UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Desarrollo de la nueva versión de la Autoridad Certificadora UNAMgrid

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Jhonatan Rafael Pontaza López

ASESOR DE INFORME

M.I. Aurelio Adolfo Millán Nájera

Ciudad Universitaria, Cd. Mx., 2016

AGRADECIMIENTOS

El problema siempre es empezar, pero ya entonado salen las letras y después de tanto pensar creo que no hay mejores palabras que las que nacen del corazón.

Desde que era pequeño mi sueño fue tener algo en la vida y pues veanme, por que con su apoyo directo o indirecto estoy aquí escribiendo lo último para obtener mi título profesional. Hay tantas personas que influyen en mi vida cotidiana que no quiero que pasen desapercibidos y recuerden que los quiero y los aprecio hoy y siempre.

Primeramente quiero agradecer a Dios que me ha permitido llegar hasta este punto de mi vida por lo que soy y siempre trato de ser una mejor persona aunque todos me conocen y sabran que soy muy gruñón pero es un defecto que me ayudó a ser lo que soy.

Quiero agradecerle a la persona que me dio la vida Ma. Susana López Velarde que sin su apoyo y sus esfuerzos por sacar mis estudios no estaría el día de hoy aquí, muchas gracias mamá por todos tus sacrificios y por siempre creer en mí y en las decisiones que he tomado.

A la Mtra. Angélica Lizbeth Barreto Zuñiga, por creer en mí y darme la oportunidad de ser parte de su equipo de trabajo aunque le he hecho pasar malos ratos, gracias por los consejos, las enseñanzas para poder ser un mejor profesionista y claro una mejor persona, pues si, por que por ella realicé éste trabajo ya que me apoyó en muchas partes del trabajo y en la redacción del mismo.

A mi novia Carolina Bazán Mosqueda, ya que siempre ha estado a mi lado, por que comparte mis sueños, alegrías, momentos difíciles que gracias a ella los he podido superar. Muchas gracias por ser parte de mi vida y caminar conmigo. También agradezco a su familia por su apoyo y comprensión en todo.

A mis tíos y abuelos que en los momentos de adversidad y soledad estuvieron a mi lado, apoyándome en todo momento, muchas gracias por todo.

Al Ing. Aurelio Adolfo Millán Nájera, por aceptar ser mi director universitario y ayudarme a corregir el trabajo hasta que quedara listo.

Además quiero dedicar el esfuerzo para la obtención del título profesional a todos ellos que son gente importante y muy querida, muchas gracias por su amor y por su entrega en cada uno de los papeles que tienen en mi vida.

Jhon.

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

Para obtener el título de ingeniero en computación por parte de la Facultad de Ingeniería y haciendo uso de la opción de titulación por trabajo profesional. En este documento plasmó las actividades que he realizado en el Departamento de Firma Electrónica Avanzada de la UNAM.

El Departamento de Firma Electrónica Avanzada de la UNAM está encargado de brindar a toda la comunidad certificados digitales para poder firmar digitalmente sus actas de calificaciones en el caso de profesores y en el caso de funcionarios firmar órdenes de pago, contrataciones, etc.

He participado en diversos proyectos, de los cuales he tomado la administración y la implementación de la nueva Autoridad Certificadora UNAMgrid, por lo que este documento describe las actividades de dicho proyecto.

En conjunto con el Departamento de Firma Electrónica he contribuido para garantizar la generación de certificados y mantener siempre actualizados los sistemas.

UNAMgrid es de vital importancia para los académicos e investigadores de México ya que con su certificado que se les entrega, ellos pueden acceder a los recursos computacionales para procesar la información que su proyecto demande.

CAPÍTULO I - DEPARTAMENTO DE FIRMA ELECTRÓNICA AVANZADA

CAPÍTULO I - DEPARTAMENTO DE FIRMA ELECTRÓNICA AVANZADA

El servicio de Firma Electrónica Avanzada proporcionado por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM a través del Departamento de Identidad y Firma Electrónica Avanzada "consiste en proporcionar certificados digitales a la comunidad universitaria para firmar electrónicamente en los sistemas de la UNAM que adopten el uso de la Firma Electrónica Avanzada"[1].

La Firma Electrónica Avanzada (FEA) está basada plenamente en los conceptos y fundamentos de la infraestructura de llave pública, con la finalidad de que las comunicaciones en Internet sean seguras.

La adopción de esta tecnología permite a las organizaciones y a las personas agilizar sus operaciones, aunque es necesario contar con algún mecanismo que permita establecer lazos de confianza entre las personas, la Infraestructura de Llave Pública (PKI) provee un método de identificación fuerte. Ésta permite construir un marco de confianza sobre un sistema basado en red (Internet, Intranet, Extranet) para las organizaciones, haciendo que las transacciones en Internet cuenten con niveles de seguridad equiparable o mejor que los que se ofrecen en la vida diaria.

Para cumplir con este propósito el 3 de octubre de 2005 se publicó el "Acuerdo por el que se Implementa el Uso de la Firma Electrónica Avanzada en la UNAM"[2].

I.1 OBJETIVOS

- Agilizar los procesos y reducir el tiempo de respuesta en los trámites universitarios mediante el uso de la Firma Electrónica Avanzada.
- Otorgar certeza y legalidad a los trámites electrónicos en un ámbito de modernidad y vanguardia tecnológica.
- Reducir los costos derivados del almacenamiento, traslado y uso de personal para estas actividades.
- Modernizar y actualizar los trámites relativos a los procesos involucrados en la FEA. Replantear el esquema de elaboración de trámites académico-administrativos en el ámbito universitario.
- Acercar a la comunidad universitaria a tecnología de vanguardia.

[1] Firma Electrónica Avanzada. Recuperado el 12 de mayo de 2016, de http://sistemas.tic.unam.mx/?q=firma_electronica

[2] Acuerdo de implementación de Firma Electrónica Avanzada, recuperado 12 de mayo de 2016, de http://www.fea.unam.mx/sites/default/files/archivos/acuerdo_para_la_implementacion.pdf

I.2 SERVICIOS

Los servicios del Departamento de Firma Electrónica Avanzada ofrecidos a los usuarios son:

- Proporcionar certificados digitales a los usuarios finales
- Capacitación para la generación de los certificados
- Capacitación a los usuarios vía telefónica y remota
- Revisión de los sistemas para la generación de certificados
- Herramientas para el análisis de los certificados (estatus del certificado y vigencia)

El Departamento de FEA empieza a dar un servicio de transferencia de conocimientos a las universidades que desean implementar la Firma Electrónica en sus planteles.

