo de acceso 104A que está separado de un nodo 104B que posee un recurso 106 dentro de una red RELOAD 100. El nodo de acceso 104A comprende un comunicador 600 que comprende un receptor 601 y un transmisor 602. El nodo de acceso 104A comprende además un firmante 604 y una memoria 606. Cada uno del receptor 601, el transmisor 602, el firmante 604 y la memoria 606 está en comunicación eléctrica con todos los otros rasgos 601, 602, 604, 606 en el nodo de acceso 104A. Además, el comunicador 600 está en comunicación eléctrica con otros nodos en la red 100 y configurado para transmitir y recibir mensajes a/desde esos nodos. El nodo de acceso 104A se puede implementar como una combinación de hardware y software informático. En particular, el firmante se puede encarnar en software para ejecutar en un

procesador. La memoria 606 almacena los diversos programas/archivos ejecutables que se implementan por un procesador y también proporciona una unidad de almacenamiento para cualesquiera datos requeridos. Los programas/archivos ejecutables almacenados en la memoria 606 e implementados por el procesador, pueden incluir pero no están limitados a un firmante y un comunicador que se configuran para implementar los métodos descritos anteriormente.

El firmante 604 está configurado para firmar datos a ser escritos en el recurso 106 usando la clave de escritura secreta. El comunicador 600 se configura para generar una petición para escribir los datos en el recurso 106 no poseído por el nodo de acceso 104A y para enviar la petición al par responsable 102D. El firmante se puede configurar para usar un algoritmo de firma predeterminado, tal como un MAC. La petición puede comprender una Petición de Almacenamiento que comprende el ID de Recurso del recurso 106.

Con referencia de nuevo a la Figura 1, el par responsable 102D, nodo propietario 104B y el nodo de acceso 104A pueden formar juntos un sistema para controlar el acceso de escritura a un recurso 106 en una red RELOAD 100.

La Figura 8 muestra un diagrama de flujo para un método de control de un dispositivo de red configurado como un par responsable de un recurso dentro de una red RELOAD. En el dispositivo de red, se recibe 800 un mensaje que se origina desde un nodo que posee el recurso. El mensaje comprende la clave de escritura cifrada usando una clave pública del dispositivo de red. Se recibe 802 una petición para almacenar datos en el recurso. La petición se origina desde uno o más nodos de acceso y comprende datos firmados que usan la clave de escritura. El uno o más nodos de acceso son diferentes al nodo que posee el recurso. La clave de escritura cifrada se descifra 804 usando la clave privada del dispositivo de red. El acceso de escritura al recurso se controla 806 por el uno o más nodos de acceso en base a la clave de escritura y los datos recibidos.

La Figura 9 muestra un diagrama de flujo para un método de control de un dispositivo de red configurado como un nodo que posee un recurso dentro de una red RELOAD. El dispositivo de red comunica 900 con uno o más nodos dentro de la red RELOAD para obtener una clave pública de un par responsable del recurso. La clave de escritura se cifra 902 usando la clave pública obtenida. La clave de escritura cifrada se envía 904 al par responsable del recurso para controlar el acceso de escritura al recurso.

La Figura 10 muestra un diagrama de flujo para un método de control de un dispositivo de red configurado como un nodo de acceso para escribir datos en un recurso dentro de una

red RELOAD, en donde el recurso se posee por un nodo diferente. En el dispositivo de red, los datos a ser escritos en el recurso se firman 1000 usando la clave de escritura. Se genera 1002 una petición para escribir los datos firmados en el recurso no poseído por el dispositivo de red. La petición se envía 1004 al par responsable del recurso.

La Figura 11 muestra un diagrama de flujo para un método de control de acceso de escritura por uno o más nodos de acceso a un recurso dentro de una red RELOAD. En el nodo que posee el recurso, se obtiene la clave pública del par responsable del recurso, la clave de escritura se cifra usando la clave pública obtenida y la clave de escritura cifrada se envía al par responsable del recurso 1100. En el par responsable del recurso, se descifra 1102 la clave de escritura. En el nodo de acceso, se firman datos a ser escritos en el recurso usando la clave de escritura y se envía una petición al par responsable del recurso para escribir los datos firmados en el recurso 1104. En el par responsable del recurso, el acceso de escritura al recurso se controla en base a la clave de escritura descifrada y los datos firmados.

Un programa informático se puede configurar para proporcionar cualquiera de los métodos descritos anteriormente. El programa informático se puede proporcionar en un medio legible por ordenador. El programa informático puede ser un producto de programa informático. El producto puede comprender un medio de almacenamiento utilizable por ordenador no transitorio. El producto de programa informático puede tener código de programa legible por ordenador encarnado en el medio configurado para realizar el método. El producto de programa informático se puede configurar para hacer a al menos un procesador realizar algo de o todo el método.

