Generación de certificados de registro basados en firmas agregadas

Generation of copyright certificates based on aggregate signatures

Kyrna M. Quintanilla Machado1, María de Lourdes López García2
1Vicerrectoría de Estudios de Postgrados, Universidad Don Bosco,
Final Av. Albert Einstein No. 233, Col. Jardines de Guadalupe, Antiguo Cuscatlán, La Libertad, El Salvador,
(sin apartado postal)
1,2CU-UAEM Valle de Chalco, Universidad Autónoma del Estado de México,
Hermenegildo Galeana No.3, Col. María Isabel Valle de Chalco, Estado de México, México, C.P. 56615
kyrna.quintanilla@gmail.com,
Autor de correspondencia: mllopezg@uaemex.mx

PALABRAS CLAVE:

Trabajo, Eficiencia, Ciclo, Brayton, Regenerador, Recalentador.

RESUMEN

La propiedad intelectual es un derecho de los autores para registrar sus creaciones artísticas. Tal derecho se obtiene con la generación de un certificado de registro que es avalado por tres entidades: Registrador, Secretario y Registrador Jefe. El procedimiento se realiza de forma manual, por lo cual es un proceso poco eficiente y presenta diversos problemas de seguridad como falsificaciones o firmas no autorizadas.
En este trabajo es propuesto un protocolo seguro basado en firmas agregadas para la generación de un certificado de registro de una propiedad intelectual. El objetivo es producir un certificado que asegure que la firma de cada autoridad sea generada de acuerdo a una jerarquía. De tal manera que la autoridad de más alto rango pueda comprobar la validez de las firmas de las autoridades subordinadas, permitiendo un valor agregado a la certeza jurídica de los servicios ofrecidos por las oficinas de Propiedad Intelectual, así como, para los autores de las obras registradas.

KEYWORDS:

Work, Efficiency, Cycle, Brayton, Reheat, Regenerator.

ABSTRACT

Intellectual property is the right of the creators to register their artistic works. A right is obtained by generating a certificate of registration which is approved by three authorities: Registrar, Secretary, and Chief registrar. The process is done manually. Therefore, it is an inefficient and presents several bugs of security, such as fakes or unauthorized signatures.
In this work, a secure protocol based on aggregate signatures for generating a certificate of registration of intellectual property is proposed. The goal is to produce a certificate to ensure the signature of each authority is generated according to a hierarchy. Such that, the authority from highest level can prove the validity of the signatures of the lower-level authorities, allowing the added valued to the proper legal form of services offered by Intellectual Property offices, as well as to the creators of the registered works.

Recibido: 4 de septiembre de 2015 • Aceptado: 9 de abril de 2016 • Publicado en línea: 9 de junio de 2016

1 INTRODUCCIÓN

La Propiedad Intelectual, según la definición de la Organización Mundial de la Propiedad Intelectual, es toda creación del intelecto humano [1]. Los derechos de la propiedad intelectual protegen los intereses de los creadores al ofrecerles prerrogativas en relación con sus creaciones. Funcionalmente, este derecho se adquiere con la obtención de su correspondiente certificado de registro, el cual lleva la firma del registrador que lo emite, y la firma del registrador jefe, sin la cual, la primera no tiene ninguna validez legal. En algunas oficinas se utiliza la figura de un secretario que adiciona una firma entre esa cadena de validaciones.

Comúnmente, en las oficinas de Propiedad Intelectual se han venido entregando certificados de registros, los cuales son la herramienta legal y jurídica para comprobar el derecho sobre cualquier creación fruto del intelecto humano. Desde sus inicios donde todos los procesos se efectuaban de forma manual hasta la automatización por medio de sistemas informáticos, estos certificados de registro han sido vulnerables a muchas situaciones de seguridad como falsificaciones, firmas no autorizadas, emisión de certificados sin firmas completas, alteraciones en los certificados ya firmados, por mencionar algunas.

En tal sentido, aunque muchos procesos están automatizados, garantizando el principio de prioridad registral, aún falta mucho por hacer con relación a la firma electrónica de los documentos y de los certificados digitales de los registradores. De tal manera que es necesario proveer un mecanismo confiable que ayude a prevenir y detectar los actos que atenten contra los derechos de los titulares de un registro de Propiedad Intelectual y evitar que exista competencia desleal relacionada con la misma.

