Ciencias Matemáticas, Vol. 35, No. 1, 2021, Pag. 1-8
Recibido 11-2020, Aceptado 04-2021

Autoridad de certificación de la Facultad de Matemática y Computación de la Universidad de la Habana

Certification Authority of the Faculty of Mathematics and Computing of the University of Havana

Yavseny Roque Hernández[1]*, DraC Teresa Bernarda Pagés López[1], Yaidir Mustelier Ruiz[1]

Resumen El presente trabajo propone alcanzar una autoridad de certificación que brinde un nivel de seguridad en la emisión de certificados digitales en la Facultad de Matemática y Computación de la Universidad de la Habana y que funcione como base y experimento para un próspero resultado a nivel de universidad, donde todas las facultades internas se conecten a una autoridad raíz. Como resultado se ha desarrollo una integración de aplicaciones que proporcionan el flujo de acciones necesario para desplegar una infraestructura de llave pública que permita el intercambio seguro de información a través de canales pocos seguros como Internet, a partir del uso de mecanismos de seguridad criptográfica.

Abstract The present work proposes to achieve a certification authority which provides a security level in the issuance of digital certificates in the Faculty of Mathematics and Computing at the University of Havana and that it works as a base and experiment for a prosperous result at the university level, where all internal faculties will are connected to the root authority. As a result have an integration of applications that provide the flow of actions necessary to implement a public key infrastructure that allows the insurance of information through an unsecure channel through the Internet, as of use of cryptographic security mechanisms.

Palabras Clave
Seguridad, Servicios, Certificados

Keywords
Security, Services, Certificates

[1] *Instituto de Criptografía, Facultad de Matemática y Computación, Universidad de la Habana, Cuba, yavseny.roque@matcom.uh.cu, teresa.bernarda@matcom.uh.cu, yaidir.mustelier@matcom.uh.cu*
***Autor para Correspondencia, Corresponding Author**

Introducción

La Universidad de la Habana (UH) presenta la necesidad de informatizar sus procesos de trabajo, con servicios y tecnologías que ofrezcan certificados digitales y por consiguiente responder a la firma digital institucional, a la transmisión segura de información, a asegurar y controlar el acceso a servidores web y la posibilidad de agilizar los procesos administrativos mediante la firma y el estampado de tiempo. El Instituto de Criptografía (IC) se encuentra adscripto a la Facultad de Matemática y Computación de la Universidad de la Habana (MATCOM), con un objeto social dirigido a resolver problemas de seguridad en los servicios tecnológicos desplegados en las redes de la misma y colaborar en este sentido, con todas aquellas entidades del país que así lo requieran. Dentro de sus proyectos está, poner en marcha una infraestructura de clave pública (por sus siglas en inglés PKI) para la Facultad de MATCOM, que ayude a garantizar la seguridad de los datos intercambiados en cualquier tipo transmisión, ya sea entre usuarios o entre clientes y servidores, en aras de apoyar al proceso de informatización dentro la organización.

1. Normativas de las PKIs en Cuba

Nuestro país ha trabajado en las normativas que hacen posible la utilización de las técnicas criptográficas sobre certificados digitales. Dichos certificados se basan en infraestructuras de clave pública y proporcionan seguridad jurídica y tecnológica de acuerdo con lo establecido por la Resolución No 2 del 2016, del Ministro del Interior. [Interior, 2016] Esta resolución tiene como objetivo, fundar un ordenamiento que garantice la confianza en el empleo y validez de los certificados digitales y técnicas asociadas, brindando a su vez, seguridad a la información y a sistemas de informática y comunicaciones en el marco de la informatización de la sociedad. De igual forma, fue creada para regular las implementaciones

PKI que fuesen realizadas en el país y definir así las entidades del estado que fiscalizan estas implementaciones.

2. PKI

Una infraestructura de clave pública basa su importancia en garantizar la seguridad de la información en redes no seguras, como Internet. Es un sistema diseñado para generar certificados digitales de clave pública que permitan firmar digitalmente y cifrar datos para las organizaciones, garantizando el intercambio seguro de la información a partir del uso de una clave pública y otra privada. El uso de esta tecnología consiste en que el usuario del sistema se registra, obtiene su par de claves utilizando algoritmos asimétricos. La clave pública es utilizada a través de autoridades certificadoras que la hacen pública en los certificados digitales que emiten y publican, mientras que la clave privada se mantiene secreta y no puede ser publicada bajo ningún motivo.

Definición 1 *El RFC 4949 define PKI: como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados digitales basados en criptografía asimétrica. [Shirey, 2007]*

2.1 Principios fundamentales de una PKI

El concepto de PKI, en su totalidad, está basado en la confianza, pues la información que se transmite dentro de la infraestructura se encuentra en un marco de confiabilidad entre todas las partes. Dentro de este marco existen cuatro principios fundamentales que se deben cumplir. [Kuhn, 2001]

1. Integridad de los datos: este servicio está dirigido a evitar la modificación no autorizada o accidental de la información.