Diversos métodos y un aparato se describen en la presente memoria con referencia a diagramas de bloques o ilustraciones de diagramas de flujo de métodos implementados por ordenador, aparatos (sistemas y / o dispositivos) y/o productos de programas informáticos. Se entiende que un bloque de los diagramas de bloques y/o ilustraciones de diagramas de flujo y combinaciones de bloques en los diagramas de bloques y/o ilustraciones de diagramas de flujo, se pueden implementar por instrucciones de programa informático que se realizan por uno o más circuitos de ordenador. Estas instrucciones de programa informático se pueden proporcionar a un circuito procesador de un circuito informático de propósito general, circuito informático de propósito especial y/u otro circuito de procesamiento de datos programable para producir una máquina, de manera que las instrucciones, que se ejecutan a través del procesador del ordenador y/u otro aparato de procesamiento de datos programable, transforman y controlan los transistores, los valores

almacenados en las posiciones de memoria y otros componentes hardware dentro de tal circuitería para implementar las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagramas de flujo y por ello crear medios (funcionalidad) y/o la estructura para implementar las funciones/actos especificados en los diagramas de bloques y/o bloque(s) de diagramas de flujo.

También se pueden almacenar instrucciones de programa informático en un medio legible por ordenador que pueden dirigir un ordenador u otro aparato de procesamiento de datos programable para funcionar de una manera particular, de manera que las instrucciones almacenadas en el medio legible por ordenador producen un artículo de fabricación que incluye instrucciones que implementan las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagramas de flujo.

Un medio legible por ordenador tangible, no transitorio puede incluir un sistema, aparato o dispositivo de almacenamiento de datos electrónico, magnético, óptico, electromagnético o de semiconductores. Ejemplos más específicos del medio legible por ordenador incluirían los siguientes: un disquete de ordenador portátil, un circuito de memoria de acceso aleatorio (RAM), un circuito de memoria de sólo lectura (ROM), un circuito de memoria de sólo lectura programable y borrable (EPROM o memoria rápida), un disco compacto portátil de memoria de sólo lectura (CD-ROM) y un disco de vídeo digital portátil de memoria de sólo lectura (DVD/Blu-ray).

Las instrucciones de programa informático también se pueden cargar en un ordenador y/u otro aparato de procesamiento de datos programable para causar una serie de pasos de operación a ser realizados en el ordenador y/u otro aparato programable para producir un proceso implementado por ordenador de manera que las instrucciones que se ejecutan en el ordenador u otro aparato programable proporcionan pasos para implementar las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagramas de flujo.

Por consiguiente, la invención se puede encarnar en hardware y/o en software (incluyendo microprogramas, software residente, microcódigo, etc.) que se ejecuta en un procesador, que se puede conocer en conjunto como "circuitería", "un módulo" o variantes de los mismos.

También se debería señalar que en algunas implementaciones alternativas, las funciones/actos señalados en los bloques pueden ocurrir fuera del orden señalado en los diagramas de flujo. Por ejemplo, dos bloques mostrados en sucesión de hecho se pueden

ejecutar sustancialmente concurrentemente o los bloques a veces se pueden ejecutar en el orden inverso, dependiendo de la funcionalidad/actos implicados. Además, la funcionalidad de un bloque dado de los diagramas de flujo y/o diagramas de bloques se puede separar en múltiples bloques y/o la funcionalidad de dos o más bloques de los diagramas de flujo y/o diagramas de bloques se puede integrar al menos parcialmente. Finalmente, se pueden añadir/insertar otros bloques entre los bloques que se ilustran.

Los expertos concebirán realizaciones adicionales de la invención sin apartarse del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un dispositivo de red para control de acceso de escritura a un recurso dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD, (100), el dispositivo de red (102D) configurado como un par responsable de un recurso (106) que comprende:

un comunicador (400) configurado para recibir un mensaje que se origina desde un nodo (104B) que posee el recurso, el mensaje que comprende una clave de escritura cifrada que usa una clave pública del dispositivo de red,

y configurado además para recibir una petición para almacenar datos en el recurso, la petición que se origina desde uno o más nodos de acceso (104A) y que comprende datos firmados que usan la clave de escritura, el uno o más nodos de acceso que son diferentes al nodo que posee el recurso;

un descifrador (404) configurado para descifrar la clave de escritura cifrada usando la clave privada del dispositivo de red; y

un controlador de acceso (405) configurado para controlar el acceso de escritura al recurso por el uno o más nodos de acceso en base a la clave de escritura y los datos firmados recibidos.

2. Un dispositivo de red (102D) según la reivindicación 1, en donde el controlador de acceso (405) se configura para escribir los datos recibidos en el recurso si los datos recibidos se han firmado usando la clave de escritura.

3. Un dispositivo de red (102D) según la reivindicación 1 o 2, en donde el mensaje que se origina desde el nodo (104b) que posee el recurso comprende además un algoritmo de firma a ser usado por el uno o más nodos de acceso (104a) cuando se firman los datos,

y en donde el controlador de acceso (405) se configura además para escribir los datos recibidos en el recurso (106) si los datos recibidos se han firmado usando el algoritmo de firma y la clave de escritura.

4. Un dispositivo de red (102D) según cualquier reivindicación precedente, que comprende además un replicador (407) configurado para replicar el recurso (106) en un par adicional (102E) de la red RELOAD (100) enviando un mensaje de Petición de Almacenamiento al par adicional y en donde el replicador se configura para cifrar la clave de escritura con la clave pública obtenida del par adicional y enviar la clave de escritura cifrada al par adicional en el mensaje de Petición de Almacenamiento.