I.3 ESTRUCTURA ORGANIZACIONAL

I.3.1 DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

La Universidad Nacional Autónoma de México (UNAM) es la institución educativa de nivel superior en México más grande e importante de Latinoamérica, cuyas funciones sustantivas incluyen la difusión de la docencia, la investigación y la cultura.

La Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), "contribuye al logro de los objetivos de la UNAM como punto de unión de la comunidad universitaria para aprovechar los beneficios que las tecnologías de la información y las comunicaciones pueden aportar a la docencia, la investigación, la difusión de la cultura y la administración universitaria"[3].

Asimismo, la DGTIC tiene entre sus atribuciones, las de orientar a las entidades y dependencias universitarias en la gestión de infraestructura, soluciones de cómputo y telecomunicaciones para cumplir los objetivos del plan de desarrollo de la UNAM, así como asesorar en la adquisición y mantenimiento de equipos de cómputo y en el aprovechamiento óptimo de los recursos institucionales.

Como parte de sus responsabilidades está la de proporcionar a la comunidad universitaria a través de su experiencia en materia de cómputo avanzado y tecnologías de la información, soluciones que permitan que sus miembros cuenten con herramientas y aplicaciones que garanticen sus procesos y operaciones en la vida académica.

[3] Universidad Nacional Autónoma de México, 19 de abril de 2012. ¿Quiénes Somos? Recuperado 12 de mayo de 2016, de http://www.tic.unam.mx/mision.html

I.3.2 ORGANIGRAMA DGTIC

En la ilustración I.1, se puede observar que la DGTIC tiene diez áreas, una Subdirección, una Unidad Administrativa, una Secretaria Privada, dos Coordinaciones y cinco Direcciones, que a su vez están bajo la Dirección General del Dr. Felipe Bracho Carpizo.

Ilustración I.1 Organigrama DGTIC[4]

La Dirección de Sistemas y Servicios Institucionales (DSSI) cuenta con Departamentos y Coordinaciones entre los cuales destaca el Departamento de Firma Electrónica Avanzada:

- Departamento de Firma Electrónica Avanzada
- Departamento de Visualización y Realidad Virtual
- Supercómputo
- Voto electrónico

[4] Universidad Nacional Autónoma de México, 30 de noviembre de 2015, Recuperado 12 mayo de 2016 http://www.tic.unam.mx/organigrama.html

- Coordinación de Seguridad de la Información
- Centro de Datos

Es por ello que la DGTIC a través del Departamento de Firma Electrónica Avanzada, es responsable de la custodia y administración de la Autoridad Certificadora para los sistemas de la grid en la UNAM.

I.3.3 ORGANIGRAMA FEA UNAM

En la Ilustración I.2 - Organigrama FEA UNAM, se muestra la estructura del Departamento de Firma Electrónica Avanzada en la que se tiene un jefe de Administración de Aplicaciones que está a cargo de dos administradores de aplicaciones entre los cuales soy uno de ellos.

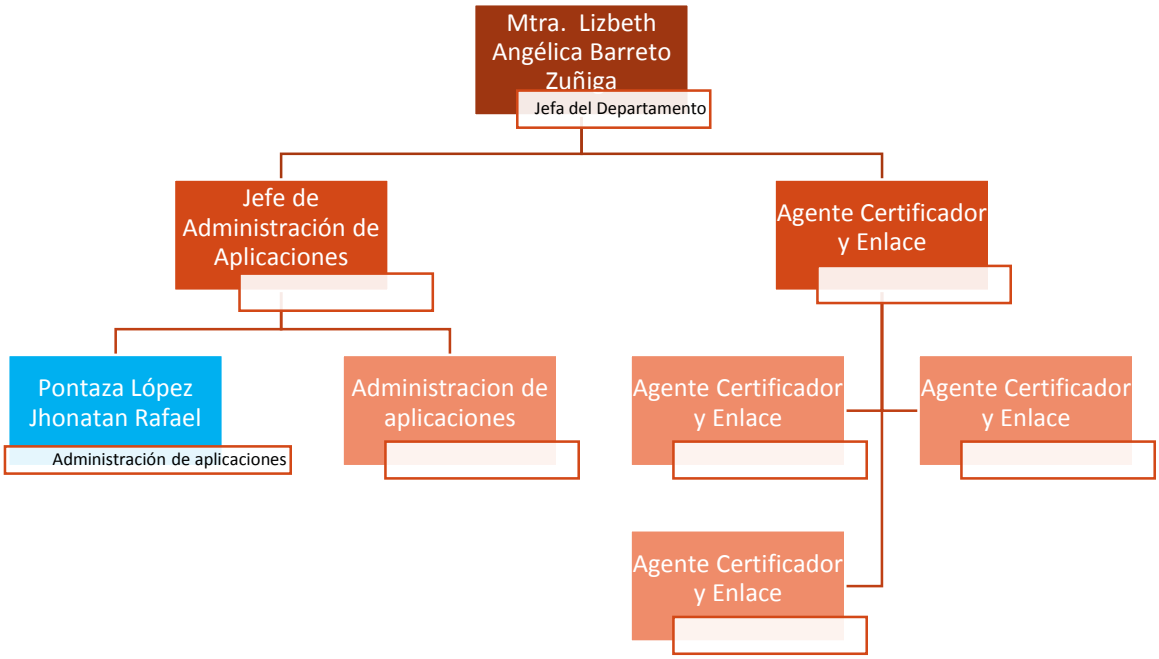


Ilustración I.2 - Organigrama FEA UNAM

CAPÍTULO II - CAMPO LABORAL

CAPÍTULO II - CAMPO LABORAL

II.1 INGRESO AL CAMPO LABORAL

En mi último semestre de la carrera de Ingeniería en Computación (2012-2), con el módulo de salida en Redes y Seguridad, inicié mis trámites para realizar mi servicio social en el Departamento de Firma Electrónica Avanzada.

Entre las actividades que desarrollaba como parte del servicio social estaban:

- La revisión de los servidores (memoria, procesos, conexiones).
- La generación de respaldos y su almacenamiento, así como las pruebas de dichos respaldos en sistemas alternos que tiene la FEA.
- Pruebas de emisión de certificados en la nueva Autoridad Certificadora que se estaba implementando
- Configuración de eventos en el ciclo de certificación de un usuario (envío de notificaciones, almacenamiento de certificados en un servidor independiente).

Al término de mi servicio, el 29 de agosto del 2012, la Jefa del Departamento de Firma Electrónica Avanzada me permitió ser parte de su equipo de trabajo de forma oficial, por lo que en septiembre del mismo año ingrese a laborar en el Departamento.