2. Confidencialidad: este servicio restringe el acceso a la información sensible únicamente a los usuarios que estén autorizados a consultarla.

3. Identificación y Autenticación: establece la validez del mensaje y de los participantes en la comunicación.

4. No-repudio: previene la negación por parte del emisor de haber emitido un mensaje cuando realmente lo ha hecho y que un receptor niegue su recepción cuando realmente lo ha recibido.

2.2 Componentes de una PKI

Una PKI puede estar conformada, primeramente, por las políticas de seguridad (PS) y por la declaración de prácticas de certificados (DPC) como elementos rectores en la organización de la misma, y luego por una autoridad de certificación raíz y una o varias autoridades de certificación subordinadas (ACs), autoridad/es de registro/s (AR), autoridad/es de validación, repositorio/s de certificados, entidades finales etc. Cada componente tiene un conjunto de funciones, las cuales pueden variar en dependencia del diseño que se realice. Esto hace posible que se puedan incluir otros tipos de componentes, como pueden ser: la autoridad de sellado o estampado de tiempo, que permite obtener una prueba de que un determinado dato existía en una fecha concreta y la autoridad de recuperación de claves, que es quien almacena y recupera archivos de clave PKCS #12 y contraseñas generados por la AC. [Lapuente, 2016]

2.3 Estructuras de datos

2.3.1 Certificados digitales

Los certificados digitales, también conocidos como certificados de clave pública o de identidad, son definidos como estructuras de datos que establecen una asociación entre un nombre, denominado nombre distinguido (por sus siglas en inglés, Distinguished Name (DN)) y la respectiva clave pública del usuario durante un periodo válido de tiempo. Los certificados proveen de autenticidad a los usuarios ya que son emitidos por una AC que verifica y confía plenamente en la identidad del usuario al que pertenece dicho certificado y manifiesta esta conformidad firmando el certificado con su clave privada y adjuntando dicha firma al final del mismo [Lapuente, 2016], [Suranjan Choudhury, 2014]

2.3.2 Lista de revocación de certificados

Una lista de revocación de certificados (por sus siglas en inglés, Certificate Revocation List (CRL)) es un archivo, con un sello de tiempo, firmada por una autoridad de certificación, que contiene una lista de los números de serie de los certificados que han sido revocados y que puede estar en un repositorio público a disposición de los usuarios. [R. Housley and Ford, 2002] Las CRL están protegidas por la firma digital del emisor, de manera que cualquier usuario puede verificar que el contenido de la misma no ha sido alterado desde su generación. [Cooper M, 2008]

3. Análisis de soluciones

Con la invención de la criptografía de clave pública y los certificados digitales algunas empresas predijeron la creación de un gran mercado en torno a las PKIs, el comercio electrónico y otros servicios que se podrían comenzar a desarrollar a través de Internet mediante el uso de protocolos seguros de comunicaciones. En el mercado podemos encontrar un gran número de soluciones PKI, algunas libres y gratuitas, otras de pago e incluso algunas desarrolladas a medida para soluciones concretas. Para dar solución al problema planteado en la introducción del presente documento y crear de una AC en la Facultad de Matemática y Computación de la Universidad de la Habana, se realizó un estudio del estado del arte de algunos paquetes de software de PKI no comerciales. Los software analizados fueron los siguientes: EJBCA (Enterprise Java Bean Certificate Authority), OpenCA, OpenXPKI, XCA y la plataforma PKI de Safelayer: KeyOne. La solución EJBCA fue la herramienta escogida para el desarrollo de esta investigación por las ventajas que se exponen a continuación, para

ellos el autor se basó en su sitio web oficial. [PrimeKey, 2019]

1. EJBCA demuestra una constante evolución, tanto en el ciclo de lanzamientos de nuevas versiones estables, así como de características funcionales en el software.

2. La página oficial del proyecto mantiene una actualización constante de todo lo relacionado con la herramienta. Tiene un equipo de desarrolladores activo y muestran una documentación extensa y bien elaborada.

3. Cuenta con numerosos casos de éxitos en instituciones con alto grado de responsabilidad.

4. Presenta alta escalabilidad, muy importante si se desea implementar una PKI en constante crecimiento.

5. Se adapta a las recomendaciones del RFC5280 y al uso de una licencia LGPL (GNU Lesser General Public License) que permite ser integrada casi sin ninguna limitación con cualquier programa propietario.

6. No solo soporta claves de firma RSA sino también las ECDSA (los algoritmos que se basan en la criptografía de curva elíptica son los preferidos entre los algoritmos base de la criptografía de clave asimétrica: ECDSA es uno de ellos).

