Desarrollo de una autoridad de certificados digitales para una intranet universitaria

Dorian Omar González Cortés, Jesús Eduardo Torres Castañeda,
Petar Zaprianov Doychev y Arturo Pruneda Martínez

Escuela Superior de Computo del Instituto Politécnico Nacional,
Av. Juan de Dios Bátiz S/N esquina Miguel Othón de Mendizával
Unidad Profesional Adolfo López Mateos
Col. Nueva Industrial Vallejo C. P. 07738, México, D. F
dorian_omar@hotmail.com, jetorresc@hotmail.com,
petar555@hotmail.com, apruneda@ipn.mx

Resumen. Un certificado digital proporciona la posibilidad de autentificar a una entidad para permitir el acceso a servicios proporcionados por diversos sistemas de información. La Autoridad de Certificados (AC), es la parte más importante de una infraestructura de llave pública (PKI), debido a que en ella descansa la confianza de toda la seguridad proporcionada por este sistema [1]. Los certificados digitales emitidos por la AC son el resultado de un proceso riguroso de verificación, que garantiza la legitimidad de la entidad certificada.

La AC requiere de los servicios de entidades auxiliares para su adecuado funcionamiento, por ejemplo una Autoridad de Registro (AR) y un repositorio de datos. En este trabajo se presenta el desarrollo de una AC, la cual provee certificados digitales que serán usados para autentificar a los usuarios de una Intranet universitaria. Se detalla cada parte que compone el sistema, además del proceso de certificación adecuado al entorno particular en el que se desarrolla el proyecto, así como políticas de seguridad necesarias para asegurar el uso adecuado de los certificados.

1 Introducción

Actualmente, el creciente uso del Internet, no solo como medio de consulta o comunicación, si no como un medio por el cual se llevan acabo transacciones, en las que se manejan datos sensibles, ha motivado un gran interés en la utilización de diversas herramientas para la protección de dichos datos.

El uso de una Infraestructura de Llave Pública (PKI) ofrece la plataforma necesaria para el uso de certificados digitales. Los certificados digitales proporcionan un tipo de identificación digital para una entidad, y por medio de éstos, una entidad A se puede identificar con otra entidad B, presentando su correspondiente certificado.

Un certificado digital es un documento emitido por una Autoridad de Certificados Digitales (AC), la cual firma este documento dándole validez para aquellas instancias que reconozcan a la Autoridad de Certificados, como una autoridad emisora de certificados de confianza.

A. Gelbukh, M. Hernández Cruz (Eds.) Avances en la ciencia de la computación en México, CORE-2003, pp. 255–265, 2003.

El certificado digital es una forma eficaz de distribuir la llave pública de la entidad certificada [8]; sin una adecuada distribución de la misma, el uso de criptografía asimétrica no serviría de mucho. De nada sirve que una entidad cuente con una llave pública si esta no es dada a conocer. La llave pública esta contenida en el certificado digital, y una forma de distribuir los certificados digitales es almacenándolos en un repositorio, él cual esta disponible a todas las personas para obtener el certificado de otra entidad.

Dentro de una Infraestructura de Llave Pública, la AC juega un papel central, ya sea que pertenezca a la propia PKI, o bien sea externa; por el simple motivo que AC se encarga de la gestión y emisión de los certificados digitales.

La confianza de los usuarios del sistema se deposita en la AC, y ésta debe proporcionar la garantía de que su llave privada está bien resguardada, ya que con esa llave se firman los certificados que emite. Cuando los usuarios dejan de confiar en la Autoridad de Certificados, toda la infraestructura de seguridad se viene abajo y los certificados dejan de tener validez [1].

Un certificado digital tiene un tiempo de validez finito, determinado por la AC de acuerdo a las especificaciones requeridas en el medio en el que se implementen los certificados.

La información que será incluida dentro del certificado digital, es verificada por Autoridad de Registro (AR), que son entidades autorizadas por una Autoridad Certificadora. La AR, es un puente de comunicación entre las entidades finales y la AC.

Este artículo trata sobre la implementación de certificados digitales en un entorno universitario, él cual tiene características particulares que serán tratadas en los siguientes párrafos; por lo que deben hacerse las adecuaciones necesarias para su funcionamiento. Estas características comprenden los componentes de la arquitectura propuesta, las tecnologías usadas, el proceso de certificación, así como las políticas adecuadas a este entorno y el ciclo de vida del certificado digital.

