(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 631 828**

(21) Número de solicitud: 201630949

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

12.07.2016

(43) Fecha de publicación de la solicitud:

05.09.2017

(71) Solicitantes:

DIAZ BAÑO, Álvaro (50.0%)
GRAN VIA DE LES CORTS CATALANES, 996, 4º 2ª
08018 BARCELONA ES y
DÍAZ BAÑO , Pablo (50.0%)

(72) Inventor/es:

DIAZ BAÑO, Álvaro y
DÍAZ BAÑO , Pablo

(54) Título: **MÉTODO PARA INCLUIR DOCUMENTOS ELECTRÓNICOS EN LOS FICHEROS ELETRÓNICOS QUE CONTIENEN CERTIFICADOS X.509**

(57) Resumen:

Método para incluir documentos electrónicos en los ficheros electrónicos que contienen certificados x.509. Se dispone de un documento electrónico (1) del que se obtiene el hash (15); antes de ser emitido el certificado x.509 (11), se incluye el hash (15) en una extensión (16) cuyo identificador ha sido definido específicamente para ese fin; una vez emitido, el fichero electrónico (10) que contiene los bytes del certificado x.509 (11) se edita y se localizan los separadores (12) que determinan el inicio y final de los bytes del certificado x.509 (11), antes del separador de inicio de los bytes o después del separador de final de esos bytes; se introduce el documento electrónico (1).

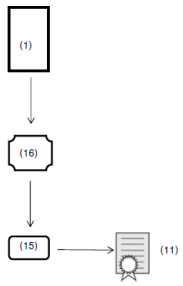

Figura 1

ES 2 631 828 A1

D E S C R I P C I Ó N

MÉTODO PARA INCLUIR DOCUMENTOS ELECTRÓNICOS EN LOS FICHEROS ELETRÓNICOS QUE CONTIENEN CERTIFICADOS X.509

SECTOR DE LA TÉCNICA

La presente invención pertenece al sector de la seguridad informática.

El objeto principal de la presente invención se refiere a un nuevo método que hace posible introducir los bytes de documentos electrónicos, en certificados que han sido emitidos en conformidad con el estándard UIT-T x.509, manteniendo su funcionalidad e interoperabilidad técnica, garantizando la integridad del documento electrónico y responsabilizando de su inclusión al emisor del certificado.

ANTECEDENTES DE LA INVENCIÓN

La versión 3 del estándar x.509 permite que una entidad emisora de certificados defina libremente sus propios campos de extensiones privados, y que introduzca en ellos cualquier tipo de información, sin límite de tamaño o tipo de datos. Incluir documentos en los ficheros electrónicos que contienen certificados x.509 tiene una gran utilidad. Por ejemplo: la mayor parte de apoderamientos son limitados, por lo tanto, determinar el alcance de un poder solo es posible si se realiza un bastanteo y para ello es necesario todo el poder. Pese al alto interés de incluir documentos, esta opción no se lleva a cabo porque los procedimientos conocidos hasta la fecha tienen diversas limitaciones que esta invención resuelve definitivamente. Las principales limitaciones son:

1- De forma definitiva, si se incluyen documentos en las extensiones del certificado, el tamaño del certificado x.509 v3 aumenta considerablemente, esto ocasiona importantes trastornos funcionales, por ejemplo al tener que ser transmitidos para autenticación de las comunicaciones, o en sistemas de gestión de certificados en Cloud.
2- La clave privada y el certificado x.509 están íntimamente asociados, cuando la clase privada y su certificado x.509 están alojados en un procesador

criptográfico (HSM), el tamaño del certificado queda directamente condicionado a la memoria disponible de ese procesador, por lo tanto, según el tamaño del documento a incluir, puede resultar materialmente imposible.

Se ha realizado un amplio estudio sobre las patentes existentes,y ninguna de ellas describe los métodos reivindicados en esta invención. Concretamente:

La publicación “Moderne Verfahren der Kryptographie” (“Procedimientos modernos de criptografía”) Beutelspacher, Schwenk, Wolfenstetter, 3. Edición, 1999, Vieweg Verlag, contiene una descripción detallada de los procedimientos criptográficos de clave pública.

El sistema criptográfico RSA que se describe en la Patente de EE.UU. Nº 4.405.829 concedida a Rivest y otros describe un ejemplo de metodología de un sistema criptográfico de clave pública.

La publicación de la Unión Internacional de las Telecomunicaciones UIT en su publicación RFC 5280, especifica y describe de forma pormenorizada los certificados x.509 versión 3.