7. Permite la integración de módulos criptográficos diferentes a los que usa su librería Bouncy Castle.

4. Diseño de la arquitectura de la solución

Uno de los objetivos más importantes a tener en cuenta en el diseño de una PKI, es determinar la arquitectura más adecuada para ofrecer facilidades en el uso de los certificados digitales a usuarios y administradores, flexibilizar las necesidades actuales y futuras de la organización y a la vez, garantizar un nivel elevado de seguridad hacia las componentes de la infraestructura. En la figura 1 se muestra la arquitectura de la PKI desarrollada, para ello se ha logrado la configuración de varios componentes, donde se pueden encontrar: la AC de MATCOM instalada en un servidor que también funge como AR, para el registro y validación de los datos de los usuarios, el servidor de validación, ofreciendo la consulta instantánea del estado de los certificados y el servidor de sellado de tiempo, como otro elemento de garantía y confianza. La AC cuenta con una base de datos local y un servidor LDAP que en conjunto utiliza para el almacenamiento y publicación de certificados, CRL, información de los usuarios y sus solicitudes de certificados, etc. Se tiene también un firewall que está configurado para que proteja del tráfico no autorizado a cada uno de los componentes de la PKI. Del mismo modo el diseño propone que cada usuario deba tramitar la emisión de su certificado digital mediante un administrador de la AR.

5. Definición de las ACs del sistema

Dentro de cada proceso de la solución existen múltiples actores que definen las acciones que se llevan a cabo al alcanzar un objetivo específico. La AC de MATCOM (ACMC) es un componente fundamental en la definición del correcto funcionamiento de la PKI. Ella es la encargada de emitir los certificados digitales a los usuarios finales para la protección de los canales de comunicación y los servicios desplegados en la facultad. Dentro de sus funciones está:

- Generar claves: crea el par de claves para equipos y aplicaciones, no sucede igual para los usuarios, ya que en esta solución se aplica la política de que sea el usuario quien genere su par de claves, para que este siempre tenga en su poder la llave privada.

- Emitir certificado: crea certificados digitales en formato X.509 v3.

- Publicar CRL: cambia el estado de los certificados en la base de datos, a no válidos para agregarlos a una futura CRL.

- Publicar certificado: crea archivo de certificado y lo deposita en un subdirectorio o repositorio en formato x.509v3 en codificación binaria

- Exportar claves: crea un archivo protegido por contraseña que contiene claves de usuario y certificado. Formato PKCS #12.

- Definir campos opcionales: Define los certificados con las extensiones: uso de clave y uso de certificado.

- Interactuar con la AR: Emite un certificado digital de acuerdo con la información proveída por la AR.

Por otro lado la AR de MATCOM (ARMC) es un elemento fundamental dentro de una PKI, ya que es la que permite verificar la identidad real de los usuarios y proporcionarles la información necesaria para realizar las gestiones oportunas con la autoridad de certificación. A continuación se explicarán las funciones relacionadas con la AR y el manejo de los certificados de las entidades finales:

- Registrar la identidad de un usuario: realiza la comprobación de la veracidad de los datos del solicitante.

- Interactuar con la BD: Registra en la DB local, las solicitudes de emisión de certificados.

- Gestionar el ciclo de vida de los certificados: revocación, expiración, renovación (extensión periodo de validez del certificado, respetando el plan de claves) y actualización de los datos del certificado.