2 Características del entorno

Actualmente la Escuela Superior de Cómputo del IPN, no cuenta con sistemas de información propios para la administración de sus procesos internos. Es por eso que en la actualidad se está desarrollando un proyecto llamado "Intraescom", el cual tiene como objetivo el desarrollo de una Intranet que servirá para conectar las diversas áreas que comprende la escuela, y facilitar todo el proceso administrativo y académico dentro de ésta.

Dentro de un ambiente universitario, la implantación de una Intranet puede tener altos beneficios, cuando se toma en cuenta la reducción de tiempos en procesos que regularmente se realizan de manera manual.

Entre los sistemas que se están desarrollando, solo por mencionar algunos se encuentran: El Sistema de Control Escolar, el Sistema de Contabilidad y el Sistema de Administración de Activo Fijo.

En una Intranet, los usuarios tradicionalmente se identifican mediante un nombre de usuario (*username*) y una contraseña (*password*) para acceder a los recursos restringidos. Este método presenta la problemática del robo o falsificación de *password* cuando éste viaja por la red de manera insegura. Además, las contraseñas

suelen ser fácilmente atacadas, ya que teniendo tan solo algunos caracteres de ella, se pueden utilizar ataques conocidos como de prueba y error. Existen además otras razones por las cuales las contraseñas son un mecanismo de autentificación que no se considera seguro [2].

El proyecto de IntraEscom contempla la implementación de una Infraestructura de Llave Pública (PKI) para proveer los servicios de seguridad que requieren los usuarios y las aplicaciones. Una PKI se define como un conjunto de mecanismos criptográficos de llave pública basados en la existencia de dos llaves (una pública y otra privada) que se utilizan para garantizar la identidad del usuario, la confidencialidad y la integridad de la información transmitida [6].

Los certificados tienen la función de autentificar a las entidades que intentan entrar a un sistema, para permitir el acceso. Éstos estarán almacenados dentro de algún objeto físico conocidos como *tokens*, los cuales pueden ser un disco compacto, una tarjeta inteligente (*smartcard*), o una ikey [7]. El uso de un medio de almacenamiento portátil para el material criptográfico es necesario para que los usuarios puedan llevar su certificado correspondiente con ellos y no necesiten dejarlo en una máquina, que es donde normalmente se guarda el certificado así como la llave privada. Se pretende que el usuario desde cualquier computadora o terminal pueda usar su certificado digital, sin necesidad de copiarlos al disco duro, ya que esto representa un proceso molesto para el usuario, o bien, un posible robo.

Algunos *tokens* tienen características de seguridad que evitan el acceso a la información contenida dentro del mismo, si no se introduce una contraseña. Esto permite que a pesar de que el dispositivo de almacenamiento sea robado o perdido, no sea fácil acceder a la llave privada de la entidad certificada.

El uso de certificados digitales permite el uso del protocolo SSL (Secure Sockets Layer) para sesiones seguras, donde los datos van cifrados con una llave de sesión que acuerdan las dos entidades que se comunican. En los pasos del protocolo SSL, el servidor le presenta su certificado al cliente, este verifica la validez del certificado. El cliente puede o no presentar su certificado. Se crea una llave de sesión con un algoritmo que tanto cliente como servidor soportan., y como su nombre lo indica, solo se usa esa llave para esa sesión [5].

El protocolo SSL es soportado por los principales navegadores que existen actualmente, por ejemplo IExplorer, Netscape, Mozilla, etc. Para que la información aloja en un servidor pueda verse protegida mediante el protocolo SSL es necesario instalar un certificado digital, siendo este un requisito para establecer una conexión segura, dentro de los pasos del protocolo SSL [3].

3 Arquitectura propuesta

Los componentes del sistema son los siguientes:

- Autoridad Certificadora
- Autoridad de Registro
- Repositorio de Datos

En la Fig. 1 se muestra la interacción entre ellos.