5. Un dispositivo de red (104B) configurado como un nodo que posee un recurso (106) dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD, (100), el dispositivo de red que comprende:

un comunicador (500) configurado para comunicar con uno o más nodos dentro de la red RELOAD para obtener una clave pública de un par (102D) responsable del recurso; y

un cifrador (504) configurado para cifrar una clave de escritura usando la clave pública obtenida;

en donde el comunicador se configura además para enviar la clave de escritura cifrada al par responsable del recurso para controlar el acceso de escritura al recurso.

6. Un dispositivo de red (104B) según la reivindicación 5, en donde el comunicador (500) se configura además para enviar un algoritmo de firma al par (102D) responsable del recurso (106) que identifica el algoritmo de firma que se debería usar por uno o más nodos de acceso (104A) que solicitan acceso de escritura al recurso.

7. Un dispositivo de red (104B) según cualquiera de las reivindicaciones 5 o 6, en donde el comunicador se configura para enviar la clave de escritura cifrada y/o el algoritmo de firma en un mensaje de Petición de Almacenamiento que define una estructura StoreKindData.

8. Un dispositivo de red (104B) según cualquiera de las reivindicaciones 5 a 7, en donde el dispositivo de red está incrustado dentro de un sistema informático y comprende además un procesador de instrucciones (505) configurado para recibir instrucciones desde uno o más nodos de acceso (104A), a través del recurso (106).

9. Un dispositivo de red (104B) según la reivindicación 8, en donde el procesador de instrucciones (505) se configura para sondear el recurso (106) en diferentes momentos para recuperar instrucciones.

10. Un dispositivo de red (104B) según cualquiera de las reivindicaciones 7 a 9, configurado además para cambiar la clave de escritura antes de se dé la vuelta a un contador de generación, el contador de generación que se asocia con valores almacenados en el recurso (106).

11. Un vehículo (700) que comprende un dispositivo de red (104B) según cualquiera de las reivindicaciones 7 a 10.

12. Un dispositivo de red (104A) configurado como un nodo de acceso para escribir datos en un recurso (106) dentro de una red de Localización Y Descubrimiento de Recursos,

RELOAD, (100), en donde el recurso es propiedad de un nodo diferente, el dispositivo de red que comprende:

un firmante (604) configurado para firmar datos a ser escritos en el recurso usando una clave de escritura;

un comunicador (600) configurado para generar una petición para escribir los datos firmados en el recurso no poseído por el dispositivo de red y enviar la petición a un par (102D) responsable del recurso.

13. Un dispositivo de red (104A) según la reivindicación 12, en donde el firmante (604) se configura para firmar los datos usando la clave de escritura y un algoritmo de firma predeterminado.

14. Un dispositivo de red (104A) según la reivindicación 13, en donde el comunicador (600) se configura para generar y enviar una Petición de Almacenamiento.

15. Un dispositivo de red (104A) según la reivindicación 14, en donde la Petición de Almacenamiento comprende un ID de Recurso del recurso.

16. Un dispositivo para control de acceso de escritura a un recurso en una red RELOAD método de control de un dispositivo de red (102D) configurado como un par responsable de un recurso (106) dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD, (100), el método que comprende, en el dispositivo de red:

recibir (800) un mensaje que se origina desde un nodo (104B) que posee el recurso, el mensaje que comprende una clave de escritura cifrada que usa una clave pública del dispositivo de red;

recibir (802) una petición para almacenar datos en el recurso, la petición que se origina desde uno o más nodos de acceso (104A) y que comprende datos firmados usando la clave de escritura, el uno o más nodos de acceso que son diferentes al nodo que posee el recurso;

descifrar (804) la clave de escritura cifrada usando la clave privada del dispositivo de red; y

controlar (806) el acceso de escritura al recurso por el uno o más nodos de acceso en base a la clave de escritura y los datos recibidos.

17. Un método de control de un dispositivo de red (104B) configurado como un nodo que posee un recurso (106) dentro de una red de Localización Y Descubrimiento de Recursos,

RELOAD, (100), el método que comprende, en el dispositivo de red:

Comunicar (900) con uno o más nodos dentro de la red RELOAD para obtener una clave pública de un par (102D) responsable del recurso;

Cifrar (902) una clave de escritura usando la clave pública obtenida; y

Enviar (904) la clave de escritura cifrada al par responsable del recurso para controlar el acceso de escritura al recurso.

18. Un método de control de un dispositivo de red (104A) configurado como un nodo de acceso para escribir datos en un recurso (106) dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD, (100), en donde el recurso se posee por un nodo diferente (104B), el método que comprende, en el dispositivo de red:

firmar (1000) datos a ser escritos en el recurso usando una clave de escritura;

generar (1002) una petición para escribir los datos firmados en el recurso no poseído por el dispositivo de red; y

enviar (1004) la petición a un par (102D) responsable del recurso.