EXPLICACIÓN DE LA INVENCIÓN

Con el fin de alcanzar el objetivo y evitar los inconvenientes mencionados en el apartado anterior, esta invención desarrolla los siguientes procedimientos:

1. Previo a la emisión del certificado x.509 se procede a definir la extensión que contendrá el hash del documento electrónico que se desea incluir. Cabe reseñar que no existe ninguna limitación en cuanto al número de extensiones y, tampoco existe límite en el número de documentos a incluir.
2. El documento electrónico se procesa con un algoritmo de digestión para obtener su hash, el hash se incluye en la extensión definida a tal efecto..El hash tendrá garantizada su propia integridad al quedar firmado electrónicamente por el emisor del certificado x.509; otra cualidad de este procedimiento es que el hash siempre tiene el mismo tamaño, independientemente del tamaño de los datos de los que se obtiene, por lo

tanto, el tamaño de documento no está condicionado por el tamaño de la memoria del módulo de seguridad hardware (HSM que ensambla un microprocesador criptográfico).

3. Una vez que el certificado x.509 ha sido emitido, para incluir el documento electrónico se edita el fichero electrónico que contiene los bytes del certificado x.509; se determina, según tipo de codificación, cuales son los separadores de inicio y fin de contenido de los bytes del certificado x.509; el documento electrónico se introduce antes del separador de inicio, o después del separador de final de contenido. Mediante este procedimiento el certificado x.509 puede alternar la inclusión o extracción de los documentos electrónicos según conveniencia, y sin que ello afecta a su integridad o interoperabilidad técnica.

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, se acompaña como parte integrante de dicha descripción un dibujo, en el que se ha representado lo siguiente:

Figura 1 Diagrama en el que se aplica un algoritmo de digestión sobre un documento electrónico, obteniendo el hash, y anota ese hash en una extensión propietaria del certificado x.509.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

Una realización preferente del método aquí descrito, comprende esencialmente, los siguientes elementos:

a) Un documento electrónico (1) que es una copia de un Poder Notarial en formato pdf, cuyo tamaño es de 756 Kb.
b) Un token HSM (2) que ensambla un microprocesador criptográfico de la marca ST Microelectronics que dispone de memoria de 64 Kb., este microprocesador tiene la capacidad de generar claves públicas, firmar certificados de petición según estándar PKCS#10, y almacenar la clave privada y el certificado x.509 que contiene la clave pública en codificación DER (5); y una memoria no volátil (18) Nand Flash de 16 Gb.

c) Un criptosistema (3) con capacidad para: interoperar con la API PKCS#11 del token HSM; generar un certificado de petición (4) según estándar PKCS#10; recoger del emisor el certificado x.509 v3 codificado en DER (5) una vez emitido, y cargarlo en la memoria del token HSM (2). Se ha seleccionado el criptosistema Bouncy Castle, que permite interoperar con programas Java y que ofrece una amplia colección de API's que contiene los algoritmos y los procesos criptográficos requeridos por este método, incluida la capacidad para hacer llamadas según el estándar PKCS#11, y procesado del documento electrónico (1) mediante algoritmo de digestión (19) que permite obtener su hash (15).

d) Lógica informática (6) programada en java, que dispone de un interfaz de usuario que permite cumplimentar un formulario de datos que serán incluidos en el certificado electrónico, este formulario tiene asociados los OID de las extensiones, comunes y propietarias, en la que cada información será introducida en el certificado de petición (4), se ha seleccionado el OID 1.3.6.1.4.1.18332.10.10 (según el estándar ITU-T Rec. X.660 y el estándar ISO/IEC 9834-1:2005)para identificar la extensión propietaria (16) que contendrá el hash (15) del documento electrónico (1); integra el protocolo de comunicaciones con la entidad emisora de certificados (17) para enviar y descargar certificados; localizar y seleccionar el documento electrónico que desea incorporar al certificado electrónico; cuenta con la capacidad de operar con el criptosistema; además se ha dotado de la capacidad para realizar conversión de formatos de codificación de certificados x.509 V3, para esta realización preferente se ha dotado de la capacidad de realizar conversión y codificación DER (Distinguished Encoding Rules)a CER (Canonical encoding rules) (7) obteniendo un fichero electrónico (10) que contiene los bytes del certificado x.509 v3 codificado CER (11) que incluye separadores (12) de inicio y final -----BEGIN CERTIFICATE----- (13) y -----END CERTIFICATE----- (14) respectivamente; permite editar el fichero electrónico (10) localizar alguno de los separadores (12) e introducir, antes de la etiqueta de inicio o después de la etiqueta final, el documento electrónico (1). Todas estas operaciones están ampliamente documentadas en internet, y no presuponen un reto relevante para un programador de java.

e) Entidad emisora de certificados x.509 version 3, se ha elegido ANF Autoridad de Certificación (ANF AC) que tiene el identificador 18332 otorgado por la organización internacional IANA. ANF AC ha determinado el OID 1.3.6.1.4.1.18332.10.10como identificador de la extensión (16) que contendrá el

hash del documento electrónico.