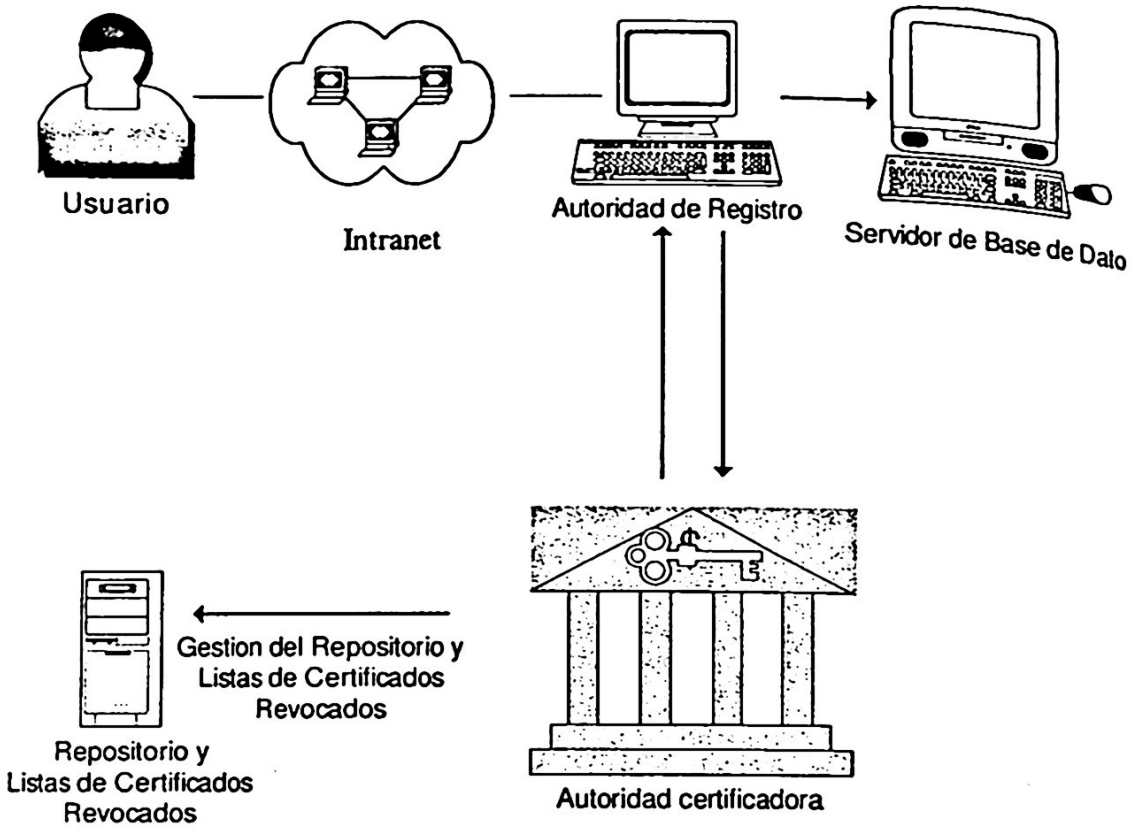

Fig. 1. Interacción entre componentes de la arquitectura

3.1 Autoridad Certificadora

La AC es la encargada de la gestión y emisión de los certificados, así como establecer las políticas adecuadas para asegurar su correcto uso. La AC esta aislada, (desconectada de la red) con el propósito de resguardar su llave privada y evitar accesos de entidades no autorizadas. Por el motivo anterior la comunicación con Autoridad de Registro es mediante dispositivos de almacenamiento físico, tales como CD-ROM, diskette, etc.

Las funciones de la Autoridad Certificadora son las siguientes:

- Emisión de los certificados de usuarios registrados y validados por la Autoridad de Registro (AR).
- Revocación de certificados (CRL - Lista de Certificados Revocados). Un certificado puede ser revocado por que los datos han dejado de ser válidos, llave privada ha sido comprometida o el certificado ha dejado de tener validez dentro del contexto para el que había sido emitido.
- Renovación de certificados.
- Distribución de certificados e información asociada a los mismos. Se debe ofrecer un mecanismo para el fácil acceso a los certificados. La forma mas empleada de publicar los certificados es un repositorio público.

La AC es operada por un administrador, el cual cuenta con una interfaz que permite emplear todas las funciones que la AC proporciona.

3.2 La Autoridad de Registro (AR)

La AR sirve de puente entre las entidades finales y la AC. Una AR tiene como principal función recibir los requerimientos de certificación, para el caso de esta Intranet, la información necesaria para hacer un requerimiento ya se encuentra capturada dentro de los sistemas que la componen, principalmente el de Control Escolar (para los alumnos), y el de Administración y Control de Personal (para los profesores y otros empleados no docentes). La AR obtendrá entonces de estos sistemas, los datos necesarios para hacer los requerimientos.

3.3 Repositorio de datos

Un repositorio de datos es una base de datos que tiene la característica de poder ser accedida fácilmente por el usuario que requiera la información.

