(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 685 126**

(21) Número de solicitud: 201700375

(51) Int. CI.:

H04L 9/00 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

31.03.2017

(43) Fecha de publicación de la solicitud:

05.10.2018

(71) Solicitantes:

GRUPREX S.L. (100.0%)
Ríos Rosas 36, 7º C
28003 Madrid ES

(72) Inventor/es:

ASENSIO ARROYO, Jesús Damaso

(74) Agente/Representante:

CAPITAN GARCÍA, Nuria

(54) Título: **Dispositivo de cifrado corporativo con método de refresco de claves en tiempo real y autenticación**

(57) Resumen:

Dispositivo de cifrado simétrico que permite proteger la información que reside en cualquier servidor corporativo pero que también puede actuar como un router de cifrado o como un HSM (Hardware Security Module, Módulo de Seguridad Hardware) con capacidad de calcular claves de cifrado y enviarlas a los dispositivos extremos correspondientes, independientemente de su número y mediante una técnica que no se basa en certificación X.509 o PGP. Dicho dispositivo puede conectarse a la red local donde reside el servidor a proteger pero también puede actuar en forma "standalone" conectándose a la red local y a Internet en modo router o bien en modo HSM. El dispositivo incorpora en su hardware embebido un algoritmo que lleva a cabo los cálculos necesarios para que una clave pueda ser enviada a un número ilimitado de dispositivos, conectados a Internet directa o indirectamente y cuyo refresco podemos afirmar que se lleva a cabo en tiempo real.

ES 2 685 126 A1

DESCRIPCIÓN

Dispositivo de cifrado corporativo con método de refresco de claves en tiempo real y autenticación.

Objeto de la invención

Es objeto de la presente invención, tal y como el título establece, un dispositivo de cifrado corporativo que realiza un cifrado simétrico que permite proteger la información que reside en cualquier servidor corporativo pero que también puede actuar como un router de cifrado o como un HSM (Hardware Security Module, Módulo de Seguridad Hardware) con capacidad de calcular claves de cifrado y enviarlas a los dispositivos extremos correspondientes, independientemente de su número.

Dicho dispositivo puede conectarse a la red local donde reside el servidor a proteger pero también puede actuar en forma “standalone” conectándose a la red local y a Internet en modo router o bien en modo HSM. El dispositivo incorpora en su hardware embebido un algoritmo que lleva a cabo los cálculos necesarios para que una clave pueda ser enviada a un número ilimitado de dispositivos, conectados a Internet directa o indirectamente y cuyo refresco podemos afirmar que se lleva a cabo en tiempo real.

Por lo tanto, la presente invención se circunscribe dentro del ámbito de los dispositivos de cifrado, y de manera particular de entre aquellos utilizados para proteger la información de servidores corporativos.

Antecedentes de la invención

Son conocidos distintos tipos de dispositivos de cifrado de la información en el actual estado de la técnica, casi todos ellos basados en comunicaciones entre un emisor y un receptor exclusivamente. Así pues, se conoce el documento de patente ES2245305 que describe un sistema de encriptación de clave pública que emplea un par de clave pública/clave privada así como un procedimiento y un aparato para aumentar la seguridad de la autenticación empleando un sistema de autenticación biométrico más resistente a la manipulación y que se caracteriza por generar un par clave pública/clave privada a partir de un registro biométrico, utilizando la clave privada tras la autenticación biométrica previa. En este sistema de encriptación no se contempla reivindicación sobre el proceso de encriptación en ninguna de las modalidades contempladas, comunicaciones de red extremo a extremo ni multidifusión, sino que hace mención a la fiabilidad de la clave privada, previa autenticación biométrica.

La patente ES2094135 se centra en una red de comunicaciones con distribución de claves sobre una arquitectura analógica de redes de abonado, aunque también menciona comunicaciones digitales. El sistema está formado por varios dispositivos, una unidad de cifrado que obtiene los códigos de cifrado desde una autoridad de distribución de códigos y un elemento de gestión de asignación de dichos códigos de cifrado, también haciendo mención que el módulo de gestión de asignación de códigos puede conectarse a un servidor de autenticación para gestionar una lista de certificados. En este caso, el documento no contempla un solo elemento de seguridad bien para toda una red local, bien para redes locales unidas virtualmente o, en caso necesario, a redes donde se necesita multidifusión.

La patente ES2130570 hace mención a un sistema y aparato para el cifrado/descifrado de bloques de datos. El sistema utiliza el llamado método de cadena de bloques de cifras (CBC) y cuyo dispositivo se liga a un algoritmo basado en bloques, operaciones XOR y utilización de registros de desplazamiento. En este caso, de nuevo, no se hace mención ninguna al cifrado en entornos multidifusión ni a un dispositivo especialmente concebido para cifrar

simultáneamente en ambos escenarios, unidifusión y multidifusión y que distribuye una clave simétrica a todo un grupo de usuarios de tamaño ilimitado y en un rango de tiempo dentro de los milisegundos. Tampoco hace referencia ninguna a mecanismos de protección especiales para el dispositivo tales como mecanismos antiapertura, antidesplazamiento, etc.

La patente ES2158081 hace alusión a un sistema criptográfico y método con característica de depósito de claves y más concretamente a la generación, certificación, almacenamiento y distribución segura de claves criptográficas utilizadas en sistemas criptográficos de comunicaciones y más particularmente, el documento se refiere a un sistema de gestión de depósito de claves criptográficas y de certificados de claves públicas ejecutado por un dispositivo de chip de auto-certificación. Es evidente la no relación con la invención descrita en este documento.