II.2 ADMINISTRADOR DE APLICACIONES

El puesto de administración de aplicaciones se desempeña bajo las órdenes del Jefe de Administración de Aplicaciones, como se muestra en el organigrama del Departamento de Firma Electrónica del capítulo anterior (ilustración I.1), para obtener este puesto se requieren personas que estén en los últimos semestres de las carreras de ingeniería en computación, telecomunicaciones o carreras afines.

Los conocimientos que debe tener la persona para adquirir el puesto son:

- Conocimientos en sistemas operativos Linux.
- Conocimientos en bases de datos y desarrollo de páginas web.
- Habilidades para desarrollar manuales operativos.

Estos conocimientos son necesarios para cumplir con las funciones del puesto de trabajo.

II.3 ACTIVIDADES DEL PUESTO DE TRABAJO

Mis actividades como administrador de aplicaciones en el Departamento de Firma Electrónica es mantener y administrar las aplicaciones que tienen que ver con la generación de certificados para los usuarios de la comunidad UNAM.

Entre mis principales funciones se encuentran:

- Monitoreo y mantenimiento.
- Apoyo a los agentes de enlace.
- Implementación de infraestructura en el centro de datos de DGTIC.
- Asesorías para la implementación de Autoridades Certificadoras (AC's)

II.3.1 MONITOREO Y MANTENIMIENTO

Para garantizar la disponibilidad de nuestros servicios se realizan inspecciones en cada servidor para ver el uso de los recursos (disco duro, CPU, memoria, conexiones, entre otros), de manera semanal. En caso de que presenten algún riesgo se tiene que revisar y dar solución al problema para mantener la disponibilidad del servicio.

Independientemente de que se hagan revisiones semanales cada periodo vacacional se suspende el servicio para prevenir algún incidente.

El resultado de esta actividad es garantizar, que tanto los servidores como los servicios estarán en línea y dando servicio ya que el sistema de Firma Electrónica es crítico.

Se generan respaldos de las bases de datos de acuerdo con el plan de contingencia que fue elaborado por parte del Departamento de Firma Electrónica, mi labor es almacenar y probar dichos respaldos en un ambiente alterno. Esta actividad se realiza a diario ya que el sistema es crítico, el resultado de esta actividad es para tener listo el plan de contingencia y se pueda seguir brindando el servicio.

II.3.2 APOYO A LOS AGENTES DE ENLACE

Los agentes de enlace dan soporte tanto a los agentes certificadores (Facultad, Posgrado, Instituto, Dirección, entre otros) como a los usuarios finales, mi labor es revisar el proceso de generación ya que en algún momento del trámite el agente puede tener problemas de red, o el usuario se equivoca el ingresar los datos, por consiguiente, la generación de certificados tiene que repetirse de nuevo y en algunos casos necesitan mi apoyo para poder cambiar de estatus el certificado e iniciar de nuevo el proceso.

El desarrollo de esta actividad es para brindarle al usuario de manera rápida y eficaz su certificado para firmar exitosamente.

II.3.3 IMPLEMENTACIÓN DE INFRAESTRUCTURA EN EL CENTRO DE DATOS DE DGTIC

Dado que fuimos la primera universidad en implementar Firma Electrónica a nuestros sistemas, me atrevo a decir que ha tenido éxito, algunas universidades se acercan al Departamento de Firma Electrónica para pedir asesoría o en algunos casos requieren que les brindemos el servicio de Firma Electrónica para después en una etapa de desarrollo les brindemos apoyo y conocimiento, y generen su propia infraestructura.

En este caso se genera una infraestructura alterna en el centro de datos de DGTIC, para esto tengo que generar una Sub Autoridad Certificadora (SubAC) con las características de la universidad (correo electrónico, nombre oficial de la universidad, alias de la universidad, etc.), todos estos datos los recaba la Jefa del Departamento de Firma Electrónica. Cuando se tienen los datos necesarios para hacer una SubAC, la genero y realizo las pruebas de interoperabilidad entre los diferentes servicios que se brindan.

Al final de esta actividad se tiene una SubAC en un sitio alterno, garantizando que sus certificados están avalados por nuestra Autoridad Certificadora.

II.3.4 ASESORÍAS PARA LA IMPLEMENTACIÓN DE AUTORIDADES CERTIFICADORAS

A inicios del año 2016, se inició el proceso de transferencia de conocimientos de Firma Electrónica a la Universidad Autónoma del Carmen (UNACAR)[5], esta etapa consiste en que dichas universidades en su propia infraestructura desarrollarán su AC y su componente de firma.

En esta etapa soy el encargado de transmitir los conocimientos adquiridos para que la UNACAR pueda generar su propia Autoridad Certificadora, personalización de los procesos de acuerdo a los que tenemos en firma. Así como toda la infraestructura que ésta conlleva (hardware, software, configuración e implementación).

[5] Firma electrónica Avanzada, una realidad en la UNCAR, Recuperado 19 mayo de 2016. http://www.unacar.mx/comunicacion_social_unacar/unacar/noticia.php?id=891

CAPÍTULO III - PROYECTOS EN EL DEPARTAMENTO DE FIRMA ELECTRÓNICA AVANZADA

CAPÍTULO III - PROYECTOS EN EL DEPARTAMENTO DE FIRMA ELECTRÓNICA AVANZADA

Desde mi ingreso al Departamento de Firma Electrónica he participado en varios proyectos que principalmente tienen que ver con Autoridades Certificadoras que no sólo es a nivel comunidad UNAM, sino también en universidades externas.

Uno de los proyectos que me asignaron como lo mencioné anteriormente es la administración de la Autoridad Certificadora UNAM, que consiste en gestionar y garantizar que los servicios estén siempre en línea.

El proyecto principal al que me asignaron en 2015 fue dar soporte a los usuarios para generar certificados en la Autoridad Certificadora UNAMgrid, cabe mencionar que el proyecto estaba a cargo de la Coordinación de Seguridad de la información/UNAM-CERT[6] y fue transferido a mi Departamento dado que nosotros tenemos más experiencia, en cuanto a certificados digitales.

Actualmente me desempeño como, líder de proyecto del desarrollo y configuración de la nueva plataforma de Autoridad Certificadora UNAMgrid y como el administrador de los sistemas grid de la UNAM en su plataforma actual.