Para brindar la seguridad requerida, existen los mecanismos criptográficos como la firma digital, la cual es comúnmente utilizada para certificar documentos o mensajes [2]. Una variante de ésta, es la firma agregada que permite producir una firma a partir de varias firmas generadas por distintas entidades y diferentes mensajes [3]. Tal característica puede ser de gran utilidad en aplicaciones donde dos o más entidades requieren certificar un documento.

Por lo anterior, en el presente trabajo se presenta un mecanismo de seguridad basado en firmas agregadas, que permite firmar los certificados de registro de forma anidada y jerárquica, es decir, que coexistan más de una firma para un mismo documento y que estás hayan sido plasmadas en un orden establecido, de tal manera que el director no firme antes que su subalterno, sino por la jerarquía definida. Este mecanismo tiene su correspondiente contraparte de validación, para verificar la fiabilidad de los certificados firmados. Así, la implementación de la firma electrónica agregada dentro de la automatización de los procesos de registro, específicamente en la firma de los certificados o títulos de registro, mejora los procedimientos internos y los problemas de seguridad claramente identificados, proporcionando con esto un valor agregado a la certeza jurídica de los servicios ofrecidos por las oficinas de Propiedad Intelectual.

El resto del artículo está compuesto como sigue. En la sección B se mencionan los elementos básicos utilizados por el esquema propuesto, como son las funciones picadillo, las firmas agregadas y los certificados digitales. En la sección C se explica el funcionamiento del esquema propuesto, mientras que en la sección D se explica el flujo de datos del mismo. En la sección E se presenta un análisis de seguridad. En las secciones F y G se presentan una discusión y las conclusiones de este trabajo, respectivamente.

2 HERRAMIENTAS CRIPTOGRÁFICAS

En esta sección se presentan las tres herramientas criptográficas utilizadas en el protocolo propuesto.

2.1 FUNCIONES PICADILLO

Una función picadillo es una función H de sólo ida que tiene como parámetro de entrada una cadena de longitud arbitraria y tiene como resultado una cadena de longitud fija. Formalmente, se puede definir como [4]:
H:{0,1}*{0,1}l
donde l representa la longitud en bits de la cadena.
Para garantizar la seguridad de una función picadillo, ésta debe cumplir las siguientes propiedades.
Transformación mezclada: un cambio a la entrada incluso en un bit, produce una salida diferente.
Pre-imagen: dado y {0,1}^l, encontrar x {0,1}^* tal que H(x)=y.
Colisión: dado x {0,1}^*, encontrar x′ {0,1}^* tal que x≠x′ y H(x)=H(x^′).
Eficiencia: dado x {0,1}^* es fácil calcular H(x).

Las funciones picadillo son ampliamente utilizadas en diversos procesos criptográficos para garantizar

integridad, ya que garantiza que cualquier modificación utilizada a los datos originales, modificará el picadillo de los mismos.

Por supuesto, garantizar la integridad implica cumplir los requerimientos mencionados. El más difícil de ellos es la colisión. Para las funciones picadillo más conocidas como MD5 (Message Digest) y SHA (Secure Hash Algorithm) se han encontrado debilidades, mismas que han causado incertidumbre. Por tal motivo, el Instituto Nacional de Estándares y Tecnología (NIST) comenzó la búsqueda de una nueva función picadillo que ofrezca digestos de 224, 256 y 512 bits. La función autorizada es la SHA-3 [5].

2.2 FIRMAS AGREGADAS BASADAS EN RSA

En 2003, Dan Boneh y colaboradores propusieron un esquema de firma digital que permitía la agregación al mezclar un conjunto de firmas para producir una única firma válida y verificable. La definición de una firma agregada es como sigue [6].

Sea U un conjunto de usuarios. Cada usuario u∈U tiene un par de llaves (PK_U,SK_U) que representan sus llaves pública y privada respectivamente. Sea σ_U una firma producida por cada u ∈U para algún mensaje de su elección. Todas las firmas producidas son agregadas en una firma σ por una entidad de agregación que tiene acceso a las llaves públicas y a los mensajes, pero no a las llaves privadas, de todas las entidades involucradas. Para verificar la firma agregada será necesario tener el acceso a las llaves públicas de los usuarios que han firmado cada uno de los mensajes, así como a sus correspondientes mensajes.

En 2004, Lysyanskaya y colaboradores propusieron un esquema de firma agregada secuencial [7]. Como su nombre lo indica, la generación de la firma agregada se realiza de manera secuencial, donde cada usuario debe esperar a que el usuario anterior termine la generación de la firma para poder agregar la propia. Esta especial característica es útil cuando las entidades a firmar tienen un rango o jerarquía y es muy importante que los miembros firmen de acuerdo a su rango.