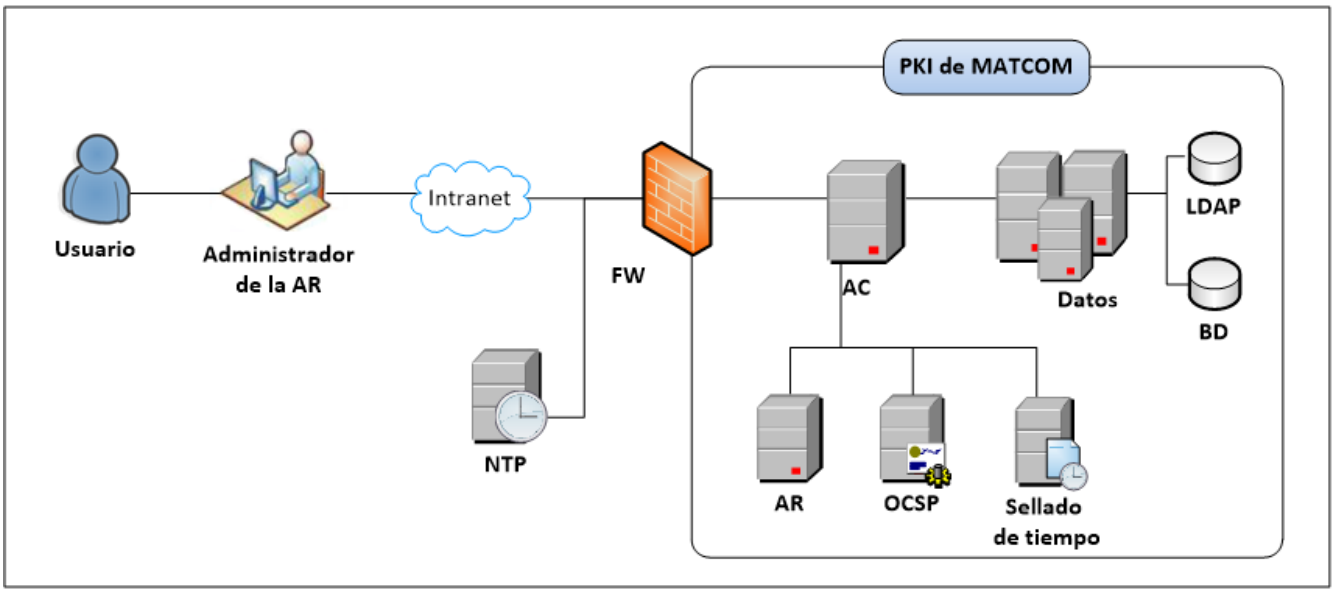

Figura 1. Arquitectura de la PKI de MATCOM

6. Plan de administración de los certificados digitales

Precisar un plan de administración de los certificados digitales durante todo su ciclo de vida implica la toma de decisiones sobre el registro, la solicitud, la emisión, la publicación y la revocación de los certificados digitales, también se establecerá la vigencia y tiempo de renovación de los mismos.

6.1 Selección del método de registro de certificados

La ARMC responderá al proceso de identificación y autenticación de usuarios y equipos (clientes y servidores) a los que se les asignará un certificado. Dicha AR estará conformada por los funcionarios del departamento de Recursos Humanos de MATCOM.

Para usuarios: El mecanismo de autenticación de la identidad inicial, se ejercerá sobre la base de la autenticación presencial, en la cual, el solicitante se deberá presentar físicamente en la ARMC para iniciar la solicitud del certificado. En caso de que exista la necesidad de generar certificados para usuarios externos a la facultad, el registro se hará de igual forma: bajo el principio de autenticación presencial y con la documentación requerida.

Para equipos (cliente y servidor): Los mecanismos de solicitudes de creación de certificado se desarrollarán a partir de que un administrador del nodo de la facultad presente una petición al administrador de la ACMC, acompañada de la fundamentación y alcance de la misma. Para ello, la administración de la ACMC producirá y entregará el certificado al solicitante en los formatos convenidos con el mismo.

6.2 Selección del método de solicitud de certificados

La política para las solicitudes de certificados al igual que las de los registros de certificados, va a variar en dependencia del tipo de entidad final que sea.

Para usuarios: Para definir este caso de uso, es importante tener en cuenta el diagrama de flujo de la Figura 2, donde se manifiesta lo siguiente: una vez que la ARMC dé de alta al nuevo usuario y le entregue sus credenciales, este podrá acceder desde su navegador web a la interfaz pública de EJBCA, a través de la dirección http://acmc.matcom.uh.cu para autenticarse y generar su par de claves. Consecutivamente, la ACMC verificar dichas credenciales a partir de la información registrada en la base de datos del sistema. Luego el usuario procede a generar su material criptográfico y envía su clave pública junto con sus datos de registro a la ACMC formando la solicitud de certificado. Con estos datos obtenidos, la ACMC valida la autenticidad e integridad del permiso de emisión y posteriormente genera y firma el certificado digital del titular, actualiza la base de datos, los logs del sistema y el repositorio. La ACMC termina enviando el certificado emitido al usuario a través de la interfaz pública. Por último, el usuario procede a obtener e instalar su certificado digital en formato PKCS#12, el cual estará protegido por una contraseña para garantizar su confidencialidad.

Para equipos (cliente y servidor): El proceso solicitud de certificado para equipos es más sencillo que el expuesto anteriormente, ya que es la ARMC quien genera el par de claves y las entrega al solicitante. De igual manera, la ACMC emite el certificado teniendo en cuenta el formato definido en la solicitud de certificación. Posteriormente le hace entrega oficial del certificado, al solicitante en cuestión.