En el repositorio de datos se almacena información que no necesita ser secreta, solo se necesita protegerla de posibles modificaciones no autorizadas. Dentro de esta información se encuentran los certificados digitales, a los cuáles los usuarios pueden acceder para verificar sus estado o bien para obtener la llave pública de otra entidad.

La información en este repositorio puede ser accedida mediante una dirección IP o un DNS, los cuáles deben darse a conocer a los usuarios al momento de la entrega del certificado.

3.4 Proceso de certificación

Dentro del entorno académico, todos los alumnos, así como personal académico y administrativo deben estar certificados por la AC. Este proceso inicia conjuntamente con el semestre escolar. En los siguientes puntos se explican los procesos de emisión de certificados, revocación y renovación

3.4.1 Creación de solicitudes de certificación

Las solicitudes de certificación son creadas por la AR, de la información obtenida de los sistemas de Control Escolar y de Administración y Control de Personal mencionados anteriormente. También se aceptan solicitudes de los usuarios mediante un formulario que se puede llenar en una pagina web y se envía a la AR Esto solo en casos en los que por alguna razón, los sistemas de Control de Escolar y el Sistemas de Administración y Control de Personal no contengan la información, o bien en el momento de la importación de datos, el registro de esa persona no era válido; se considera un registro válido aquel que contenga información de alguna persona con derecho a ser certificada, es caso de alumnos, estar inscrito, y en caso del personal, seguir laborando dentro del instituto.

La AR crea el par de llaves directamente dentro del medio físico donde serán almacenados, crea las solicitudes con la información de cada usuario. Una vez creados son exportados a la AC, para proceder a la emisión del certificado correspondiente.

3.4.2 Emisión de certificados

La AC recibe los requerimientos de certificación de parte de la AR, después Administrador selecciona aquellas solicitudes que serán firmados. Una vez firmad son exportados a la AR, para que sean almacenados dentro del *token* (ikey, tar inteligente) correspondiente, y ésta misma es la que hace entrega de los *tokens* usuarios finales. En la entrega se le pide al usuario que se identifique mediante credencial.

La Autoridad Certificadora, una vez que firmó el certificado y por lo tanto válido, lo agrega al repositorio de datos.

3.4.3 Casos de revocación

Los certificados durante el tiempo en el que son válidos, pueden ser revocados distintas causas, como perdida o robo del *token*, que la llave privada haya comprometida, o por un mal uso del certificado según lo estipulado en las políticas seguridad emitidas por la Autoridad Certificadora. También usuario puede pedir revocación a la AR, explicando los motivos por los cuales requiere revocar certificado.

Los certificados revocados se pueden consultar dentro de una lista de revocaci expedida por la AC. Esta lista de revocación esta firmada por dicha autoridad, emitida al final del día, solo en el caso de existir una revocación; en caso contrario, se emite dicha lista.

Una lista de certificados revocados solo contiene los datos relacionados con la que la creó, la fecha de creación, y la próxima actualización. Dentro de la lista revocados solo se coloca el número de serie del certificado, así como la fecha hora en la que fue revocado.

3.4.4 Casos de renovación

Los certificados se renuevan cada cambio de semestre, para esto el solicitante deb tener un registro válido en los sistemas correspondientes, ya sea alumno o personal la escuela. En el caso de los alumnos, este debe estar inscrito, por lo tanto debe alumno regular. El personal debe seguir perteneciendo al instituto.

El proceso de renovación comienza con la obtención de los registros por la AR, como se especifico en la emisión de certificados. Y los siguientes pasos son mismos que en la emisión de certificados.

También, tal como en la emisión de certificados, existe la posibilidad de solicitar renovación mediante el acceso a una pagina web, llenando todos los datos, enviándola.