Se realiza el siguiente procedimiento:

1. Mediante la lógica informática (6) se solicita al criptosistema (3) la generación de un par de claves públicas en el token HSM (2); se cumplimenta el formulario con los datos que se desea incluir en el certificado x.509 v3 (5); y se selecciona el documento electrónico (1) que se desea incorporar al certificado (5), el cual es cargado en la memora no volátil (18) del token HSM (2).
2. La lógica informática (6) realiza las llamadas necesarias al criptosistema (3) para obtener el hash (15) del documento electrónico (1), el hash (15) lo asocia a la extensión (16) del certificado y, con el resto de la información introducida en el formulario, que está asociada a sus respectivas extensiones, se genera un certificado de petición (4) según estándar PKS#10. NOTA ACLARATORIA: si la entidad emisora (17) elabora directamente los certificados x.509 v3 (5), no es necesaria la generación del certificado de petición (4), en ese caso, es la entidad emisora (17) la que introduce el hash (15) y la extensión (16).
3. La lógica informática (6) transmite el certificado de petición (4) a la entidad emisora (17) para su firma y emisión; la entidad emisora emite un certificado x.509 v3 codificado en DER (5).
4. La lógica informática (6) descarga el certificado x.509 v3 (5) y lo introduce en el microprocesador criptográfico del token HSM (2), y deja una copia del certificado (5) en la memoria no volátil (18) del token HSM (2).
5. La lógica informática (6) realiza una conversión de código del certificado x.509 v3 codificado DER (5) obteniendo fichero electrónico (10) que contiene los bytes del certificado x.509 v3 codificado CER (11).
6. La lógica informática edita el fichero electrónico(10) que contiene los bytes del certificado x.509 v3 codificado CER (11), y localiza el separador final -----END CERTIFICATE----- (14), después de ese separador introduce el documento electrónico (1) obteniendo un nuevo fichero electrónico (20), que contiene los bytes del certificado x.509 v3 (11) y los bytes del documento electrónico (1).

REIVINDICACIONES

1.- Método para incluir documentos electrónicos en los ficheros electrónicos que contienen certificados x.509 caracterizado porque comprende:

Paso 1: Con carácter previo a la emisión del certificado x.509 (11), se obtiene el hash (15) del documento electrónico (1) que se desea incluir, y se introduce ese hash (15) en extensión (16) del certificado electrónico x.509 (11). .

Paso 2: El certificado x.509 (11) es emitido incluyendo la extensión (16) que contiene el hash (15).

Paso 3: El fichero electrónico (10) que contiene los bytes del certificado x.509(11) es editado, el documento electrónico (1) es introducido antes del separador que determina el inicio de los bytes del certificado x.509 (11),o después del separador que determina el final de esos bytes.

2.- Método según Reivindicación 1, caracterizado porque el Paso 3 comprende además:
Una conversión de la codificación del certificado x.509 (5) a una codificación DER o CER (7), obteniendo un certificado x.509 (11) que tiene separadores (12) que delimitan el inicio de los bytes del certificado x.509 (11). Garantizando mediante este procedimiento que todos los certificados x.509, independientemente de la codificación en que han sido emitidos, pueden incluir un documento electrónico (1).

3.- Método según Reivindicación 1, caracterizado porque el Paso 3 comprende además:

Una codificación del documento electrónico (1) a Base 64, introduciendo el documento electrónico (1) así codificado en el fichero electrónico (10).

4.- Método según Reivindicación 1, caracterizado porque el Paso 1 se sustituye por a) y el Paso 3 se sustituye por b):

a) Con carácter previo a la emisión del certificado x.509 (11), al procesar varios documentos (1) se obtiene un hash (15) de cada documento electrónico (1) que se desea incluir, y se definen extensiones (16) específicas para cada hash (16), cargando cada hash (15) a su respectiva extensión.

b) El fichero electrónico (10) que contiene los bytes del certificado x.509 v3 (11) es editado, cada documento electrónico (1) que se va a incluir es etiquetado con el identificado de su respectiva extensión (16), y son introducidos antes del separador que determina el inicio de los bytes del certificado x.509 (11) o después del separador que determina el final de esos bytes.