La patente ES2221932 se describe un aparato criptográfico con doble función de alimentación directa, es decir, se refiere a aparatos criptográficos, y más en particular a un procesador criptográfico que utiliza una doble disposición de alimentación directa para implementar un algoritmo de cifrado que tiene una propiedad complementaria, de tal modo que las inversiones a la entrada del procesador criptográfico pueden ser detectadas en la salida del mismo. Es evidente que la invención reflejada en el documento ES2221932 no se relaciona con el dispositivo y procedimiento descrito en esta invención.

En la patente ES2262210 se contempla un sistema para la transmisión segura de señales de datos, más concretamente, un sistema que comprende medios para encriptar las señales de datos utilizando una primera clave, medios para transmitir las señales de datos encriptadas a los abonados, medios para desencriptar las señales de datos encriptadas en cada uno de los abonados utilizando la primera clave, medios para encriptar la primera clave utilizando una segunda clave, siendo distinta dicha segunda clave para cada grupo de abonados que tienen un interés común en un tipo de programas, medios para transmitir la primera clave encriptada a todos los abonados, medios para desencriptar la primera clave encriptada en cada uno de los abonados utilizando la segunda clave. En este caso podemos observar que se contempla un escenario de multidifusión donde existe una segunda clave para cada grupo de abonados. Evidentemente, la eficiencia de ancho de banda de este sistema es mejor que un sistema de extremo a extremo pero la seguridad es muy baja debido a que la clave no puede ser recalculada de forma inmediata tras la adición o eliminación de miembros de cada grupo. Además, no utiliza mecanismos de autenticación como los que se utilizan en el dispositivo central de la presente patente.

La patente ES 2274557, sistema para proporcionar datos encriptados, sistema para desencriptar datos encriptados y método para proporcionar una interfaz de comunicaciones en dicho sistema desencriptador, hace mención a un sistema para proteger información para reproductores de contenido que contienen a su vez un sistema de desencriptado también contemplado en la patente. En nuestro caso, el dispositivo es un dispositivo genérico y simétrico de encriptación/desencriptación con cálculo y distribución de clave simétrica utilizado para cifrar cualquier contenido proveniente de un computador y difundirlo en un escenario de red normal o multidifusión y donde existen mecanismos de autenticación segura de los diferentes miembros del grupo.

Así pues, ninguno de los documentos localizados en el actual estado de la técnica describe un sistema como el de la invención, formado por un dispositivo de encriptación, cálculo y distribución de clave simétrica, orientado simultáneamente a entornos normales de red y multidifusión, formado por un elemento de protección antimanipulación que engloba diversos sensores de detección de apertura y traslado no autorizado, que contiene un método de análisis de la información proveniente del computador y que posee varios métodos de cifrado estándar y propios.

Por lo tanto, es objeto de la presente invención desarrollar un dispositivo de cifrado que supere los inconvenientes apuntados, desarrollando un dispositivo como el que a continuación se describe y queda recogido en su esencialidad en la reivindicación primera.

Explicación de la invención

Es un objeto de la presente invención un dispositivo de cifrado/descifrado de información a modo de HSM (Hardware Security Module, Módulo de Seguridad Hardware) que posee la capacidad de creación de claves de cifrado a un grupo de dispositivos conectados a Internet directa o indirectamente así como de un mecanismo que permite que dos dispositivos puedan autenticarse o bien, que los dispositivos puedan comprobar que el dispositivo de cifrado es realmente quién dice ser, todo ello sin mecanismos de criptografía de clave pública basados en X.509, PGP, etc.

El dispositivo de cifrado puede utilizar cualquier algoritmo de cifrado simétrico tales como AES (AdvancedEncryption Standard), IDEA (International Data EncryptionAlgorithm) (Algoritmo internacional de cifrado de datos), etc. y se presenta en formato PCI Express (PCIe) ("Entradas/Salidas de Tercera Generación", en inglés: 3rd Generation In/Out) para ser integrado en servidores de datos corporativos ya existentes o bien en formato de caja listo para conectar en la red local del servidor de datos corporativo.

En el formato PCI Express, el dispositivo cuenta con un chip capaz de llevar a cabo el cálculo de una clave de sesión que podrá enviarse a un grupo indeterminado de dispositivos. Este chip también lleva a cabo los cálculos necesarios para que los dispositivos puedan autenticarse entre sí o bien el dispositivo de cifrado pueda autenticarse ante ellos. También posee un chip exclusivamente de cifrado simétrico que generalmente se basa en AES o IDEA pero que también acepta cualquier algoritmo de cifrado simétrico propio.

En el formato de caja, standalone, el dispositivo cuenta con una placa electrónica que contiene dos conectores para Ethernet y un conector USB además los chips correspondientes de cifrado y creación de claves de sesión.

Tanto en el formato PCI Express como en el formato de caja, el dispositivo cuenta también con un acelerómetro de tres ejes que permite detectar movimiento y dirección del mismo a modo de alerta de seguridad.