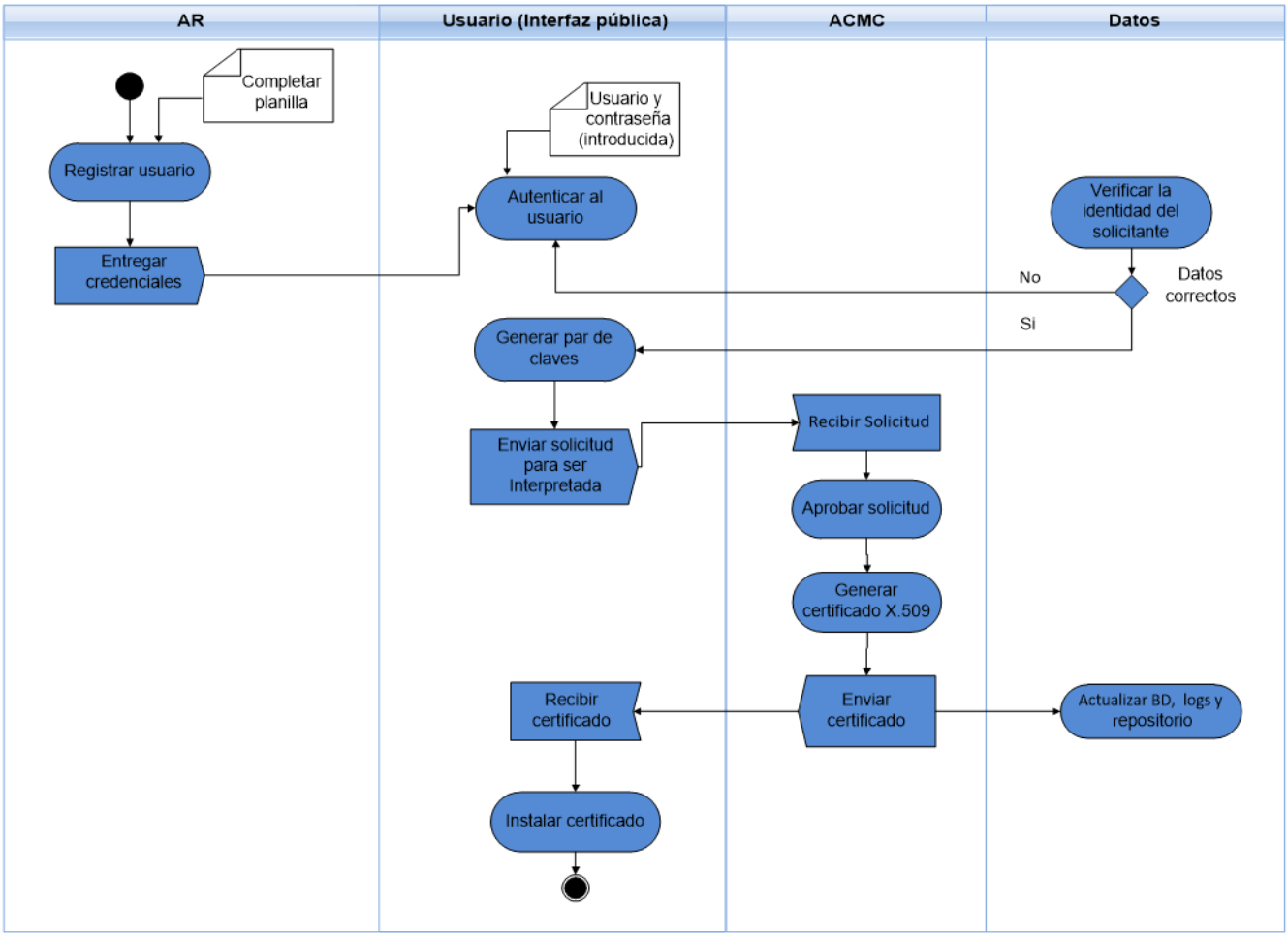

Figura 2. Diagrama de flujo del proceso de emisión de certificados.

6.3 Emisión de certificados

La emisión de certificados implica la autorización definitiva de la solicitud por parte de la ACMC. Todos los certificados iniciarán su vigencia en el momento de su emisión, salvo que se indique en los mismos una fecha y hora posterior a su entrada en vigor, que no será posterior a los 15 días naturales desde su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, temporal o definitiva, cuando se den las causas que motiven la suspensión o revocación del certificado.

6.4 Selección del método de publicación

Un servicio importante dentro de la PKI es la publicación de certificados digitales y la CRLs, para que usuarios del sistema, o incluso cualquier persona, pueda obtener dichos certificados y comprobar el estado de validez de los mismos. EJBCA proporciona páginas web, con enlaces directos a los certificados de las ACs y entidades finales. La ACMC cuenta con la configuración de un servicio de actualización de las CRLs de manera permanente, el cual se actualizará en un término no mayor a las veinticuatro (24) horas.

Igualmente, la solución ofrece el uso de un repositorio LDAP integrado a EJBCA, al que los usuarios podrán acceder desde un cliente LDAP. En la Figura 3 se muestra cómo, haciendo uso de la herramienta LDAP ADMIN se puede ver un certificado de un usuario añadido.