Entre mis principales funciones se encuentran:

- Administrador principal de la Autoridad Certificadora (AC) y la Autoridad Registradora (RA) para los procesos de emisión, revocación y autorización de certificados digitales para los accesos autorizados a sistemas grid (ver III.7).
- Líder de proyecto técnico de la implementación de la nueva plataforma AC UNAMgrid.
- Responsable de la administración, configuración y gestión de los procesos de certificación de plataforma actual de AC UNAMgrid.
- Administración de las bases de datos y servidores que alojan a la AC UNAMgrid.
- Enlace técnico principal entre los administradores de los sistemas grid de los distintos centros e institutos de todo el país, adheridos a los diversos proyectos grid.
- Responsable técnico ante The Americas Grid Policy Management Authority (TAGPMA[7]) y ante la Interoperable Global Trust Federation (IGTF[8]) de los procesos técnicos y normatividad para el mantenimiento de la certificación como miembro activo de TAGPMA.

[6] Coordinación de Seguridad de la información, Recuperado 22 de mayo de 2016. http://www.seguridad.unam.mx/index.html
[7] TAGPMA Welcome, Recuperado 22 de mayo de 2016. http://www.tagpma.org/
[8] IGTF: Interoperable Global Trust Federation, Recuperado 22 de mayo de 2016. https://www.igtf.net/

III.1 UNAMgrid

III.1.1 ANTECEDENTES DEL PROYECTO

En marzo de 2006[9] se inició el proyecto de la Autoridad Certificadora UNAMgrid a cargo de la Coordinación de Seguridad de la Información/UNAM-CERT, el 22 de noviembre del 2007 UNAMgrid empieza a dar el servicio de generación de certificados[10].

El Departamento de Firma Electrónica Avanzada de la DGTIC recibió el proyecto de parte de la Coordinación de Seguridad de la Información/UNAM-CERT, en marzo del año 2014, para atender los procesos de certificación.

III.2 OBJETIVO DEL PROYECTO

Implementar una nueva versión de la Autoridad Certificadora UNAMgrid, así como nuevos procedimientos para la certificación de usuarios que utilizan recursos grid, para cumplir con los nuevos requerimientos de certificación dictados por el organismo internacional TAGPMA, para poder tener acceso a los recursos grid.

III.3 INTRODUCCIÓN

Los avances tecnológicos en materia de cómputo, así como los requerimientos por parte de los usuarios y las aplicaciones, avanzan de manera vertiginosa demandando cada vez más de equipos con mayor capacidad de procesamiento y memoria, así como de métodos más robustos de protección de los datos. Los sistemas cada vez más complejos requieren de un alto poder de cómputo que en ocasiones se ve rebasado por las capacidades instaladas de los usuarios en sus sitios de trabajo: bases de datos, sistemas complejos, cálculos matemáticos (cifrados) entre muchos otros, son ejemplos de sistemas que requieren de procesamiento de alto nivel que supera los recursos disponibles por un usuario o una institución promedio, es por ese motivo que se buscan alternativas de solución que permitan de manera conjunta acceder a mayores recursos para la realización de estudios e investigaciones a nivel nacional e internacional. Es así que surge el concepto de grid**.**

La grid es una tecnología que permite compartir recursos de cómputo administrados, a diversos grupos de trabajo en diferentes instituciones (a nivel nacional e internacional), dedicados a la investigación y a la docencia para procesar todo tipo de trabajos que requieran un poder de procesamiento más grande que el de una computadora convencional. Ésta, administrada por un sistema que permite el acceso de los mismos, facilitando los medios para su aprovechamiento.

[9] UNAMgridCPSv0.1a, Recuperado 22 de mayo de 2016. https://ca.unamgrid.unam.mx/grid/pdf/UNAMgridCPSv1a.pdf

[10] Certificado CA en formato CRT (browser import), Recuperado 22 de mayo de 2016. https://ca.unamgrid.unam.mx/pub/cacert/cacert.crt

Dada la importancia de los proyectos, programas y aplicaciones que se corren en la grid es necesario tener una manera confiable y segura que permita a los usuarios acceder a dichos recursos, es así que surge el concepto de "Autoridad Certificadora (AC)", esta entidad permite generar certificados digitales para identificar al usuario u organización (miembro de la grid) con altos niveles de confiabilidad y certeza. La grid utiliza este método para validar el acceso de sus miembros.

El principal objetivo de la Autoridad Certificadora UNAMgrid es proveer de un medio de autenticación confiable a los usuarios a través del uso de certificados reconocidos como válidos por las entidades que están integradas a la grid. La Autoridad Certificadora UNAMgrid, es el tercero confiable en este proceso, ya que realiza diversos procesos para validar en principio la identidad del usuario y posteriormente le proporciona un certificado digital que lo relaciona de manera inequívoca con su identidad, esto les otorga a los sistemas integrados a la grid la certeza de quienes se conectan y pueden hacer uso de sus recursos que son el poder procesar datos (consultas a bases de datos, almacenamiento, operaciones matemáticas, generar y reproducir simulaciones).

Entre los principales usos de la grid son proyectos de investigación, tanto nacionales como internacionales. En el caso me México el Instituto de Ciencias Nucleares[11] de la UNAM participa en diversos proyectos por lo que se mencionarán algunos proyectos institucionales y aplicaciones[12] que hacen uso de la grid:

- *ALICE.* La colaboración ALICE está construyendo un detector de iones pesados, dedicados a explotar la física única potencial de interacciones núcleo-núcleo a energías del LHC (Large Hadron Collider).
- *Pierre AUGER.* Está diseñado para estudiar la radiación de los rayos cósmicos en el régimen de ultra alta energía.
- *LEMDisFE*. Este proyecto se basa en el procesamiento de imágenes y modelos digitales, en apoyo a la ingeniería en alimentos ya que en un entorno de producción no es posible llevar a cabo experimentos
- *Siesmic Sensore Grid.* El propósito de esta aplicación es el de contribuir a la integración de diferentes señales, procedentes de las instituciones que operan redes de observación sísmica en el país, a fin de recibir en forma automática en tiempo real el envío de las señales generadas en diferentes regiones para sentar registro y procesamiento basado en la lombriz de tierra, sistema utilizado para la adquisición, almacenamiento, procesamiento e intercambio de información recibida de las estaciones de campo.

[11] Secretaría Técnica de Cómputo, Redes y Telecomunicaciones, Recuperado 23 de mayo de 2016. http://www.nuclecu.unam.mx/secretaria_de_computo_redes_y_telecomunicaciones.php
[12] escience MÉXICO, Recuperado 23 de mayo de 2016. http://www.e-science.unam.mx/index.jsp

III.4 MARCO TEÓRICO

Para poder brindar el servicio que tiene que ver con la generación, revocación y renovación de los certificados, primeramente, tuve que aprender el funcionamiento del sistema y las obligaciones que se deben de tener (ver III.4.1.1).