3.5 Políticas de certificación

Las políticas de certificación juegan un papel muy importante dentro de un ambiente PKI donde se implementa una AC, ya que con ellas se puede asegurar funcionalidad y el uso adecuado de los certificados, así como prever posibles sanciones en el caso que no se cumpla con los reglamentos. Como ejemplo de estas políticas de certificación tenemos las siguientes:

I.- De los certificados digitales:

1. Se certificada a todo persona interna a la Escuela Superior de Computo que realice correctamente el proceso de solicitud de certificación o bien aquellas que tengan un registro válido en los sistemas de Control Escolar o Administración y Control de Personal, salvo los casos que en este mismo apartado se mencionan.
2. Se perderá el derecho de certificación por falsificación de datos durante el proceso de solicitud del certificado digital. El derecho de certificación será devuelto de acuerdo al criterio del Administrador de la AC.
3. La vigencia del certificado digital se llevará a cabo conjuntamente con el ciclo escolar (semestral). Después de este periodo el certificado es inválido, y no podrá usarse como medio de autentificación.
4. Se realizará la revocación automática del certificado en caso de:
   - Extravió o robo de la llave privada.
   - Uso indebido de información según los criterios establecidos en el Reglamento Académico.
   - El uso indebido de una llave privada ajena con o sin el conocimiento del poseedor legitimo de la llave privada.
5. La ruta de certificación para los certificados confiables dentro del sistema solo será directamente de la AC de la ESCOM.

II.- De la Autoridad de Certificados Digitales (AC):

1. La AC será operada única y exclusivamente por el administrador de la AC, que será responsable del uso correcto y protegido de la llave privada de ésta. Así como de cumplir las funciones de la AC.

III.- De la Autoridad de Registro (AR)

1. La AR será operada única y exclusivamente por el administrador de la AR. El administrador será el responsable de llevar acabo las tareas de verificación y autentificación de datos del solicitante.

IV.- Del repositorio de datos (RD)

1. El Repositorio de Datos será manejado exclusivamente por el administrador de la AC. La actualización del repositorio se realizará al final del día en caso de haber creado nuevos certificados digitales.

V.- De la lista de revocación de certificados digitales. (CRL).

1. La CRL será creada exclusivamente por el administrador de la AC y firmada por la llave privada de la AC. La CRL se actualizara al final del día en caso de haber nuevas revocaciones, o algún caso especial.

VI.- De la generación de llaves

1. El proceso de generación del par de llaves es llevado a cabo por la AR, después de haber recibido una información valida de certificación. El par de llaves es creado dentro del *token.*

VII. De la emisión de certificados.

1. Después de haber cumplido los requerimientos para una solicitud satisfactoriamente, la AC verifica la veracidad de esta solicitud, para proceder con la emisión del certificado correspondiente.

VIII. De la entrega del certificado.

1. El certificado se almacena en un medio físico (smart-card, i-key), la entidad certificada deberá acudir personalmente a recoger dicho medio físico, donde se encuentra almacenado su certificado digital y la llave privada.

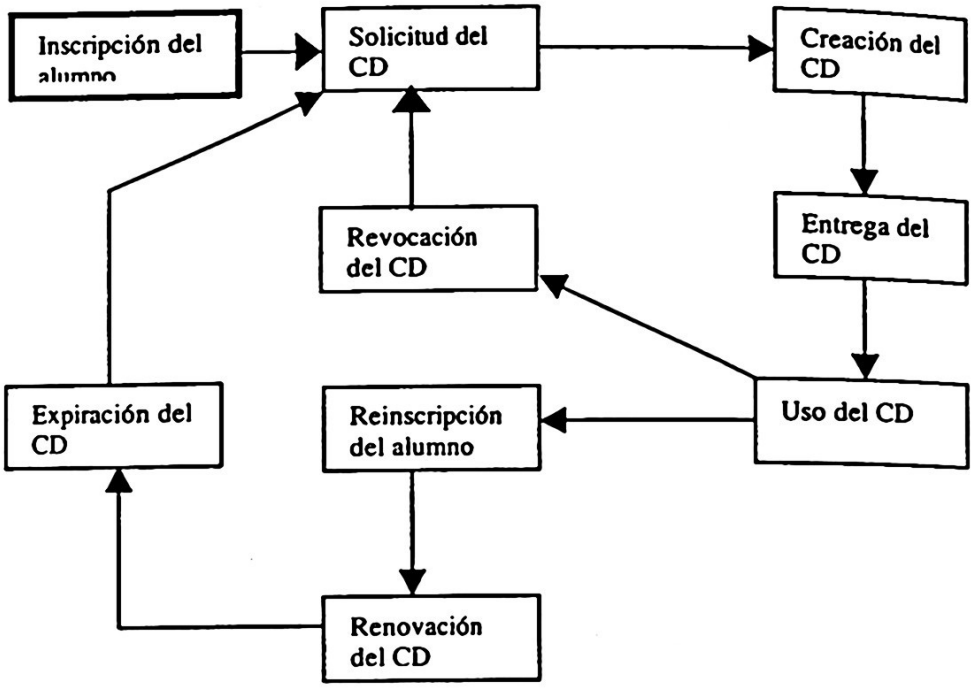

Fig. 2 Ciclo de vida del Certificado

4 Ciclo de vida del certificado digital

Los certificados digitales solo podrán pertenecer a alumnos que se encuentren inscritos en el semestre corriente, así como a personal docente y no docente internos a la escuela que se encuentren en situación regular.