El dispositivo puede funcionar en dos modos principales de operación, modo router seguro y modo cifrador de datos corporativos. En el primer caso, los datos que proceden del servidor de datos corporativo se cifran y se envían por el puerto Ethernet de salida del dispositivo a la red local o bien a Internet. Por el contrario, en modo exclusivamente de cifrado, el dispositivo cifra o descifra los datos procedentes del servidor de datos corporativo y los devuelve a éste para su almacenamiento o procesamiento correspondiente.

El dispositivo permite el control de dos direcciones IP (recordemos que el modo caja o standalone posee dos conectores Ethernet) de tal forma que obtiene la información a cifrar desde el servidor de datos corporativo y posteriormente reenviarla a través de la segunda dirección IP.

El mecanismo de creación y envío de información para distribuir claves entre los dispositivos permite llevar a cabo el refresco de claves de cifrado para cada uno de los dispositivos conectados a Internet o a una red local con un consumo mínimo de ancho de banda. Por tanto, se trata de un nuevo método donde un hardware puede llevar a cabo este mecanismo de refresco para millones de dispositivos independientemente de su poder computacional. Así, un

dispositivo de bajos recursos computacionales, podrá asegurar las comunicaciones sin necesidad de estructuras más complejas como X.509 o PGP, entre otros. Esto es especialmente válido para el entorno denominado Internet de las Cosas (IoT, Internet of Things, por su versión inglesa), donde la mayoría de los dispositivos carecen de grandes recursos computacionales.

De esta forma, se pueden también configurar subgrupos formados por un dispositivo de cifrado de estas características y por un número indeterminado de dispositivos conectados (los dispositivos pueden ser sensores, ordenadores convencionales o cualquier dispositivo para tratamiento de la información). De esta forma, los dispositivos de cifrado que controlan cada subgrupo pueden comunicarse entre sí y también con un dispositivo de cifrado central que maneja todo el entorno global en un escenario formado por un dispositivo de cifrado de las características comentadas en la presente invención y que está conectado a un número indeterminado de dispositivos, éste envía la clave de sesión, que los dispositivos del sistema reciben y, a través del cálculo matemático correspondiente de cada dispositivo, cada uno de ellos obtendrá una clave de sesión diferente de la del resto; este mecanismo es precisamente el que permite un refresco de clave a millones de dispositivos sin apenas consumo de ancho de banda. Este mecanismo permite a un grupo de dispositivos recuperar una información secreta, en tiempo real, con el envío de un solo mensaje por parte del dispositivo de cifrado específico de esta invención.

Cada dispositivo del grupo de dispositivos, de número indeterminado, puede conectarse o desconectarse de forma dinámica, en ese momento, el dispositivo de cifrado llevará a cabo el refresco de clave correspondiente.

Para el cálculo de la clave en el dispositivo de cifrado que actúa a modo de HSM y que será enviada a los dispositivos del grupo, el dispositivo de cifrado calcula al menos tres números primos grandes, denominados, g, m y p, de forma que el dispositivo de cifrado calcula, por un lado, delta tal que $\delta = k + m$, y donde k es un número entero seleccionado que fuerza a delta a ser menor que cualquiera de los x_i, (donde x_i son cada una de las claves de cada dispositivo, primos entre sí, es decir todos los x_i son primos entre sí) es decir $\delta < x_i$, para todo i = 1, ..., n.

Así pues, calcula $r = g^k mod\ p$ y $u = \delta^{-1} mod L$ con $L = \pi x$, y envía el dato u a los dispositivos del grupo. Así pues, cada miembro del grupo recibe u y calcula $u^{-1} mod\ x_n$ donde mod indica la operación módulo. Así a mod b es el resto de dividir a entre b.

δ^{-1} es el inverso del δ calculado anteriormente.

u^{-1} es el inverso de u.

Como hemos comentado anteriormente, los dispositivos pueden conectarse o desconectarse del grupo en cualquier momento, así, cuando un dispositivo se conecta al grupo, el dispositivo de cifrado procede al recalculo de una nueva clave de grupo de forma que no perjudica el rendimiento de las comunicaciones y, en tiempo real, la clave será refrescada para los dispositivos, por tanto, cuando un dispositivo se conecta al grupo, la clave se recalcula por parte del dispositivo de cifrado de forma $g^k mod\ p$ incluye la información privada de ese nuevo dispositivo en el cálculo del módulo tal que $L' = L * x_{i+1}$ donde x_{i+1} denota la información privada del nuevo dispositivo, en su lugar, cuando un dispositivo se desconecta del grupo entonces se recalcula / de la forma que $L' = L / x_{j1}$ donde x_j es la información privada del dispositivo que abandona el grupo, y a continuación se refresca con un nuevo cálculo de $g^k mod\ p$ para un nuevo valor k, tanto g como p son valores públicos que puede conocer cualquiera.

En definitiva, cada miembro del grupo recibe u y calcula $u^{-1} mod\ x_i = \delta$ ya que, $u^{-1} mod\ L = \delta \leftrightarrow u\ \delta = 1\ mod\ L \leftrightarrow u\ \delta = 1\ mod\ x_i$.

Como hemos comentado anteriormente, el dispositivo de cifrado permite a los dispositivos poder autenticarse entre sí, actuando como elemento central de confianza pero también, el dispositivo de cifrado puede identificarse ante un dispositivo.

Para que los dispositivos del grupo tengan la certeza de que el dispositivo de cifrado que está a cargo del refresco y cálculo de clave es realmente quién dice ser, se procede de la siguiente manera.