Una de las obligaciones es que UNAMgrid está abalada por el organismo internacional TAGPMA, que nos permite generar certificados para que los sistemas grid reconozcan a los usuarios. Otra de las obligaciones críticas es mantener actualizado el sitio de UNAMgrid.

III.4.1 THE AMERICAS GRID POLICY MANAGEMENT AUTHORITY

The Americas Grid Policy Management Authority (TAGPMA), es una federación de entidades de certificación (Autoridades Certificadoras) de grid en la región de América. Se rige por una Policy Management Authority (PMA), que está formada por miembros con responsabilidades en grid. El objetivo de la federación es facilitar las relaciones de confianza necesarias entre dominios para desplegar las redes en América y el resto del mundo.

A parte de TAGPMA existen dos federaciones más que comprenden la región de Europa, Medio Oriente y África que es la EUGridPMA[13] (por sus siglas en inglés European Policy Management Authority) y la región del Pacífico de Asia APGridPMA[14] (por sus siglas en inglés Asia Pacific Grid Policy Management Authority).

El organismo internacional TAGPMA está a la vanguardia en cuanto a seguridad de la información y revisa que todos los miembros cumplan con los estándares que establece dicho organismo (ver III.4.1.1), por lo que cada mes se hacen juntas para revisar el estatus de un miembro que esté en revisión por ejemplo como a situación de UNAMgrid que está en proceso de migración, dar de baja una Autoridad Certificadora por falta de actividad en las juntas de TAGPMA o algún acontecimiento importante en cuanto a seguridad informática (ver Tabla III. 2).

TAGPMA tiene diferentes miembros en toda América, por ejemplo, Estados Unidos tiene más de una Autoridad Certificadora, esto es por los recursos que pueden aportar a la grid. A continuación, en la Tabla III. 1, se muestran los miembros de TAGPMA más activos:

[13] EUGridPMA - Building Trust for Distributed IT Infrastructures for Research, Recuperado 22 de mayo de 2016. https://www.eugridpma.org/

[14] Asia Pacific Grid Policy Management Authority, Recuperado 22 de mayo de 2016. http://www.apgridpma.org/

Tabla III. 1 Miembros[15] de TAGPMA

Organización	País	Representante
DigiCert	USA	Scott Rea
GridCanada	Canada	Roger Impey
IBDS ANSP	Brazil	Sergio Lietti
InCommon	USA	Jim Basney
NCAR	USA	Steve Beaty
NCSA	USA	Jim Basney
NERSC	USA	Shreyas Cholia
NICS	USA	Victor Hazlewood
PSC	USA	Derek Simmel
REUNA	Chile	Sandra Jaque
SDSC	USA	Scott Sakai
UFF	Brazil	Vinod Rebello
ULAGrid	Venezuela	Alejandra Stolk
UNAM	Mexico	Jhonatan Pontaza
UNIANDES	Colombia	Andres Holguin
UNLP	Argentina	Paula Venosa
ESNet	USA	Dhiva Muruganantham
FNAL	USA	Irwin Gaines
OGF	USA	Alan Sill
OSG	USA	Jim Basney
REBCA	USA	Scott Rea
redCLARA	Chile/LAC	Luis A. Núñez
WLCG	Switzerland	Dave Kelsey
XSEDE	USA	Jim Marsteller

[15] TAGPMA Agenda 11 May 2016, Recuperado 23 de mayo de 2016. http://tagpma.es.net/wiki/bin/view/Main/TagPmaTv160511

III.4.1.1 REQUERIMIENTOS DE THE AMERICAS GRID POLICY MANAGEMENT AUTHORITY

En el año 2014 TAGPMA decidió que todos sus miembros sin excepción deberían hacer unas modificaciones a sus AC's, en la Tabla III. 2, se muestra el calendario establecido.

Tabla III. 2 Calendario[16] establecido por TAGPMA

2014	• Cambiar el algoritmo de firmado de la CRL a SHA-256 • Actualizar la versión de OpenSSL • Cambiar de algoritmo a SHA-256 en el tamaño de la llave de los certificados de usuario
2015	• Cambiar de algoritmo a SHA-256 en el tamaño de la llave raíz de la AC
2016	• Hacer pruebas en las aplicaciones de Grid para que se incorpore el servicio de OCSP[17] (Online Certificate Status Protocol)

III.4.2 INTEROPERABLE GLOBAL TRUST FEDERATION

IGTF (Interoperable Global Trust Federation)

La comunidad científica internacional está desplegando grids computacionales para el avance de la ciencia y la ingeniería. La promesa de grids computacionales globales requiere de políticas y procedimientos que identifiquen de forma fiable a los usuarios u organizaciones (suscriptores) y puedan tener acceso a recursos grid.

El IGTF es el organismo internacional encargado de dar una segunda aprobación de las AC´s ya que revisan la parte operativa y la forma correcta para la generación de los certificados.

Una vez que el IGTF aprueba una AC, éste agrega la información que es el número de serie del certificado de la autoridad, la dirección del sitio, la dirección para la descarga de la CRL, toda esta información se publica en un repositorio[18] del dominio público para que los administradores de la grid descarguen e instalen los certificados de cada AC en los diferentes servidores de la grid.

[16] IGTF time line statement on SHA-2 Secure Digest Mechanisms, Recuperado 22 de mayo de 2016. https://www.eugridpma.org/documentation/hashrat/sha2-timeline
[17] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, Recuperado 23 de mayo de 2016. https://tools.ietf.org/html/rfc6960
[18] IGTF Distribution of Authority Trust Anchors (PKI Certificate format), Recuperado 23 de mayo de 2016. https://dist.igtf.net/distribution/igtf/current/

El IGTF, genera un archivo con la información antes mencionada en diferentes formatos para la instalación en los servidores que prestan su poder de cómputo para la grid. Esos formatos son paquetes de instalación que son compatibles con servidores UNIX o Windows según sea el caso.

EL IGTF cada mes actualiza sus repositorios con la información de las AC´s que forman parte de la grid.

III.4.3 CRIPTOGRAFÍA

Según la tesis del Matemático Christopher Román Silva Sarabia

> *"La criptología se divide en dos ramas antagonistas, la criptografía y el criptoanálisis. La palabra criptografía de deriva de las palabras griegas criptos que quiere decir oculto, y graphein, que significa escribir. La critpgrafia entonces es el arte y ciencia de escribir en forma oculta las informaciones confidenciales. Por el contrario, el criptoanálisis es el encargado de romper las claves que se usan en los mensajes secretos, para que las personas que no son las destinatarias de los mensajes sean capaces de conocer su contenido."*[19]

La criptografía es una ciencia que aplica matemáticas complejas para aumentar la seguridad en mensajes; cuando se les aplica criptografía a los mensajes, éstos quedan inteligibles de tal manera que pueden estar a su estado normal siempre y cuando se le aplique el proceso inverso.