El esquema de firma agregada secuencial requiere de tres algoritmos que se presentan a continuación:

-Generación de llaves: cada usuario genera su par de llaves (d,n),(e,n), de acuerdo al algoritmo de generación de llaves RSA.

- Seleccionar dos números primos grandes: p y q
- Calcular n=p*q
- Calcular φ(n)=(p-q)*(q-1)
- Seleccionar e <n,mcd(e,φ(n))=1
- Calcular d1*e^(-1) mod φ(n)

Firma agregada: cada usuario agrega a la firma σ^', los mensajes (M1,…,M(x-1)) y las correspondientes llaves públicas ((N1,e1),…,(N(x-1,) e(x-1))), realizando los siguientes pasos:

Si es la primera firma,

Asigna σ_0=0 , ir al paso 3.

Verifica la firma σ_(i-1)

Si la firma es válida ir al paso 3, termina el proceso, en otro caso.

Calcula h_x=H((M1,…,M_x),((N1,e1),...,(N(x,) ex))

Calcula y=hx+σ'(i-1)

Calcula σ'i=y^(dx) mod nx

-Verificación de la firma: dada una firma σ(i-1), los mensajes M1,...,M(i-1) y sus correspondientes llaves públicas ((N1,e1),…,(N(i-1,) e(i-1))), el verificador realiza lo siguiente:

1. Verifica que no haya duplicidad en las llaves públicas
2. Calcula y=σ(i-1)^(e(i-1)) mod n(i-1)
3. Calcula h(i-1)=H((M1,,M(i-1)),((N1,e1),...,(N(i-1,) e(i-1)))
4. Calcula σ'=y-hx
5. Verificar σ' de forma recursiva hasta llegar a la primera firma, donde σ'=0.

2.3 CERTIFICADOS DIGITALES

Un certificado digital de llave pública es una estructura de datos que consiste en una zona de datos y una zona de firma. La primera incluye la información de identificación del usuario y su llave pública. La segunda contiene la firma digital que certifica la validez de la información de la primera zona, expedida por alguna autoridad de confianza.

La Autoridad Certificadora (AC) es la entidad de confianza que certifica la relación de un usuario con su llave pública. Ya que en los esquemas de llave pública, la llave privada es inversa a la llave pública y viceversa, la vinculación de una entidad con su llave pública implica de igual forma la vinculación con su llave privada.

Los certificados mantienen una estructura ordenada que permite la rápida localización de la información. El estándar establecido es el X.509 de la Unión Internacional

de Telecomunicaciones [8].

Los certificados digitales tienen gran relación con las firmas digitales, ya que obligan a la entidad signataria a vincular su identidad con la llave pública que será utilizada para verificar la firma. De esta manera, el signatario no puede negar que la firma fue generada por el, si ha sido verificada correctamente con la llave pública contenida en el certificado, cumpliendo con esto el servicio de seguridad de no repudio.

3 PROTOCOLO PROPUESTO

El protocolo consta de cuatro entidades clasificadas en la Tabla 1. Las entidades corresponden al procedimiento que se hace de forma manual. El primero de ellos es el Registrador responsable, quien se encarga de generar el certificado, previa verificación (manual) de que el proceso legal de autenticación ha sido cumplido, esta entidad genera el primer mensaje de aprobación y firma.

La segunda entidad es el Secretario que es el responsable de validar la firma del registrador, por lo tanto, posee las firmas públicas de todos los registradores, esta entidad genera la segunda firma de certificación.

La tercera entidad es el registrador jefe, responsable de validar la firma del secretario. Si la validación es correcta genera la tercera firma del flujo en forma jerárquica.

Finalmente, la entidad solicitante que requiere el registro y la certificación. El o cualquier otra persona interesada pueden verificar con las llaves públicas, la validez de las firmas agregadas que legalizan el certificado.