- el dispositivo que actúa a modo de HSM calcula un número aleatorio “a” y donde dicho número es menor que cualquiera de la clave privada de cada dispositivo del grupo, es decir, $a < x_i$ para todo *i* desde 1 hasta *n*.

- el dispositivo a modo de HSM calcula $s = (g^k)^{-1} \text{mod } I$ donde g^k es la clave distribuida y I es el producto de todos los x_i de los dispositivos, dato que evidentemente conoce el HSM, es decir, $I = \pi x_i$.

- calcula además un hash (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos) del número “a” obtenido y donde ese hash corresponde a una función hash segura, por ejemplo, sha-2 o similar.

- el dispositivo que actúa a modo de HSM, cuando envía el parámetro u, que es el mensaje de refresco a los dispositivos del grupo, añade la información (s*a, h(a)) que permitirá al dispositivo destino autenticar la procedencia de *u*.

De este modo, cuando el dispositivo destino recibe el mensaje (u, (s*a, h(a)), éste calcula $r = g^k \text{mod } m$ utilizando x_i, tal como hemos visto anteriormente, además, lleva a cabo el cálculo de s utilizando su número privado x_i y obtiene finalmente h(a) comparando ese h(a) con el que envió el dispositivo de cifrado, si ambos son iguales, se produce la autenticación con éxito.

En el caso de que un dispositivo *i* quiere autenticar a un dispositivo *j* del grupo, el dispositivo hace uso del protocolo que se indica a continuación, el dispositivo *i*, poseedor de x_i, quiere autenticar al dispositivo *i*, poseedor de x_t. para ello, el dispositivo *i* elige *t* al azar tal que $1 < t < m$ y lo envía al dispositivo de cifrado que actúa como elemento central de confianza, el dispositivo de cifrado calcula $inv = t^{-1} \text{mod } I$ y se lo devuelve al dispositivo *i*, el dispositivo *i* envía al dispositivo *j*, $(inv, g^{xi} \text{mod } m)$, por lo que el dispositivo *j* calcula $t_j = inv^{-1} \text{mod} x_i$ y $\beta_i = t_j * (g_{xi})^{xj} \text{ mod } m$, información que envía al dispositivo *i*, (β_j, g_{xj}), finalmente, el dispositivo i calcula $\beta_i = t(g^{xj})^{xi} \text{ mod } m = t*g^{xjxi} \text{ mod } m$ por lo que el dispositivo *i* autentica positivamente a *j* siempre y cuando se cumpla que $\beta_i = \beta_j$.

Podemos observar que este tipo de dispositivo que actúa a modo de dispositivo de cifrado es idóneo para llevar a cabo la securización dinámica de cualquier plataforma del internet de las cosas o cualquier entorno formado por un gran número de dispositivos, en tiempo real y con un consumo de ancho de banda mínimo.

Salvo que se indique lo contrario, todos los elementos técnicos y científicos usados en la presente memoria poseen el significado que habitualmente entiende un experto normal en la técnica a la que pertenece esta invención, en la práctica de la presente invención se pueden usar procedimientos y materiales similares o equivalentes a los descritos en la memoria.

A lo largo de la descripción y de las reivindicaciones la palabra “comprende” y sus variantes no pretenden excluir otras características técnicas, aditivos, componentes o pasos para los expertos en la materia, otros objetos, ventajas y características de la invención se desprenderán en parte de la descripción y en parte de la práctica de la invención.

Breve descripción de los dibujos

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente.

La figura 1 muestra los distintos componentes del dispositivo en formato caja.

La figura 2 muestra un esquema del sistema global en una comunicación con múltiples grupos de dispositivos.

La figura 3 muestra un esquema del sistema global en un entorno de red local.

Realización preferente de la invención

A la vista de las figuras se describe seguidamente un modo de realización preferente de la invención propuesta.

El dispositivo de cifrado comprende un microcontrolador central (1) y un chip o FPGA (2) (Field ProgrammableGateArray) que es un dispositivo programadle conectado con el microcontrolador central, donde el microcontrolador central (1) cuenta con los medios necesarios para:

- Llevar a cabo el cálculo de una clave de sesión que podrá enviarse a un grupo indeterminado de dispositivos.

- Llevar a cabo los cálculos necesarios para que los dispositivos puedan autenticarse entre sí o bien el dispositivo de cifrado pueda autenticarse ante ellos.

Mientras que el FPGA (2) es un dispositivo programadle de cifrado simétrico que permite bien un algoritmo de cifrado simétrico propio o bien un algoritmo tipo AES o IDEA.

También comprende unos medios de protección (3) basados en un acelerómetro de tres ejes que permite detectar movimiento y dirección del mismo a modo de alerta de seguridad.

Quedando todos los anteriores elementos protegidos en una protección metálica (4).

La realización hasta ahora descrita se corresponde con un PCI para ser integrado en servidores de datos corporativos ya existentes.

En la figura 1, que se corresponde con el formato caja, el dispositivo de cifrado cuenta con una placa electrónica que contiene dos conectores para Ethernet (E1) y (E2) y un conector USB (5) además los chips correspondientes de cifrado y creación de claves de sesión.

En la figura 2 podemos observar este dispositivo de cifrado (6) dentro de un entorno de comunicación y donde el dispositivo de cifrado (6) lleva a cabo la infraestructura de refresco de clave y autenticación el grupo de dispositivos a los que está conectado.