La criptografía trata sobre los diferentes mecanismos que permiten salvaguardar la privacidad y autenticación de la información que se almacena y/o trasmite entre entidades, típicamente dispositivos electrónicos. En condiciones normales la integridad de la información no sufre ningún daño cuando es intercambiada entre dos entidades tales como un emisor y un receptor. Sin embargo, cuando la información se transfiere a través de mecanismos no seguros, es posible que una tercera entidad pueda tener acceso a esta información, comprometiendo la integridad de la información. Esta tercera entidad o intruso puede entorpecer la comunicación entre emisor y receptor a través de uno de los siguientes ataques:

- Interrupción:
  La interrupción se presenta cuando el oponente captura y retiene toda comunicación entre emisor y receptor.
- Intercepción:
  La intercepción se presenta cuando el oponente sólo captura la información sin impedir la comunicación.
- Modificación:
  La modificación se presenta cuando el intruso altera la información y después la expide al receptor.

[19] Cristopher S, 2006. Criptografía y curvas elípticas, Recuperado 26 de mayo de 2016. De http://132.248.9.195/pdtestdf/0352941/Index.html

- Falsificación:
  La falsificación se presenta cuando el intruso envía información al receptor asiéndole creer a éste que viene del emisor.

III.4.3.1 CRIPTOGRAFÍA SIMÉTRICA

Con la criptografía simétrica se usa la misma clave para cifrar y descifrar. En la ilustración III. 1, se muestra el esquema de la criptografía simétrica:

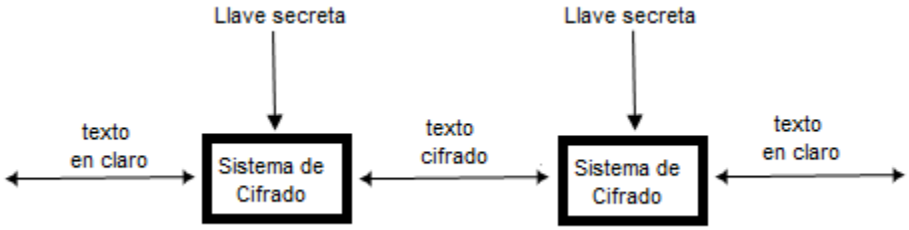


Ilustración III. 1 Criptografía simétrica

Ventajas y desventajas:

- ✓ Ventajas
  - Es rápido.
  - Es seguro.
  - El texto cifrado que resulta es del mismo tamaño que el texto plano.
  - El número de claves en la criptografía simétrica es, aproximadamente, el cuadrado del número de participantes y, por tanto, no tienen una buena escalabilidad en poblaciones muy numerosas.
  - Requiere una administración compleja de claves.
- ✓ Desventajas
  - Dado que la clave simétrica debe llegar al receptor, el cifrado simétrico está sujeto a la intersección.
  - No se ajusta a las firmas digitales.

III.4.3.2 CRIPTOGRAFÍA ASIMÉTRICA

La aparición de la criptografía asimétrica representó un cambio de paradigma muy importante en la materia, en 1976, cuando Whitfield Diffie y Martin Hellman la describieron explicando que implicaba la utilización de dos llaves: una publica y una privada. (Maiorano, 2009)[20]

A diferencia de los sistemas de llave secreta (criptografía simétrica), se involucran el uso de dos llaves; una para cifrar y otra para descifrar. De esta manera, lo que se cifra con una llave, sólo puede ser descifrada con la otra. Se le denomina sistema de llave pública debido a que una de las dos llaves puede hacerse pública, mientras

[20] Maiorano, Ariel Horacio, 2009. Criptografía: Técnicas de Desarrollo para Profesionales, 1era edición

que la otra se mantiene en secreto (llave privada) y donde, esta última llave es en la práctica computacionalmente imposible de obtener de la primera. Tal como se muestra en la ilustración III. 2.

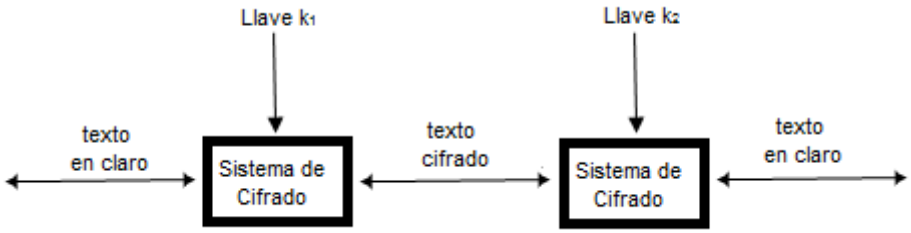


Ilustración III. 2 Criptografía asimétrica

Cuando nos referimos al tamaño de la clave, la situación es más compleja con la criptografía asimétrica que con la criptografía simétrica. Para la criptografía asimétrica se requiere de una longitud de clave mayor para lograr el mismo nivel de seguridad que en la criptografía simétrica. De igual manera no se puede hacer una comparación directa de las longitudes entre los algoritmos asimétricos.

Ventajas y desventajas:

- ✓ Ventajas
  - Con la criptografía asimétrica todo lo que se cifra con una clave (pública o privada) sólo puede ser descifrada con la otra clave (pública o privada).
  - Es seguro.
  - Debido a que no se necesita enviar una clave al receptor, la codificación asimétrica no sufre por la intercepción de claves.
  - El número de claves que se necesitan distribuir es el mismo de participaciones, de ahí que la criptografía asimétrica sirve bien en escalas de poblaciones muy grandes.
  - No tiene problemas complejos de distribución de claves.
  - No exige una relación previa entre las partes para hacer el intercambio de claves.
  - Soporta firmas digitales.
- ✓ Desventajas
  - Es relativamente lento.
  - Expande el texto cifrado

III.5 PUBLIC KEY INFRASTRUCTURE

PKI (Public Key Infrastructure) es el término utilizado para referirse a la infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de certificados digitales. Un certificado es un documento digital que identifica a una persona o institución.