1. El ciclo de vida de los certificados digitales inicia en la inscripción de los alumnos.
2. Se realiza la solicitud del mismo.
3. El Certificado Digital es creado.
4. Se entrega el Certificado Digital al dueño correspondiente.
5. A partir de este momento el certificado es valido para su uso, durante el cual podrá ser revocado.
   - En caso de revocación, se realizará nuevamente el proceso de solicitud

6. Después de la reinscripción de los alumnos, se podrá realizar el proceso de renovación de certificado digital, durante un breve tiempo antes de su expiración.

5 Desarrollo de la Autoridad de Certificados

Para el desarrollo de la AC debían de tomarse en cuenta 2 cosas: La utilización de funciones, librerías, o componentes que brindaran las funciones criptográficas que una AC lleva a cabo, y el desarrollo de las interfaces para administrar esta AC.

Para realizar las operaciones criptográficas se utilizaron las funciones que brinda OpenSSL, que es un popular proyecto de código abierto disponible en Internet. OpenSSL ofrece la posibilidad de crear el par de llaves (pública y privada), requerimientos de certificación, certificados digitales y lista de revocación.

OpenSSL maneja algoritmos como el RSA y DSA para la creación de llaves, la longitud de estas se le pueden indicar mediante las opciones que contiene en sus comandos. Usa el estándar x.509 para la creación de certificados, este estándar ha sido aceptado por la International Telecommunication Union-Telecomunication Standardization Sector (ITU-T) y por ISO/International Electrotechnical Comisión (IEC) [4].

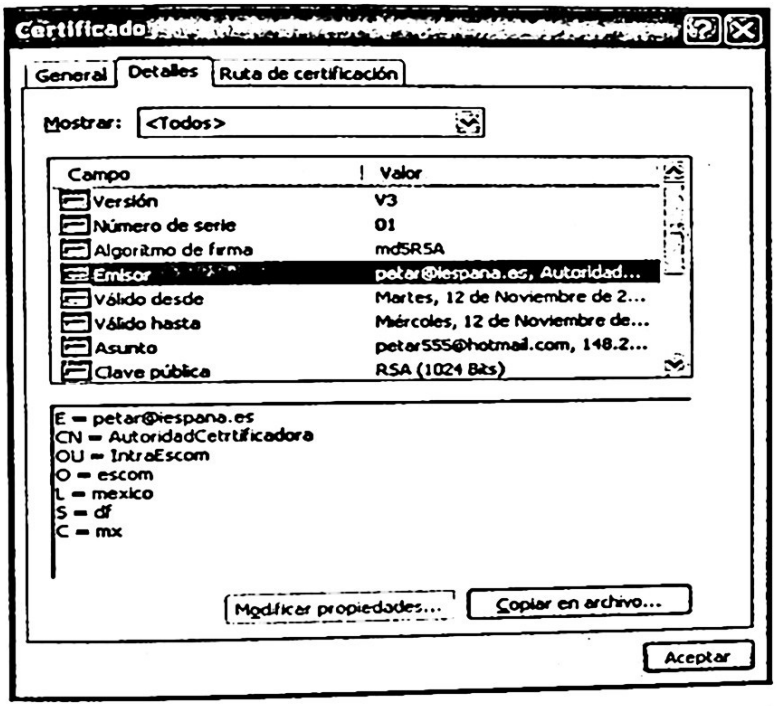

Fig. 3. Ejemplo de un certificado creado con la AC de ESCOM

La estructura del estándar x.509 contiene los campos necesarios para poder identificar a la entidad certificada. Un ejemplo de certificado digital puede verse en la siguiente figura 3.

La interfaz de la AC, se desarrollo como un software *standalone*, utilizando el lenguaje de programación Java sobre una plataforma Linux Mandrake 9.0. Las

interfaces implementan las funciones de OpenSSL, él cual habitualmente se usa mediante línea de comandos.