El dispositivo de cifrado (6) objeto de la invención se interpone entre la red Internet (9) y los dispositivos finales (7) (terminales de TV, contadores de luz o cualquier dispositivo que requiera una clave para su funcionamiento) sirviendo como dispositivo que controla el refresco de claves y autenticación ante su grupo de dispositivos.

El dispositivo de cifrado (6) también puede disponerse entre la red de Internet (9) y un servidor corporativo (8) actuando como dispositivo global encargado del refresco y autenticación con los demás dispositivos de cifrado.

En la figura 3 se muestra el dispositivo de cifrado (6) objeto de la invención en un entorno de red local (12), donde desde el dispositivo de cifrado (6) se envían mensajes (11) de refresco y de autenticación hacia los dispositivos finales (7), que pueden ser dispositivos de bajo poder computacional, o bien hacia unos ordenadores (10).

Descrita suficientemente la naturaleza de la presente invención, así como la manera de ponerla en práctica, se hace constar que, dentro de su esencialidad, podrá ser llevada a la práctica en otras formas de realización que difieran en detalle de la indicada a título de ejemplo, y a las cuales alcanzará igualmente la protección que se recaba, siempre que no altere, cambie o modifique su principio fundamental.

REIVINDICACIONES

1. Dispositivo de cifrado corporativo caracterizado porque comprende:

- Un microcontrolador central (1).

- Un chip o FPGA (2) (Field ProgrammableGateArray) dispositivo programable conectado con el microcontrolador central (1).

- Unos medios de protección (3) basados en un acelerómetro de tres ejes que permite detectar movimiento y dirección del mismo a modo de alerta de seguridad.

Donde el microcontrolador central (1) cuenta con los medios necesarios para:

- llevar a cabo el cálculo de una clave de sesión que podrá enviarse a un grupo indeterminado de dispositivos.

- llevar a cabo los cálculos necesarios para que los dispositivos puedan autenticarse entre sí o bien el dispositivo de cifrado pueda autenticarse ante ellos mientras que el FPGA (2) es un dispositivo programable de cifrado simétrico que permite bien un algoritmo de cifrado simétrico propio o bien un algoritmo tipo AES o IDEA.

2. Dispositivo de cifrado corporativo según la reivindicación 1 caracterizado por que en caso de presentar un formato caja además comprende una placa electrónica que contiene dos conectores para Ethernet (E1) y (E2) y un conector USB (5).

3. Procedimiento de refresco de claves realizado en el dispositivo de cifrado según cualquiera de las reivindicaciones anteriores caracterizado porque la nueva clave se realiza mediante el cálculo de al menos tres números primos grandes, denominados, g, m y p, de forma que el dispositivo de cifrado calcula, por un lado, delta tal que $\delta = k + m$, y donde k es un número entero seleccionado que fuerza a delta a ser menor que cualquiera de los x_i, (donde x_i son cada una de las claves de cada dispositivo primos entre sí, es decir, todos los x_i son primos entre sí), es decir $\delta < x_i$, para todo i = 1, ... n; así pues, calcula $r = g^k \bmod p$ y $u = \delta^{-1} \bmod L$ con $L = \pi x_i$ y envía el dato u a los dispositivos del grupo, así pues, cada miembro del grupo recibe u y calcula $u^{-1} \bmod x_i$, donde mod indica la operación módulo.

δ^{-1} es el inverso del δ calculado anteriormente

u^{-1} es el inverso de u

4. Procedimiento de refresco de claves según la reivindicación 3 caracterizado porque cuando un nuevo dispositivo se incorpora al grupo en el cálculo de $r = g^k \bmod p$ se incluye la información privada de ese nuevo dispositivo en el cálculo del módulo tal que $L' = L * x_i+1$ donde x_i+1 denota la información privada del nuevo dispositivo; en su lugar, cuando un dispositivo se desconecta del grupo entonces se recalcula L de la forma que $L' = L / x_j$, donde x; es la información privada del dispositivo que abandona el grupo; y a continuación se refresca con un nuevo cálculo de $g^k \bmod p$ para un nuevo valor k; tanto g como p son valores públicos que puede conocer cualquiera.

5. Procedimiento de autenticación entre dispositivos y el dispositivo de cifrado según cualquiera de las reivindicaciones 1 a 2 caracterizado porque el proceso comprende las etapas de:

- El dispositivo que actúa a modo de HSM calcula un número aleatorio “a” y donde dicho número es menor que cualquiera de la clave privada de cada dispositivo del grupo, es decir, $a<x_i$ para todo *i* desde 1 hasta n.

- El dispositivo a modo de HSM calcula $s = (gk)^{-1} \bmod L$ donde g^k es la clave distribuida y L es el producto de todos los x_i de los dispositivos, dato que evidentemente conoce el HSM, es decir, $L = \Pi x_i$.

- Calcula además un hash (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos) del número “a” obtenido y donde ese hash corresponde a una función hash segura, por ejemplo, SHA-2 o similar.

- El dispositivo que actúa a modo de HSM, cuando envía el parámetro u, que es el mensaje de refresco a los dispositivos del grupo, añade la información (s*a, h(a)) que permitirá al dispositivo destino autenticar la procedencia de u.