Tabla 1. Entidades utilizadas en el protocolo propuesto

Entidades firmantes		
Primer signatario	Segundo signatario	Tercer signatario
Registrador responsable	Secretario	Registrador jefe
Entidades verificadoras		Verificador general
Primer verificador	Segundo verificador	
Secretario	Registrador jefe	Solicitante

Antes de realizar la certificación, se debe llevar a cabo un proceso de generación de llaves públicas y privadas de cada entidad. El procedimiento para la emisión de los certificados de registro, se detalla en la Figura 1, partiendo del hecho que todo el proceso de verificación legal ha sido cumplido, y que efectivamente ya está listo para proceder a emitir el certificado de registro respectivo:

1. El sistema actual habilita la generación del certificado de registro, una vez cumplido el proceso establecido, es decir, que se ha generado el documento oficial que avala que un trabajo artístico pertenece a un autor o autores en específico. El registrador encargado del análisis legal firma el certificado de registro con su llave privada, generando la primera iteración de la firma agregada conformada por su nombre como mensaje de visto bueno y la firma digital.

2.El secretario revisa en el sistema quien fue el registrador que generó el certificado y verifica la firma con la llave pública de ese registrador.

3.Si la verificación es positiva procede a agregar su nombre como visto bueno y firma con su llave privada, adicionando esta, a la firma creada por el registrador.

4.El registrador jefe con la llave pública del secretario verifica la firma agregada del secretario.

5.Si el proceso de validación es correcto, procede a poner su nombre como mensaje y visto bueno, firma con su llave privada, adicionando esta, a la generada por el secretario.

6.El solicitante recibe su certificado y las firmas agregadas del registrador, secretario y registrador jefe, pudiendo verificar la validez de su certificado con las llaves públicas del registrador que emitió el certificado, el secretario o el registrador jefe.

Figura 1. Aplicación del protocolo de firmas agregadas en la generación de certificados

4 FLUJO DE DATOS DEL PROTOCOLO PROPUESTO

La notación utilizada por el protocolo propuesto se presenta en la Tabla 2. Es importante destacar que el solicitante del registro no requiere de ninguna información propia, es decir, no necesita un par de llaves que sean de su propiedad, debido a que en la verificación de la firma agregada se utilizan las llaves públicas todas las entidades firmantes, es decir, el registrador, el secretario y el registrador jefe.

Tabla II. Notación del protocolo propuesto

Variable	Descripción
$nombreR$	nombre del registrador responsable
$documento$	Documento oficial de la propiedad intelectual solicitada
(dR, nR)	llave privada del registrador responsable
(eR, nR)	llave pública del registrador responsable
$nombreS$	nombre del Secretario
(dS, nS)	llave privada del secretario
(eS, nS)	llave pública del secretario
$nombreRJ$	nombre del Registrador Jefe
$(dRJ, nRJ))$	llave privada del Registrador Jefe
Cert	
(eRJ, sRJ)	llave pública del Registrador Jefe
H	Función picadillo
$\|\|$	Operación de concatenación

El protocolo propuesto es una variación de la firma agregada mostrada en la sección B. En el proceso original la firma es generada con los mensajes y las llaves públicas de cada signatario. En la versión propuesta, las llaves públicas son reemplazadas por los certificados digitales, de tal manera que los signatarios no puedan negar la propiedad de la llave pública como par de la llave privada con la que fue generada la firma.

Los procesos en cada fase se muestran a continuación, agrupados por las diferentes entidades participantes.

Firma del Registrador (generación de la firma 1)

aprobacionR = documento||nombreR||CertR

hR = H(aprobacionR)

σR=⟦hR⟧^dR mod nR

Validación del Secretario (verificación de la firma 1)

validaR=⟦σR⟧^eR mod nR

hvR=H(documento||nombreR ||CertR)

Si hvR=validaR entonces la firma es válida.

Firma del Secretario (generación de la firma 2)

aprobacionS=nombreS||CertS

hS=H(aprobacionR||aprobacionS)

y=hS+σR

$\sigma S = ydS \bmod nS$

Validación del Registrador Jefe (verificación de la firma 2)

1. $validaS = \sigma SeS \bmod nS$
2. $hsV = H(aprobacionR||aprobacionS)$
3. $x = validaS - hsV$
4. $Si\ x = \sigma R$ entonces la firma es válida.

Firma del Registrador jefe (generación de la firma 3)

5. $aprobacionRJ = nombreRJ||CertRJ$
6. $hRJ = H(aprobacionR|aprobacionS|aprobacionRJ)$
7. $y = hRJ + \sigma S$
8. $\sigma RJ = ydRJ \bmod RJ$

Validación del Solicitante (verificación de la firma 3)

1. $validaRJ = \sigma RJeRJ \bmod nRJ$
2. $hRJv = H(aprobacionR|aprobacionS|aprobacionRJ)$
3. $x = validaRJ - hRJv$
4. Si $x = \sigma S$ entonces la firma es válida.