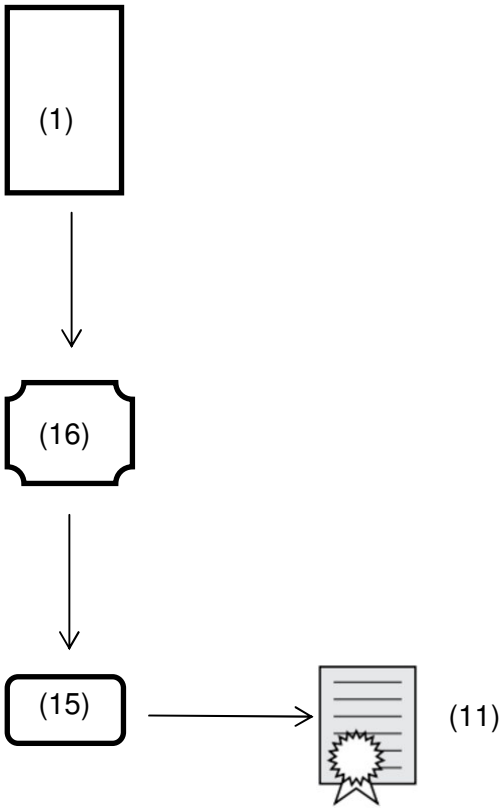

Figura 1

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201630949

(22) Fecha de presentación de la solicitud: 12.07.2016

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06F21/00*** (2013.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	CN 101931537 A (BEIJING CERTIFICATE AUTHORITY) 29/12/2010, Resúmenes EPODOC, WPI	1-4
A	JP 2003296742 A (RICOH KK et al.) 17/10/2003, Resumen EPODOC	1-4
A	CA 2203779 A1 (SURETY TECHNOLOGIES INC) 09/05/1996, Todo el documento.	1-4
A	EP 0940945 A2 (AT & T CORP) 08/09/1999, Todo el documento.	1-4
A	US 2005114666 A1 (SUDIA FRANK W) 26/05/2005, Todo el documento.	1-4

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**
24.08.2017	M. Muñoz Sanchez	1/4

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

H04L, G06F

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: 24.08.2017

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-4	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-4	**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	CN 101931537 A (BEIJING CERTIFICATE AUTHORITY)	29.12.2010
D02	JP 2003296742 A (RICOH KK et al.)	17.10.2003
D03	CA 2203779 A1 (SURETY TECHNOLOGIES INC)	09.05.1996
D04	EP 0940945 A2 (AT & T CORP)	08.09.1999
D05	US 2005114666 A1 (SUDIA FRANK W)	26.05.2005

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 describe un método para, utilizando una extensión de un certificado X.509, insertar en él un valor hash de un documento. El certificado posteriormente se firma e incluye otra información adicional (resúmenes de EPODOC y WPI, recuperados de EPOQUE). Aunque en el documento D01 no se incluya el paso de "concatenación" de certificado y documento obteniéndose un nuevo archivo, esta operación se considera asimilable a la habitual de inclusión de hash en documentos que permitan su verificación e implícitamente se podría incluso interpretar que está divulgada también en D01. Ilustrativamente, por ejemplo, en el documento D02 se menciona esta "concatenación" (*attaches the generated electronic certificate to the electronic document*; resumen EPODOC).
Por tanto, el documento D01 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley 11/86 de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2-4: las distintas conversiones de formato indicadas en estas reivindicaciones son las conocidas en los estándares. La repetición de secuencias operaciones (múltiples documentos →múltiples hashes→ múltiples extensiones) no posee un efecto técnico adicional con respecto a una única secuencia de operaciones y, por tanto, se considera una generalización evidente para el experto en la materia.
El etiquetado de archivos con su hash (hash como identificador), es una alternativa habitual y, por tanto, resulta también evidente. En particular, aparece mencionado en el documento D03 (*a name may be chosen so that it functionally depends on the document it names" an example of a "naming scheme is one that assigns to any document its hash value*).
En conclusión, el documento D01 también afecta a la actividad inventiva de las reivindicaciones 2-4 según el art. 8.1 de la Ley 11/86 de Patentes.