19. Un sistema para controlar el acceso de escritura por uno o más nodos de acceso (104A) a un recurso (106) dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD, (100), el sistema que comprende:

un nodo (104B) que posee el recurso y configurado para obtener una clave pública de un par (102D) responsable del recurso, para cifrar una clave de escritura usando la clave pública obtenida y para enviar la clave de escritura cifrada al par responsable del recurso;

el par responsable del recurso que se configura para descifrar la clave de escritura cifrada;

un nodo de acceso configurado para firmar datos a ser escritos en el recurso usando la clave de escritura y para enviar una petición al par responsable del recurso para escribir los datos firmados en el recurso;

en donde el par responsable del recurso se configura además para controlar el acceso de escritura al recurso en base a la clave de escritura descifrada y los datos firmados.

20. Un método para control de acceso de escritura a un recurso (106) dentro de una red de Localización Y Descubrimiento de Recursos, RELOAD, (100) por uno o más nodos de acceso (104A), el método que comprende:

en un nodo (104B) que posee el recurso, obtener (1100) una clave pública de un par responsable del recurso, cifrar una clave de escritura usando la clave pública obtenida y enviar la clave de escritura cifrada al par responsable del recurso;

en el par (102D) responsable del recurso, descifrar (1102) la clave de escritura;

en un nodo de acceso, firmar (1104) datos a ser escritos en el recurso usando la clave de escritura y enviar una petición al par responsable del recurso para escribir los datos firmados en el recurso; y

en el par responsable del recurso, controlar (1106) el acceso de escritura al recurso en base a la clave de escritura descifrada y los datos firmados.

21. Un medio legible por ordenador no transitorio que comprende código legible por ordenador configurado para llevar a cabo cualquiera de los métodos de las reivindicaciones 16 a 18 y 20.

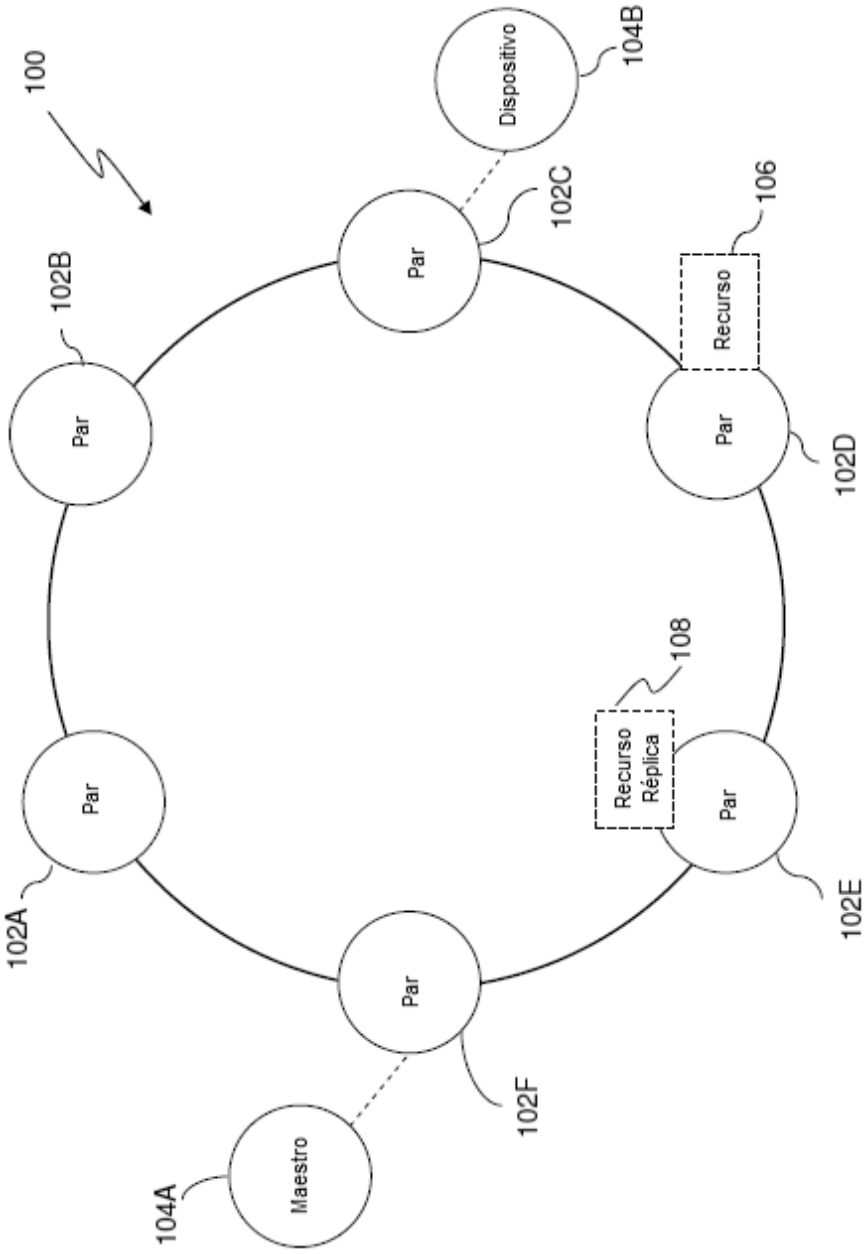
100
102A
Par
102B
Par
Dispositivo
104B
Par
102C
Recurso
106
Par
102D
Recurso
Réplica
108
Par
102E
Par
102F
Maestro
104A