En la figura 4, se muestra una interfaz usada por el administrador de la AC, donde tiene la posibilidad de elegir en los requerimientos de certificación proporcionados por la AR. Después de elegir los requerimientos deseados, son firmados, la interfaz muestra los certificados que ya han sido firmados, así como el porcentaje de avance.

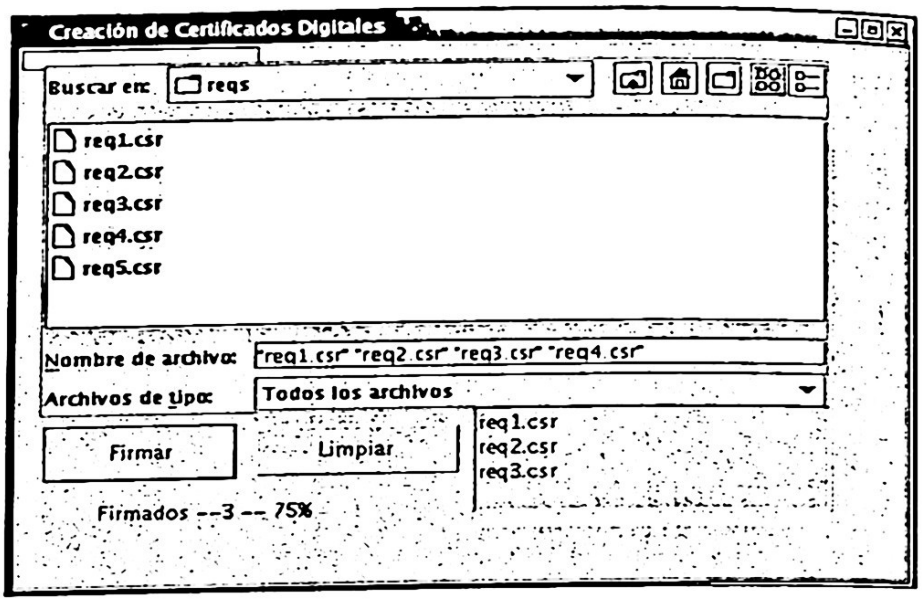

Fig 4. Interfaz de firmado de la AC

Las interfaces de la AR son mediante páginas web, que pueden ser visualizadas través de un navegador. Como se ha mencionado la AR no esta aislada, y mediante este tipo de interfaces se puede operar a distancia, aunque es preciso comentar que administrador de la AR debe contar previamente con un certificado digital para poder operar la misma. La AR utiliza un servidor web Apache sobre la plataforma Windows.

6 Conclusiones

El contar con una Autoridad de Certificados propia permite tener un mayor control os procesos de certificación, así como la creación de políticas de seguridad adecuadas l entorno, y de esta manera, implementar el nivel de seguridad deseado.

El uso de los certificados digitales genera un nivel alto de seguridad en cualquier mbiente, siendo además la base para el desarrollo de una PKI, que se vislumbra omo una de las soluciones de seguridad más completas y utilizadas en los próximos ños.

Los procesos que la AC lleva acabo para la certificación, deben ser planeados studiados con sumo cuidado, para que las entidades pueden confiar en los ificados que esta AC emita. Así también es importante la protección de la llave privada de la AC, donde recae toda la seguridad de una infraestructura de seguridad, donde una AC es la parte central.

Referencias

Pruneda A., "Desarrollo de una infraestructura de llave pública para aplicaciones de comercio electrónico seguro", CIC–IPN, México D.F. 2003, (M.S. Thesis).
Manual Pons Montorrel, "Control de accesos",
http://www.criptored.upm.es/guiateoria/gt_m013d.htm.
Certificados de seguridad SSL Server, Servidor Seguro Datacom,
www.datacommultimedia.com/certificados_seguridad_.htm
OpenSSL, "The Open Source toolkit for SSL/TSL", www.openssl.org/
HTMLWeb, Seguridad, Transacciones seguras en Internet.
http://www.htmlweb.net/seguridad/ssl/ssl_6.html.

[6] Menchaca, Pruneda., "Desarrollo de una Infraestructura de Llave Pública (PKI) para comercio electrónico", Congreso Internacional de Computación, CIC-IPN. México D.F., 2002.

[7] Rainbow Technologies: ikey 2000, http://latinamerica.rainbow.com/ikey/ikey2000.html

[8] Carlisle Adams, Steve Lloyd (1999), "Understanding Public –Key Infrastructure". Macmillan Technical Publishing.