6.5 Selección del método de revocación y suspensión de certificados

El certificado será revocado por solicitud propia o a través del jefe del titular del certificado: en caso de que se desconfíe en la integridad de la clave privada o se perciba la utilización indebida de sus datos por un tercero, por resolución judicial o administrativa que lo disponga o por invalidez del tiempo de vigencia del certificado. La solicitud de revocación tendrá como mínimo la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del titular.
- Razón detallada para la petición de revocación.

La suspensión de un certificado será bajo las mismas circunstancias que se establecen para la revocación mencionada anteriormente, lo que en este caso, la invalidez del tiempo de

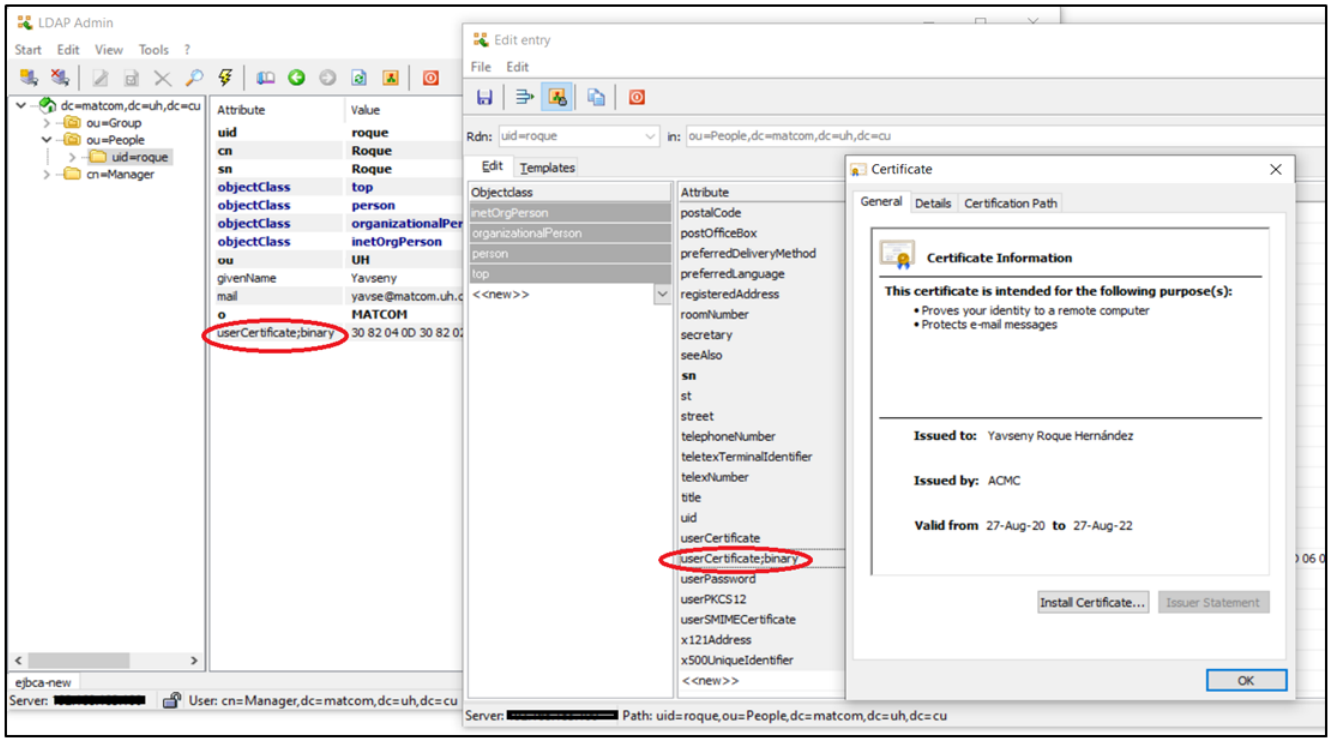

Figura 3. Vista de un certificado publicado en LDAP

vigencia del certificado va a ser a causa de alguna investigación, por lo que se procede a cancelar la validez del certificado digital durante un cierto periodo de tiempo, pudiendo volverse a levantar la suspensión siempre y cuando el certificado se encuentre dentro del periodo de validez.