Figura 1

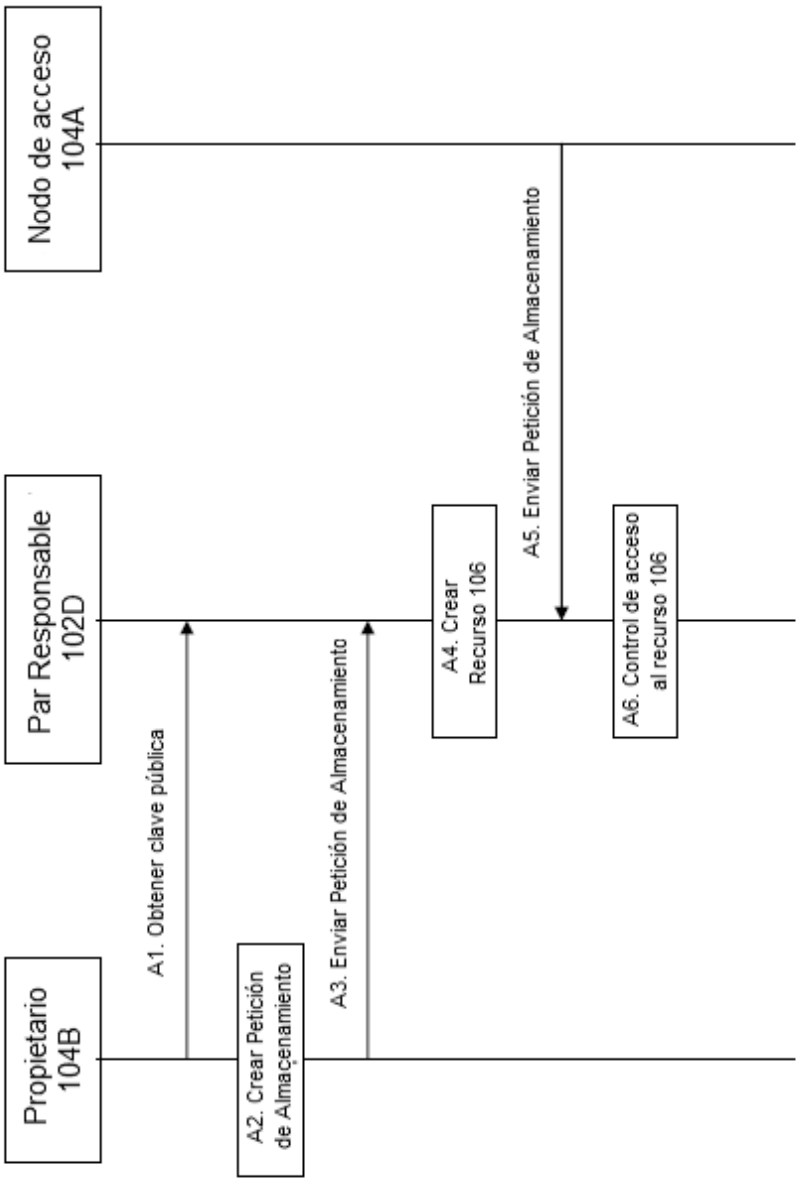
Propietario 104B
Par Responsable 102D
Nodo de acceso 104A
A1. Obtener clave pública
A2. Crear Petición de Almacenamiento
A3. Enviar Petición de Almacenamiento
A4. Crear Recurso 106
A5. Enviar Petición de Almacenamiento
A6. Control de acceso al recurso 106