El objetivo principal de la infraestructura PKI es dotar a los miembros de una corporación con los mecanismos básicos de seguridad que ésta necesita, esto es, autenticación, integridad, no repudio y confidencialidad, tanto para las conexiones Web (con el protocolo Secure Sockets Layer SSL) como para las comunicaciones a través de correo electrónico (con el protocolo Secure/Multipurpose Internet Mail Extensions S-MIME). El problema con la creación de una identidad en la que se pueda confiar, es encontrar una persona o institución que esté preparada para dar fe suficiente de la identidad.

Establecer identidades de confianza es un evento que tiene lugar en muchas formas cada día. Un ejemplo de esto puede ser el pasaporte, éste identifica a una persona y permite que una nación confíe en esa identidad con base en la entidad que lo expidió. La licencia de conducir es otro ejemplo de un certificado que brinda una identidad, al igual que demuestra el permiso para conducir un vehículo.

Existen algunas expectativas sobre la manera en ¿Cómo funcionan las autoridades que expiden identidades? La identidad emitida por una autoridad es válida en su terreno, pero probablemente no lo sea cuando se encuentre en otros dominios.

A partir de la experiencia, esperamos que la mayoría de las identidades sean expedidas por un período finito de tiempo y que, usualmente requieran un proceso de revocación cuando termine el período de validez. Esta restricción es sensible en el terreno de las identidades que no son digitales, evita que la identidad supere el tiempo de vida del poseedor y permite que los derechos asociados (como conducir un automóvil) se revaliden periódicamente. El proceso de renovación suele ser más simple que el proceso original de solicitud y, con frecuencia, usará la versión anterior que existe de la misma identidad para reducir la prueba que se requiere para validarla cuando se renueva.

Es por eso que una PKI da la certeza de que el usuario u organización es quien dice ser.

III.5.1 PKI Y ASPECTOS DE SEGURIDAD

Si una PKI se basa en la criptografía de clave pública, esto indica que una PKI contiene las siguientes propiedades de seguridad:

- *Autenticación de usuarios.* Sirve para asegurarse de la identidad de un usuario, ya sea como signatario de documentos o para garantizar el acceso

a servicios distribuidos en la red, ya que sólo el usuario puede conocer su clave privada, evitando así la suplantación.

- *No repudio.* Esto sirve para cuando un usuario firme o acceda a recursos y se niegue o se retracte de haberlo hecho.
- *Integridad.* Esto sirve para prevenir la modificación deliberada o accidental de la información durante su transporte, almacenamiento o manipulación.
- *Confidencialidad.* Esto sirve para mantener la información en secreto.

III.6 PROBLEMÁTICA

Conforme al calendario establecido por TAGPMA (Tabla III. 2), se empezó a planear y a desarrollar un plan de trabajo para cumplir con los requerimientos de TAGPMA.

De acuerdo con los requerimientos solicitados, realicé un estudio para determinar la situación de la actual Autoridad Certificadora UNAMgrid. Primeramente, revisé la infraestructura tanto software como hardware para determinar la viabilidad de actualizar el sistema.

Uno de los principales problemas fue el software (OpenCA v 0.9.2[21]) que se tiene actualmente en producción es obsoleto, ya que no se le dio mantenimiento, estudié y analicé el procedimiento para poder actualizar la versión de OpenCA ya que la versión más reciente en el año 2015 es OpenCA v 1.5.1[22]. Otro problema que encontré es el tiempo para cumplir con el calendario establecido y por lo tanto no se lograría cumplir con los requerimientos solicitados.

Debido a la amplia experiencia que se tiene en materia de Firma Electrónica en la UNAM y dado que se tiene la oportunidad de brindarle al proyecto una mejor infraestructura se decidió migrar a una nueva plataforma que se llama EJBCA[23] (Enterprise Java Beans Certificate Authority).

Primeramente, hay que saber que la actual UNAMgrid está basada en el esquema básico de una PKI (Public Key Infrastructure).

[21] OpenCA Guide for Versions 0.9.2+, Recuperado 25 de mayo de 2016. http://www2.openxpki.org/docs/guide/html_chunked/

[22] OPEN SOURCE PKI MANAGEMENT SOFTWARE, Recuperado 25 de mayo de 2016. https://www.openca.org/projects/openca/

[23] EJBCA PKI CA, Recuperado 25 de mayo de 2016. https://www.ejbca.org/

III.7 ESTADO ACTUAL UNAMGRID DE PRODUCCIÓN

Para poder desarrollar el proyecto hay que entender cuáles son los elementos que tiene UNAMgrid. El 24 de mayo de 2016 se tenía en producción la siguiente infraestructura.

III.7.1 OPENCA

OpenCA es una organización no lucrativa de software abierto para proyectos relacionados con PKI. UNAMgrid está basada en este software con la versión 0.9.2 que fue creada en el año 2006, por lo que hasta el año 2015 la Coordinación de Seguridad de la Información/UNAM-CERT no le dio las actualizaciones correspondientes. Con el calendario de TAGPMA algunos de sus requerimientos no se podrían cumplir.

Realicé una serie de investigaciones para poder actualizar dicho software uno de los problemas que enfrenté es el tiempo, ya que se tenía que actualizar toda la infraestructura y eso llevaría más tiempo que migrar a una nueva infraestructura que ya tenía dominada.

La actual Autoridad Certificadora UNAMgrid consta de dos componentes una RA (*Autoridad Registradora*) y una AC (*Autoridad Certificadora*), que forma parte modelo básico de una PKI. Estos dos componentes son independientes e incomunicados entre ellos.

En la Ilustración III. 3, se muestran los componentes que son 2 servidores que están en sitios diferentes e incomunicados entre ellos, cada servidor tiene su propia base de datos.