De este modo, cuando el dispositivo destino recibe el mensaje (u, (s*a, h(a)), éste calcula $r = g^k \bmod m$ utilizando x, tal como hemos visto anteriormente. Además, lleva a cabo el cálculo de s utilizando su número privado x_i y obtiene finalmente h(a) comparando ese h(a) con el que envió el dispositivo de cifrado si ambos son iguales, se produce la autenticación con éxito.

6. Procedimiento de autenticación entre un dispositivo i quiere autenticar a un dispositivo j del grupo empleando el dispositivo de cifrado según cualquiera de las reivindicaciones 1 a 2 caracterizado por que el dispositivo i elige t al azar tal que $1 < t < m$ y lo envía al dispositivo de cifrado (6) que actúa como elemento central de confianza; el dispositivo de cifrado (6) calcula $inv = t^{-1} \bmod L$ y se lo devuelve al dispositivo *i*; el dispositivo *i* envía al dispositivo *j*, $(inv, g^{xj} \bmod m)$, por lo que el dispositivo i $calculat_j = inv^{-1} \bmod x_j y$ $(\beta_j = t_j * (g_{xi})x_j \bmod m$, información que envía al dispositivo i, $(\beta_j\ g_{xj})$;finalmente, el dispositivo i $calcula\beta_i = t(g_{xj})^{xj} \bmod m = t*g^{xjxi} \bmod m$ por lo que el dispositivo i autentica positivamente a j siempre y cuando se cumpla que $\beta_¡ = \beta j$.

7. Uso del dispositivo de cifrado según cualquiera de las reivindicaciones 1 a 2 caracterizado porque se interpone entre una red de Internet (9) y unos dispositivos finales (7) sirviendo como dispositivo que controla el refresco de claves y autenticación ante su grupo de dispositivos, también puede usarse entre la red de Internet (9) y un servidor corporativo (8) actuando como dispositivo global encargado del refresco y autenticación con los demás dispositivos de cifrado.

8. Uso del dispositivo de cifrado según cualquiera de las reivindicaciones 1 a 2 caracterizado porque el dispositivo de cifrado (6) se usa en un entorno de red local (12), donde desde el dispositivo de cifrado (6) se envían mensajes (11) de refresco y de autenticación hacia los dispositivos finales (7), que pueden ser dispositivos de bajo poder computacional, o bien hacia unos ordenadores (10).