Figura 2

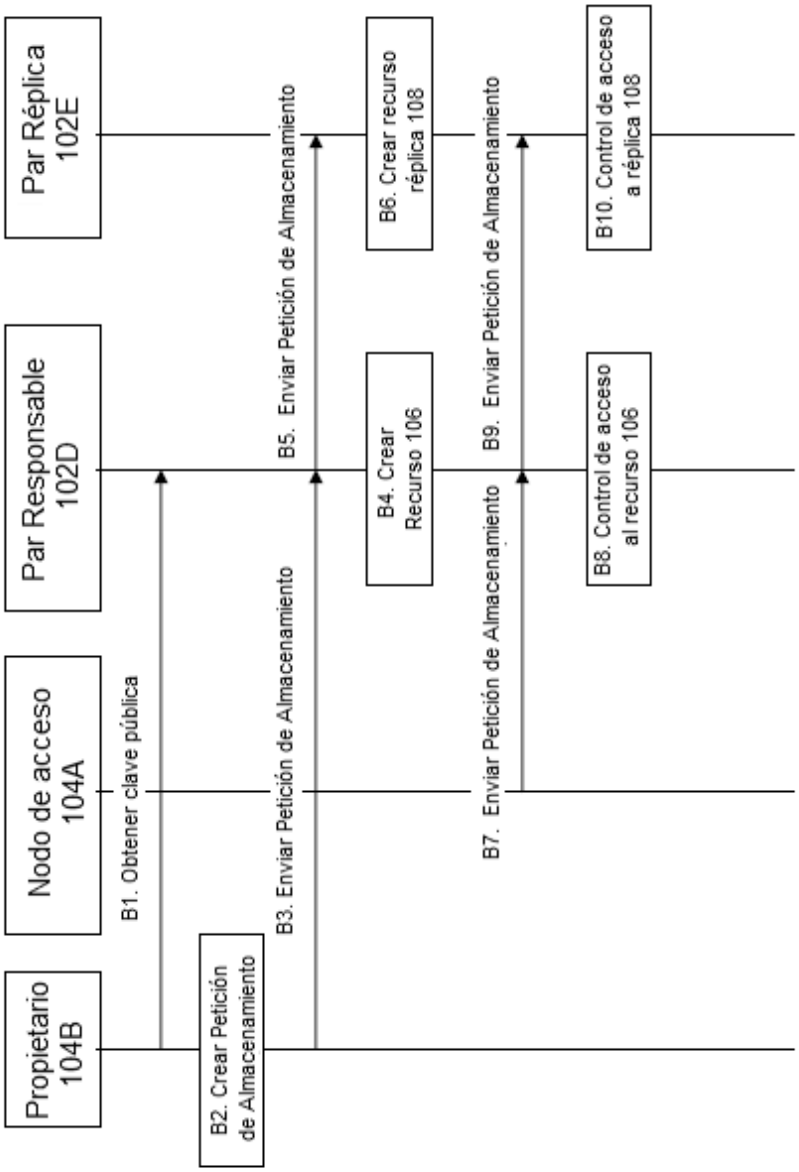
Propietario 104B
Nodo de acceso 104A
Par Responsable 102D
Par Réplica 102E
B1. Obtener clave pública
B2. Crear Petición de Almacenamiento
B3. Enviar Petición de Almacenamiento
B4. Crear Recurso 106
B5. Enviar Petición de Almacenamiento
B6. Crear recurso réplica 108
B7. Enviar Petición de Almacenamiento
B8. Control de acceso al recurso 106
B9. Enviar Petición de Almacenamiento
B10. Control de acceso a réplica 108