7. Servicio de sellado de tiempo

Los servicios de sellado de tiempo se prestan de acuerdo con el artículo 9 de la Resolución No.2-2016 de la gaceta oficial [Interior, 2016] y a lo descrito por el estándar RFC-3161. [C. Adams, 2005] El servidor de sellado de tiempo será la tercera parte de confianza, quien dará fe, de la fecha y hora de una transacción, es decir, va a añadir el dato ?tiempo? a la transacción o al documento, por el cual las partes aceptan la validez temporal que se asocia a ese dato determinado. La Figura 4 muestra el proceso de sellado de tiempo, para ello, el usuario interactuará con una aplicación (p. ej. Abobe Acrobat) que mediará entre el servidor y el usuario para la obtención de la firma. Primeramente el cliente calcula el hash del documento a sellar. Este hash se envía en un mensaje de petición de token o de sellado de tiempo (TimeStamp Request) a una URL de la ACMC que responde a la autoridad de sellado de tiempo (AST). La AST recibe la petición, realiza un control de acceso del cliente y revisa si la petición está completa y correcta. Si el resultado es correcto la AST crea un sello de tiempo que contienen una combinación del hash con la marca de tiempo (fecha y hora obtenida de una fuente confiable), lo cual es firmado digitalmente con la clave privada de la ACMC. A este sello se le denomina respuesta de token o de sellado de tiempo (TimeStamp Reponse) y es enviado a la entidad solicitante. La AST mantiene un registro de los sellos emitidos para su futura verificación. El cliente debe validar la firma del sello y custodiarlo debidamente.

7.1 Validación del servicio

Para implementar la infraestructura sobre la cual se va a montar el servicio de sellado de tiempo se escogió un servidor asociado a la solución de Primekey: Signserver. Se establece para la fuente confiable de tiempo el protocolo NTP, el cual va a ser consultado por el servidor de estampado de tiempo, para sellar las solicitudes, siendo este el protocolo estándar para la sincronización de tiempo en la red. A continuación se muestra el resultado de una prueba de acceso hacia el servidor Signserver.

```
bin/signclient timestamp
http://tsa.matcom.uh.cu:8080/signserver/pr
ocess?workerName=TimeStampSigner

Salida de commando

2020-08-20 23:50:05,887 INFO
[TimeStampCommand] Got reply after 1945 ms
2020-08-20 23:50:06,075 INFO
[TimeStampCommand] TimeStampRequest
validated with status code: 0 (Operation
Okay)
```