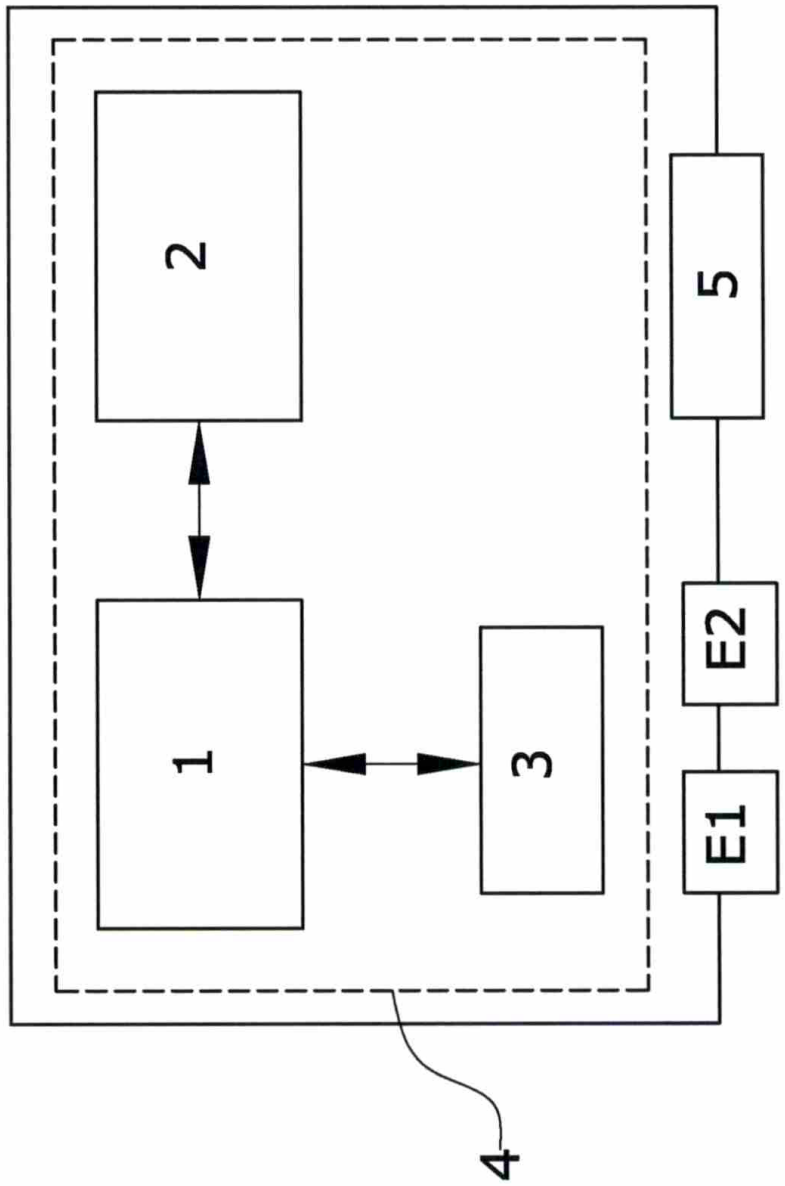

FIG.1

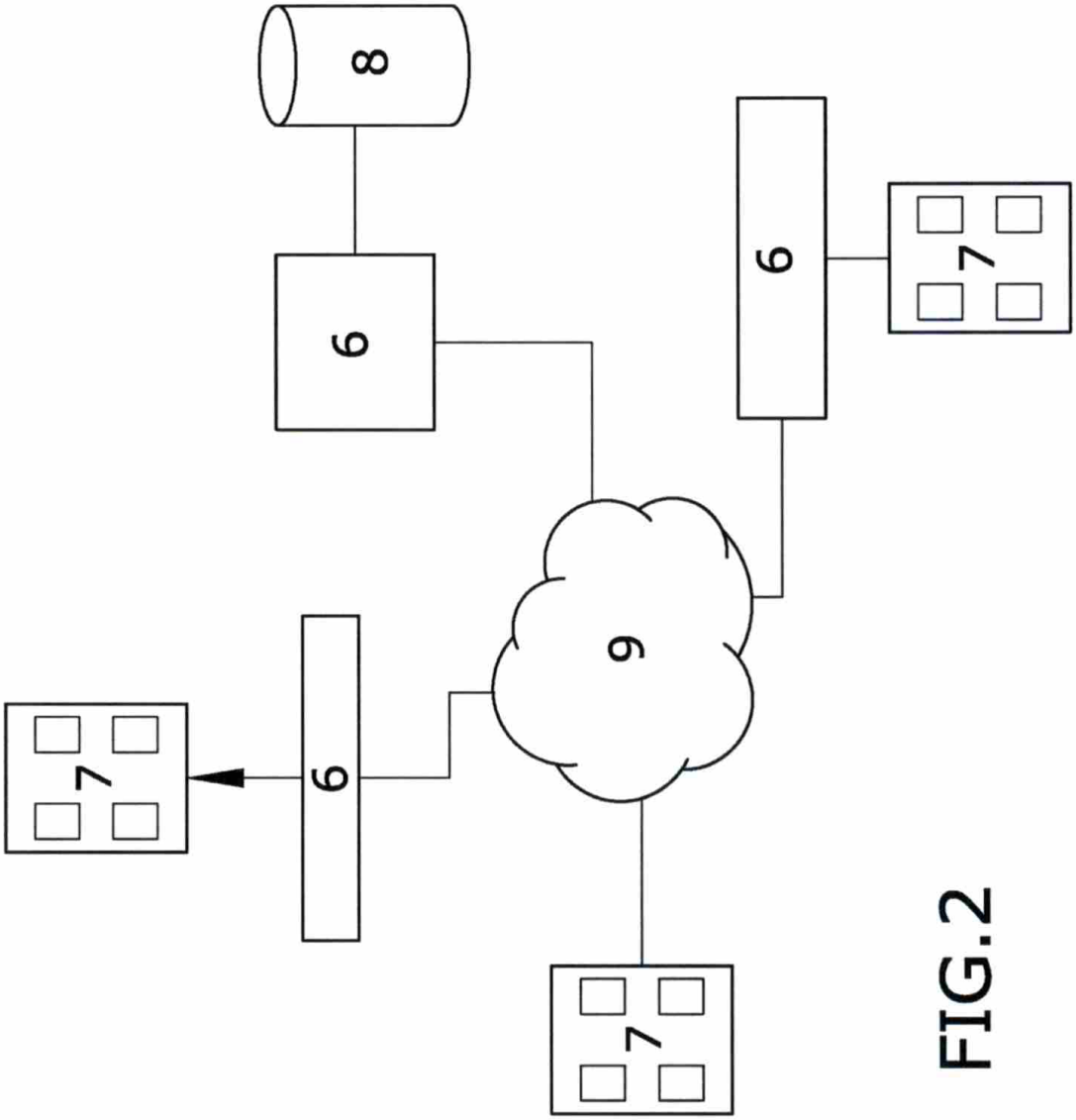

FIG.2

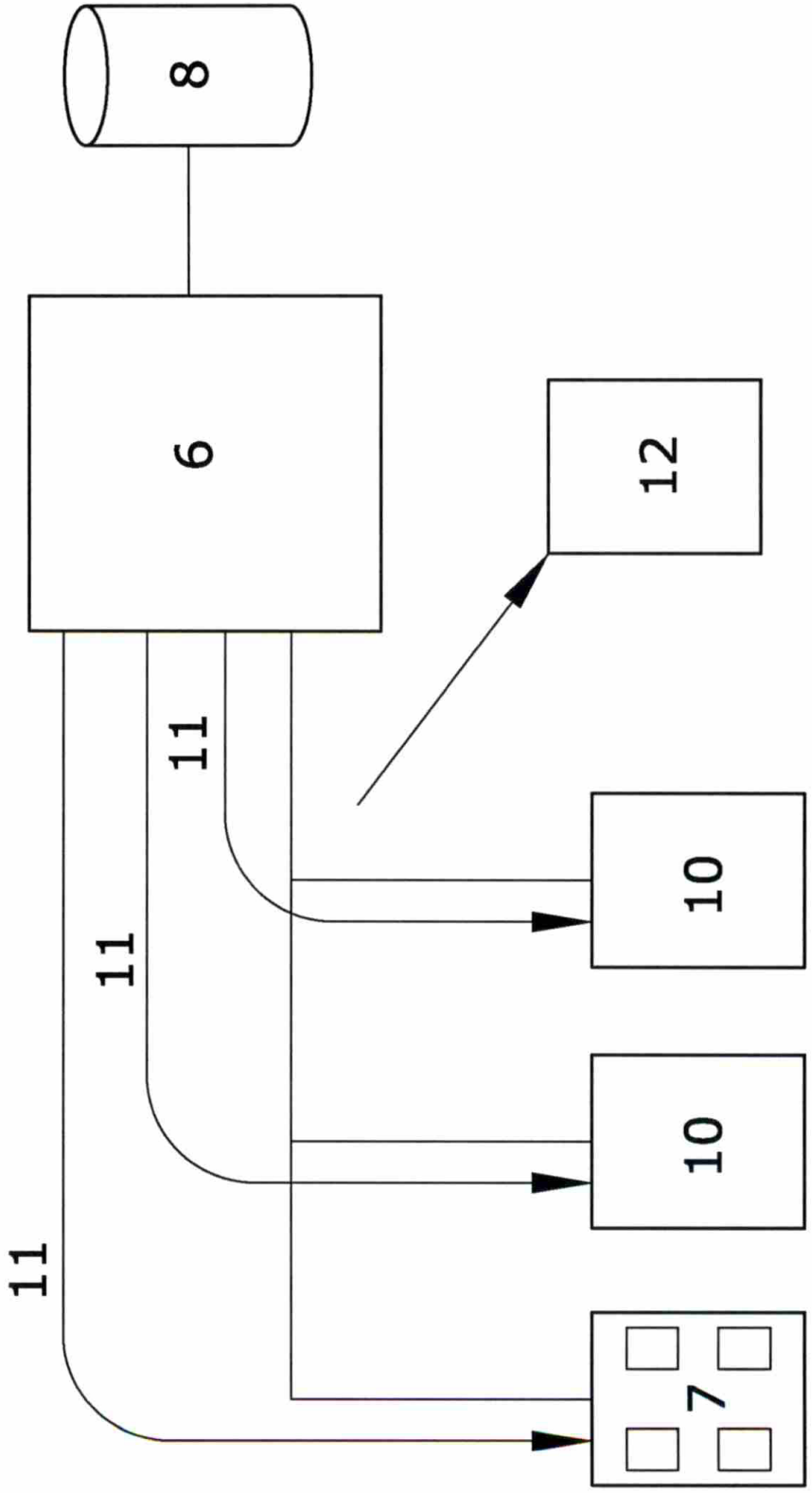

FIG.3

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201700375

(22) Fecha de presentación de la solicitud: 31.03.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/00*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	ES 2523423 A2 (CRYPTO SOLUTIONS S L) 25/11/2014, Reivindicaciones.	1-8
A	US 4229817 A (MORGAN BARRIE O et al.) 21/10/1980, Todo el documento.	1-8
A	US 2009133610 A1 (BAKER DAVID L) 28/05/2009, Todo el documento.	1-8

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**
01.08.2018	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: 01.08.2018

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-2, 7-8	**SI**
	Reivindicaciones	3-6	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-2, 7-8	**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	ES 2523423 A2 (CRYPTO SOLUTIONS S L)	25.11.2014
D02	US 4229817 A (MORGAN BARRIE O et al.)	21.10.1980
D03	US 2009133610 A1 (BAKER DAVID L)	28.05.2009

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 cifrado simétrico de protección de la información entre un grupo ilimitado de usuarios. El dispositivo comprende un microprocesador, conectores Ethernet, un conector USB y un acelerómetro. El dispositivo del documento D01 incluye además un algoritmo de autenticación entre los usuarios (sus dispositivos) y entre dispositivos de usuarios y el dispositivo de cifrado. Además, el documento incluye un algoritmo de refresco de claves.