Figura 3

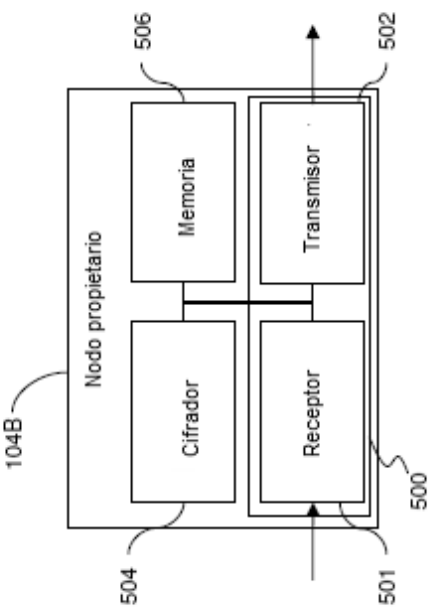

Figura 5

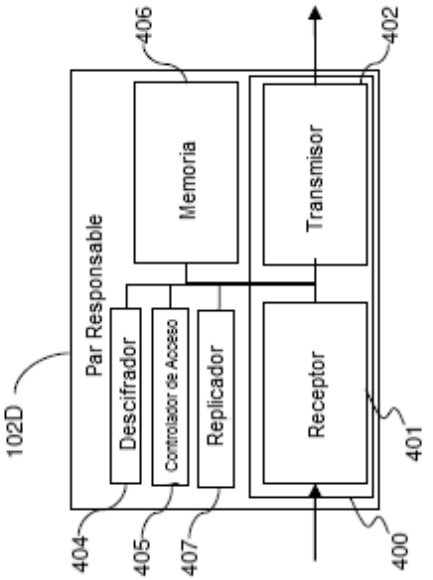

Figura 4

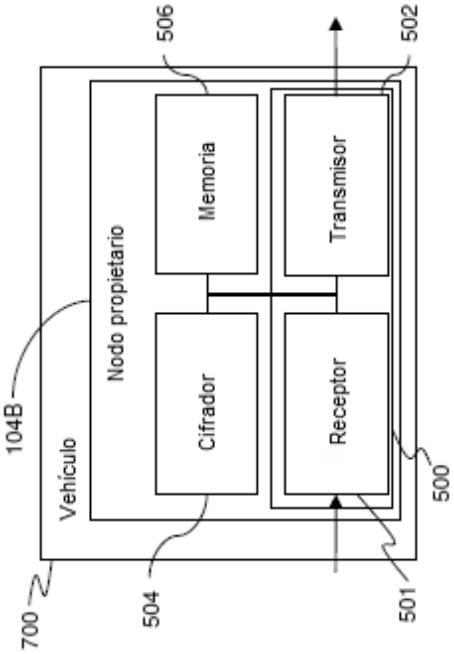

Figura 7

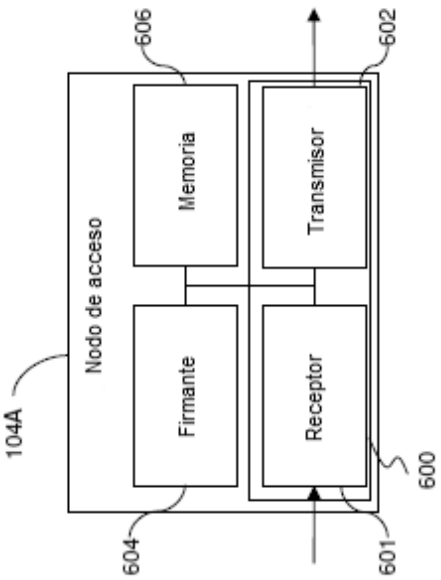

Figura 6

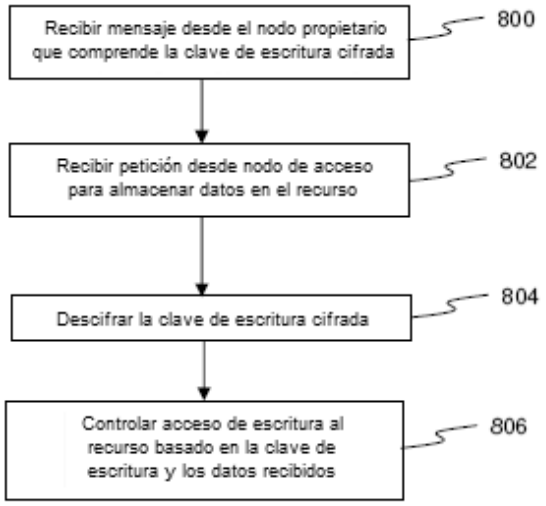

Figura 8

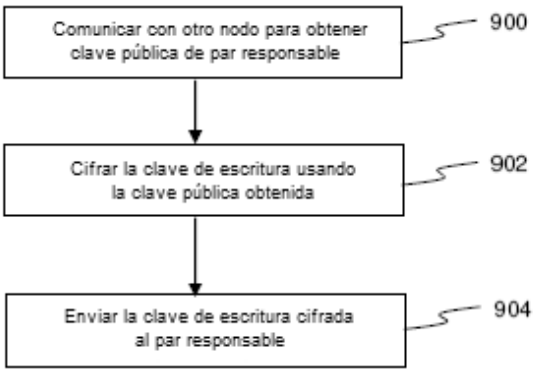

Figura 9

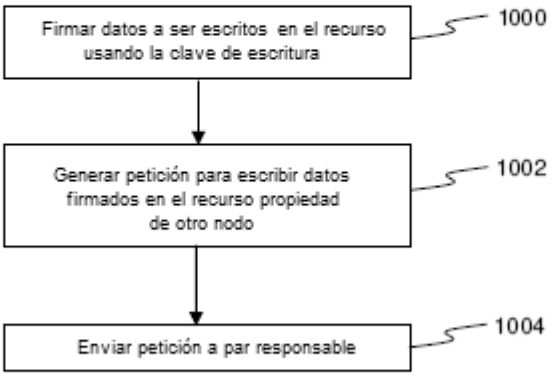

Figura 10

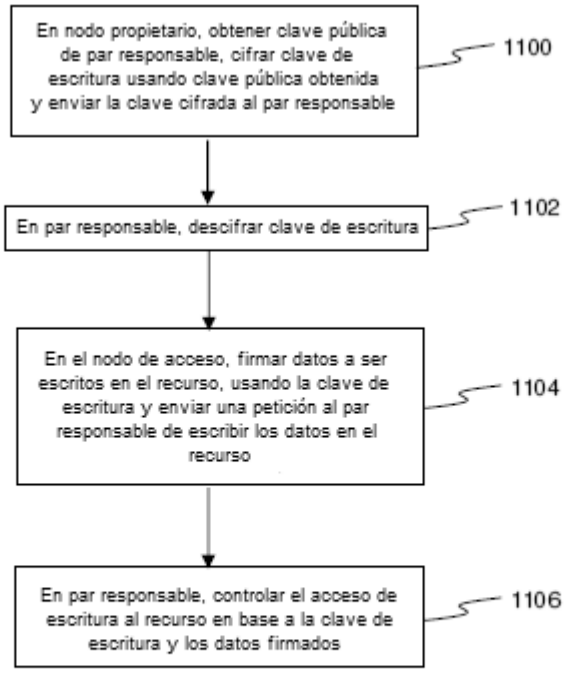

Figura 11

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201590098

(22) Fecha de presentación de la solicitud: 07.03.2013

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L29/08*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
X	JENNINGS CISCO B LOWEKAMP C et al. REsource LOcation And Discovery (RELOAD) Base Protocol; draft-ietf-p2psip-base-24.txt.Resource LOcation And Discovery (RELOAD) Base Protocol; draft-ietf-p2psip-base-24.txt, 20130119 Internet Engineering Task Force, IETF; StandardWorkingDraft, Internet Society (ISOC) 4, rue des Falaises CH-1205 Geneva, Switzerland 19.01.2013 VOL: Págs: 1-173 (Secciones 4.1, 7.3)	12-15,18,21
A		1-11,16-17,19-20
A	KNAUF T C SCHMIDT A et al. A Usage for Shared Resources in RELOAD (ShaRe); draft-ietf-p2psip-share-01.txt.A Usage for Shared Resources in RELOAD (ShaRe); draft-ietf-p2psip-share-01.txt, 20130224 Internet Engineering Task Force, IETF; StandardWorkingDraft, Internet Society (ISOC) 4, rue des Falaises CH-1205 Geneva, Switzerland 24.02.2013 VOL: Págs: 1-24	1-21

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
07.04.2016	M. Muñoz Sánchez	1/5

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

Fecha de Realización de la Opinión Escrita: 07.04.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-11, 16-17, 19- 20	**SI**
	Reivindicaciones	12-15, 18, 21	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	1-11, 16-17, 19-20	**SI**
	Reivindicaciones		**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.