Figura 5. Funcionamiento de TSA

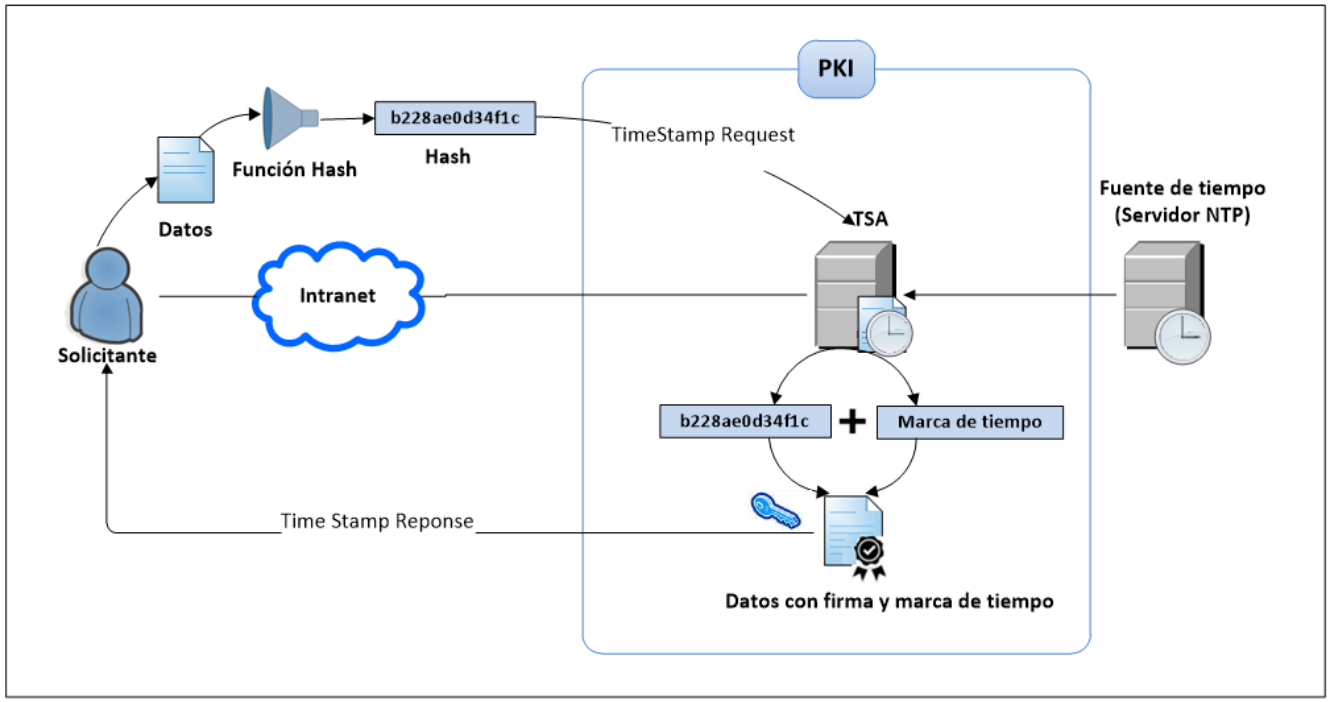

Figura 4. Esquema del servicio de sellado de tiempo

8. Servicio OCSP

OCSP (Online Certificate Status Protocol) El protocolo de comprobación del estado de un certificado en línea proporciona un método para determinar el estado de revocación de un certificado X.509 sin necesidad de utilizar CRLs. Este protocolo se describe en el RFC 6960 y está en el registro de estándares de Internet. El protocolo OCSP es uno de los más utilizados en la actualidad para realizar consultas sobre el estado de los certificados. Todas las respuestas OCSP tienen que estar obligatoriamente firmadas digitalmente por la autoridad de certificación que emitió el certificado en cuestión o por una entidad confiable para el usuario para firmar respuestas OCSP. La manera de acceder a este tipo de servicios suele venir definida en el propio certificado digital que se desea verificar. En la Figura 6 se puede ver el funcionamneto del protocolo OCSP utilizando OpenSSL, en una primera instancia se realiza la solicitud del estado de un certificado y en una segunda la respuesta emitida por el servidor.[Myers, 1999]

```
openssl ocsp -issuer ACMC.pem -CAfile ACUH.pem -cert
yavse.pem -req_text -url
https://acmc.matcom.uh.cu/ejbca/publicweb/status/ocsp

Salida de comando (en caso de que el certificado esté
revocado):

OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash:
999FC00189B49C42EA475AC9C23A7A44D21
          Issuer Key Hash:
4BCAB8DCC51EF0DEF5148E70B575004A7D9
          Serial Number: 75B78E99D2D4A3DC
    Request Extensions:
        OCSP Nonce:
4102B43FF682066257F4694A2D372D1BED
Response verify OK
        yavse.pem: revoked
        This Update: Jul 1 17:27:25 2020 GMT
        Reason: keyCompromise
        Revocation Time: Jul 1 17:26:46 2020 GMT
```

Figura 6. Funcionamiento del protocolo OCSP utilizando OpenSSL

9. Conclusiones

Esta solución es una propuesta de un diseño de PKI para contribuir al proceso de informatización de la Facultad de Matemática y Computación de la Universidad de la Habana, frente a las amenazas, ataques y riesgos en la trasferencia de información. La arquitectura definida afirma los niveles de seguridad y confianza requeridos por las directivas nacionales y los estándares internacionales, para el uso de los certificados digitales y su compatibilidad e interoperabilidad con las actuales y futuras aplicaciones utilizadas en la facultad. En resumen, el producto propone la integración y configuración de un conjunto de herramientas y servicios que le aportan funcionalidad a la infraestructura de llave pública: una autoridad de registro y certificación, un servidor LDAP, servicios de validación en línea y de sellado de tiempo, etc. Todo esto para garantizar la gestión de diferentes procesos elementales como la autenticación, autorización, validación de los recursos compartidos, la verificación instantánea del estado de los certificados, el no repudio de la información, entre otros. El servicio fue implementado en su totalidad con componentes

de software libre aprovechando las ventajas que otorga este paradigma.

Agradecimientos

Agradecer a mi esposo y mi niña por su comprensión, mis tutores, amigos y familiares.

Referencias

[C. Adams, 2005] C. Adams, S. F. (2005). Internet x.509 public key infrastructure cmp. *Technical report, IETF, United States*.

[Cooper M, 2008] Cooper M, Ankney R, M. A. G. S. A. C. (2008). Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. *IETF RFC 5208. http://tools.ietf.org/html/rfc5280*.

[Kuhn, 2001] Kuhn, D. e. N. (2001). Technology. an introduction to public key technology and the federal pki infrastructure. *U.S: Government.*, pages 15–21; 26–27.

[Lapuente, 2016] Lapuente, C. G. (2016). Implantación de un sistema de certificados.

[Interior, 2016] Ministerio, Interior. (2016). Resolución no.2.

[Myers, 1999] Myers, Ankney R, M. A. G. S. A. C. (1999). X.509 internet public key infrastructure, online certificate status protocol ocsp. *Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 2560*.

[PrimeKey, 2019] PrimeKey (2019). Ejbca integration guide.

[R. Housley and Ford, 2002] R. Housley, P. and Ford, W. (2002). X.509 public key infrastructure: Certificate and crl profile. rfc 3280.

[Shirey, 2007] Shirey (2007). Rfc 4949 (informational). internet security glossary, version 2. request for comments 4949.

[Suranjan Choudhury, 2014] Suranjan Choudhury, K. B. (2014). Public key infrastructure implementation and design. *John Wiley Sons, Inc., New York, USA, 2sd edition(ISBN 0764548794.)*.