5 ANÁLISIS DE SEGURIDAD

A continuación, se presenta una lista de los problemas, los ataques que se pueden derivar y las soluciones que ofrece el protocolo propuesto.

Problema 1: No existe un mecanismo que autentique a los funcionarios correctamente.

Ataque: Posible usurpación de la identidad de los funcionarios.

Solución: La firma digital es generada con una llave privada que sólo conoce el funcionario a firmar; si la llave pública indicada por el funcionario y el mensaje no es modificado entonces el firma es válida, lo que garantiza que la autenticación es correcta y que no es posible usurpar la identidad de los funcionarios.

Problema 2: El certificado de registro es propenso a sufrir alteraciones.

Ataque: Editar la información importante del certificado, de tal manera que los cambios sean imperceptibles al ojo humano.

Solución: En el proceso de la firma digital se utilizan funciones picadillo, las cuales tienen la característica de que si un dígito es alterado en el documento original, el nuevo picadillo calculado es completamente diferente al del original, lo que permite detectar alteraciones en el documento por mínimas que sean.

Problema 3: Certificados falsificados.

Ataque: Cualquier interesado en este tipo de ataques puede con buenas herramientas digitales crear un duplicado del certificado original a partir del cual puede crear múltiples certificados falsos con firmas falsificadas.

Solución: Con el uso de la llave privada para firmar los certificados se evita tener duplicados de un certificado, ya que cada firma está asociada a un documento en particular.

Las firmas para dos documentos diferentes, aunque sean firmados por la misma persona, generan dos firmas digitales distintas, lo que evita la falsificación de certificados.

Problema 4: Firma de certificados que no cumplen la jerarquía legal establecida.

Ataque: El orden de las firmas es importante ya que el secretario certifica la validez del registrador y el registrador jefe del secretario, si este orden es alterado, la legalidad del título de registro sería discutible.

Solución: El uso de firmas agregadas permite establecer un orden jerárquico obligatorio, en el cual si se altera el orden, no podría existir la validación correcta ni la firma adecuada.

Problema 5: El secretario o el registrador no efectúen la validación de las firmas y/o no tienen un mecanismo adecuado que garantice la validez de la firma anterior.

Ataque: Sin un mecanismo correcto de validación de firmas, cualquier entidad puede generar un certificado con firmas falsificadas, y al ojo humano podrían verse iguales, pero ser falsas.

Solución: Con las firmas digitales se asegura que la firma la hizo la persona correcta, y con las firmas agregadas, se establece el mecanismo de validación usando la llave pública del signatario, por tanto, si la firma ha sido efectuada por otra persona, la validación daría error y no se procedería efectuar la firma actual.

6 DISCUSIÓN

La firma electrónica permite vincular al signatario y validar los datos permitiendo detectar posibles modificaciones. Para el caso en particular de las firmas agregadas en los certificados, éstas avalan que la firma plasmada en cada paso del proceso, pueda ser asociada a un signatario específico y que el siguiente valide la firma del signatario anterior, garantizando el no repudio, brindando de esta manera una solución al problema planteado sobre la seguridad de que cada firma corresponda a la entidad correcta. El uso de la función picadillo en el proceso de generación de firmas garantiza la integridad del certificado, por lo que con el proceso manual este puede ser alterado de tal forma que no pudiera detectarse alguna modificación. Con el uso de funciones picadillo, esto se descarta garantizando la integridad del certificado, ya que una de las características principales de una función picadillo es que esta devuelve un valor completamente diferente, con un dígito que sea alterado en el mensaje original.

Otra situación planteada como problema de seguridad en el proceso actual, es la posibilidad de la falsificación de firmas, lo cual es solventado con el proceso de firmas agregadas, ya que cada signatario firma con su llave privada, esto aparte de garantizar que las firmas corresponden a la entidad correcta, es decir, que son auténticas.

En el diseño planteado, utilizando firmas agregadas, se estipula la jerarquía en que las firmas deben ser validadas, de tal forma que si el registrador jefe quiere validar la firma anterior y esta no es del secretario, la validación sería incorrecta, ya que su validación la efectúa con la llave pública del secretario, garantizando el orden correcto de aprobación y firma.

El uso de firmas agregadas provee una solución a todos los problemas de seguridad planteados, garantizando el no repudio, la integridad y la autenticidad del certificado de registro, servicios que actualmente no pueden ser brindados por el sistema actual.