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	JENNINGS CISCO B LOWEKAMP C et al. REsource LOcation And Discovery (RELOAD) Base Protocol; draft-ietf-p2psip-base-24.txt.Resource LOcation And Discovery (RELOAD) Base Protocol; draft-ietf-p2psip-base-24.txt, 20130119 Internet Engineering Task Force, IETF; StandardWorkingDraft, Internet Society (ISOC) 4, rue des Falaises CH-1205 Geneva, Switzerland 19.01.2013 VOL: Págs: 1-173 (Secciones 4.1, 7.3)	19.01.2013
D02	KNAUF T C SCHMIDT A et al. A Usage for Shared Resources in RELOAD (ShaRe); draft-ietf-p2psip-share-01.txt.A Usage for Shared Resources in RELOAD (ShaRe); draft-ietf-p2psip-share-01.txt, 20130224 Internet Engineering Task Force, IETF; StandardWorkingDraft, Internet Society (ISOC) 4, rue des Falaises CH-1205 Geneva, Switzerland 24.02.2013 VOL: Págs: 1-24	24.02.2013

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 dispositivo de red configurado como par responsable de un recurso dentro de una red RELOAD. El dispositivo de red tiene un comunicador para recibir un mensaje del nodo que posee el recurso y configurado además para recibir una petición para almacenar datos, petición originada de uno o más nodos de acceso y que comprende datos firmados que una clave de escritura, siendo el uno o más nodos de acceso diferentes al nodo que posee el recurso. El dispositivo de red también tiene un controlador de acceso configurado para controlar el acceso de escritura al recurso por el uno o más nodos de acceso en base a la clave de escritura y los datos firmados recibidos. En el documento D01 se plantean varias opciones para controlar el acceso basándose todas ellas en el control de acceso aplicando funciones hash.
La diferencia entre la reivindicación 1 y el documento D01 se refiere a la forma de control de acceso al recurso de forma eficiente (mediante cifrado de la clave de escritura del poseedor del recurso con la clave pública del dispositivo de red para descifrarla en el dispositivo de red utilizando su clave privada y comparar dicha clave de escritura descifrada con la aportada por el uno o más nodos de acceso) por lo que, a la luz del documento D01, el problema técnico objetivo que la invención resuelve de forma no evidente consistiría en cómo conseguir dicho control de acceso eficiente.
El documento D02 por su parte define un uso para la gestión de acceso para escribir datos en recursos RELOAD. El documento no concreta el control del acceso mediante clave pública del dispositivo de red sino mediante listas.
En conclusión, ninguno de los documentos D01 o D02 resuelve el problema técnico objetivo planteado y así la reivindicación 1 tiene actividad inventiva según el art. 8.1 de la Ley 11/86 de Patentes.

Reivindicación 5: esta reivindicación se corresponde directamente con el dispositivo de la reivindicación 1 y, por tanto, también tiene actividad inventiva según el art. 8.1 de la Ley 11/86 de Patentes.

Reivindicación 12: el documento D01 divulga un dispositivo de red configurado como nodo de acceso para escribir datos en un recurso dentro de una red RELOAD. El dispositivo de red tiene un firmante configurado para firmar los datos a escribir en el recurso utilizando una clave de escritura y un comunicador configurado para generar una petición para escribir los datos firmados en el recurso no poseído por el dispositivo de red y enviar la petición a un par responsable del recurso. Así la reivindicación 12 no presenta novedad según el art. 6.1 de la Ley 11/86 de Patentes.

Reivindicaciones 16, 17, 19 y 20: estas reivindicaciones se corresponden directamente con el dispositivo de la reivindicación 1 (dispositivo y método) y, por tanto, también tienen actividad inventiva según el art. 8.1 de la Ley 11/86 de Patentes.

Reivindicación 18: el método reivindicado se corresponde directamente con la configuración de los elementos del dispositivo de la reivindicación 12 y, por tanto, la reivindicación 18 tampoco presenta novedad según el art. 6.1 de la Ley 11/86 de Patentes.

Reivindicación 21: el medio legible por ordenador carece de novedad según el art. 6.1 de la Ley 11/86 de Patentes por corresponderse directamente con la reivindicación 18.

Reivindicaciones dependientes

Reivindicaciones 2-4, 6-11: estas reivindicaciones tienen actividad inventiva según el art. 8.1 de la Ley 11/86 de Patentes por depender de la reivindicación 1 y de la reivindicación 5 respectivamente que también la poseen.

Reivindicaciones 13-15: el contenido de estas reivindicaciones está incluido en D01. Por tanto, las reivindicaciones 13-15 carecen de novedad según el art. 6.1 de la Ley 11/86 de Patentes.