La diferencia entre la reivindicación 1 y el documento D01, se refiere a la implementación de la lógica de cifrado, en el caso de la solicitud, microcontrolador con FPGA. Esta diferencia es meramente una alternativa común en el campo técnico de la solicitud y, por tanto, evidente para el experto en la materia.
Por tanto, el documento D01 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley 24/2015 de Patentes.
Reivindicación 3: el algoritmo de refresco de claves está incluido en el documento D01.
Reivindicación 5: el algoritmo de autenticación entre un dispositivo de usuario y el dispositivo de cifrado está incluido en el documento D01.
Reivindicación 6: el algoritmo de autenticación entre dispositivos de usuarios está incluido en el documento D01.
Reivindicación 7: el uso reivindicado es propio (el específico para el que se concibe) del dispositivo de cifrado del documento D01.
Reivindicación 8: el uso reivindicado es propio (el específico para el que se concibe) del dispositivo de cifrado del documento D01.
Así, el documento D01 afecta a la novedad de las reivindicaciones 3, 5, y 6 y a la actividad inventiva de las reivindicaciones 7 y 8 según los arts. 6.1 y 8.1, respectivamente, de la Ley 24/2015 de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2, 4: el contenido de estas reivindicaciones forma parte del documento D01.
Por tanto, el documento D01 afecta a la actividad inventiva de la reivindicación 2 y a la novedad de la reivindicación 4 según los arts. 8.1 y 6.1, respectivamente, de la Ley 24/2015 de Patentes.