El uso de firmas agregadas trae consigo el beneficio que cualquier entidad aparte del solicitante como aduanas, jueces, bancos, etc., puedan validar la autenticidad del certificado con una seguridad más precisa que la que pueda brindar cualquier proceso manual actual.

Para que la validación de los certificados de registro sea exitosa, es importante que el usuario no pueda elegir qué firma desea validar, si no que su par de llave pública contenida en su certificado digital, sea incluida dentro del flujo del proceso. De esta manera si firma otra entidad, en la validación se obliga a utilizar sólo la firma de la persona que legalmente estaba autorizada para efectuarla. Es importante señalar que un certificado digital tiene la propiedad de vincular una llave pública con una entidad en específico, ofreciendo con esto el no repudio.

La longitud de las llaves es muy importante para establecer la seguridad, de tal manera que RSA se considera seguro si utiliza llaves de 1024 bits para el público en general, pero para el gobierno, que es el caso de estas instituciones la seguridad debe ser de 2048 bits.

Al aumentar el tamaño de las llaves, es importante considerar que los requerimientos del hardware también aumentan, ya que la cantidad de procesos a efectuar es mucho más elevada, y esta necesidad también dependerá de la cantidad de personas efectuando estas operaciones.

Los tiempos de ejecución y el hardware necesario, también dependerán del tamaño del documento a firmar, por lo que hay que efectuar pruebas con los certificados que contengan la mayor información para establecer así, los tiempos adecuados de respuesta.

7 CONCLUSIONES

En este trabajo se presenta un protocolo basado en firmas agregadas para la generación de certificados de registro. La propuesta permite que los autores registren y comprueben la propiedad del producto registrado con una serie de tres firmas en forma jerárquica.

El protocolo propuesto garantiza la veracidad en la vinculación del autor y su propiedad, siguiendo los pasos de verificación correspondiente en una fase manual, para posteriormente generar la firma agregada para la certificación. Tal proceso evita los principales problemas de los registros de propiedad como son falsificación y/o usurpación.

REFERENCIAS

1. Organización Mundial de la Propiedad Intelectual (OMPI). Recuperado el 15 de junio de 2015. Sitio Oficial en español: http://www.wipo.int/portal/es/.
2. FIPS PUB 186-4, Digital Signature Standard (DSS), Computer Security, U. S. Department of Commerce & National Institute of Standards and Technology, July 2013.
3. Boneh, D. Aggregate Signatures. In: Tilborg, H., Jajodia, S. (Eds). Encyclopedia of Cryptography and Security, 2nd Edition, Springer New York Dordrecht Heidelberg London, A-27, 2011.
4. Stinson, D. Cryptography: Theory and Practice. New York: Chapman & Hall/CRC, 2006.
5. Computer Security Division. Secure Hashing: approved algorithms. National Institute of Standards and Technology, August, 2015.
6. Boneh, D., Gentry, C., Lynn B., and Shacman, H., Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Biham, E. (Ed.). Advances in Cryptology, EUROCRYPT 2003, Lecture Notes in Computer Science 2656. Poland: Springer Berlin Heidelberg, 2003, 416-432.
7. Lysyanskaya, A., Micali, S., Reyzin, L., Shacham, H. Sequential Aggregate Signatures from Trapdoor Permutations. Cachin, C., Camenish, J. (Eds.). Advances in Cryptology, EUROCRYPT 2004, Lecture Notes in Computer Science 3027, Switzerland: Springer, 2004, 74-90.
8. Tuecke, S., Welch, V., Engert, D., Pearlman, L., Thompson, M. Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile. RFC 3820 (Proposed Standard), June 2004.

Acerca de los autores

Kyrna Quintanilla es Ingeniera en Sistemas y Computación, egresada de la Universidad Tecnológica de El Salvador. Realizó sus estudios de postgrado en la Maestría de Seguridad y Riesgos Informáticos en la Universidad de Don Bosco en El Salvador. Sus áreas de interés son la Propiedad Intelectual, bases de datos Oracle, implementación de sistemas y seguridad en sistemas de información.

María de Lourdes López García es Doctora en Computación egresada del Centro de Investigaciones y de Estudios Avanzados el IPN (CINVESTAV-IPN). Profesora de Tiempo de Completo e investigadora en el Centro Universitario UAEM Valle de Chalco, en la Universidad Autónoma del Estado de México. Sus áreas de interés son: criptografía, seguridad en sistemas de información y visión artificial.