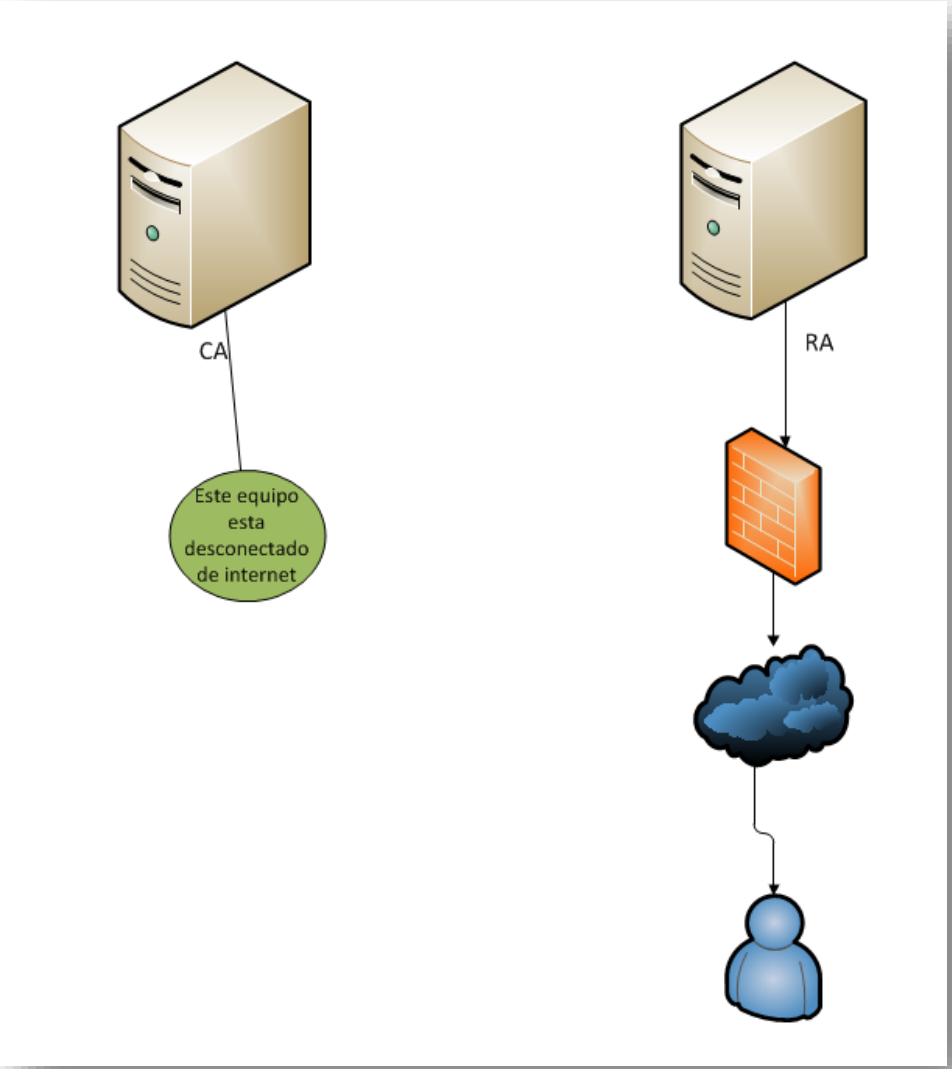


Ilustración III. 3 Infraestructura UNAMgrid AC

III.7.2 COMPONENTES DE UNAMGRID ACTUAL

Los elementos que componen la infraestructura de llave pública (PKI) actual son:

- Autoridad Certificadora (AC). Está alojada en un servidor que esta fuera de línea, firma las peticiones de los usuarios para generar certificados tanto de usuario como de servidor (ver III.7.4.2)
- Autoridad Registradora (RA). Es un servidor que se encuentra conectado a la red y por el cual los usuarios hacen las peticiones de certificados (ver III.7.4.1).

III.7.3 TIPOS DE CERTIFICADOS

En UNAMgrid existen dos tipos de certificados, actualmente, el estándar es el X.509.v3 como está definido por RFC 3280[24].

1. *Certificados de Usuario.* Estos certificados se entregan a los usuarios y son para autenticarse a los sistemas grid
2. *Certificados de Servidor.* Son para los servidores que brindan su poder de cómputo de procesamiento. Los certificados de servidor sólo pueden ser solicitados por los administradores de la grid.
3. *Certificado de AC.* Es el certificado que firma los certificados tanto de usuario como se servidor. Este certificado está en la AC que esta fuera de línea.
4. *Certificate Revocation List (CRL).* Es un certificado que contiene la lista de todos los certificados revocados por UNAMgrid.

III.7.3.1 CERTIFICADO DE LA AUTORIDAD CERTIFICADORA

El certificado de la AC es el que firma los certificados tanto de usuario como de servidor, este certificado fue creado antes de la aprobación y verificación de TAGPMA y del IGTF. La llave pública es del dominio público y se encuentra en la página web de UNAMgrid[25].

Este certificado se tiene que descargar e instalar en el navegador del usuario que solicitará un certificado, es un requerimiento tenerlo instalado en el almacén de certificados del navegador, ya que algunos navegadores no descargan el certificado del usuario firmado por dicha AC y si no lo descarga no contiene la cadena de certificación correspondiente. Dicho certificado tiene las siguientes características:

- Algoritmo de cifrado RSA 2048 (Rivest, Shamir y Adleman)
- Atributo de AC que permite el firmado de certificados
- Dirección para la descarga de la CRL
- Duración de la AC 10 años

En la Ilustración III. 4, se muestran los atributos del certificado de la AC actual. Esta información se obtuvo con un comando de OpenSSL[26] (software libre basado en Secure Sockets Layer).

[24] Internet X.509 Public Key Infrastructure, Recuperado 24 de mayo de 2016. https://www.ietf.org/rfc/rfc3280.txt
[25] Get CA certificate, Recuperado 25 de mayo de 2016. https://ca.unamgrid.unam.mx/pub/cacert/cacert.crt
[26] OpenSSL, Recuperado 25 de mayo de 2016. https://www.openssl.org/

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=MX, O=UNAMgrid, OU=UNAM, CN=CA
        Validity
            Not Before: Nov 23 01:09:23 2007 GMT
            Not After : Nov 20 01:09:23 2017 GMT
        Subject: C=MX, O=UNAMgrid, OU=UNAM, CN=CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:6c:e9:d4:2c:38:b2:7c:cf:c7:22:0b:b0:0a:
                    56:9b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                73:35:B7:8F:77:27:F2:6C:4E:EE:E7:5C:61:35:31:AF:F0:04:AF:99
            X509v3 Authority Key Identifier:
                keyid:73:35:B7:8F:77:27:F2:6C:4E:EE:E7:5C:61:35:31:AF:F0:04:AF:99

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            Netscape Comment:
                UNAMgrid Certification Authority Certificate
            Netscape CA Policy Url:
                https://ca.unamgrid.unam.mx/pub/policy.html
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://ca.unamgrid.unam.mx/pub/crl/cacrl.crl

            Netscape Revocation Url:
                http://ca.unamgrid.unam.mx/pub/crl/cacrl.crl
    Signature Algorithm: sha1WithRSAEncryption
         9f:c4:c3:e0:bc:07:23:ac:f7:7b:94:d8:b2:7a:8b:bf:41:04:
```

Ilustración III. 4 Certificado de la AC visto con la herramienta de OpenSSL

III.7.3.2 CERTIFICADOS DE USUARIO

Los certificados de usuario son entregados a los usuarios que colaboran en algún proyecto aprobado por los administradores, estos certificados sirven para poder identificarse ante la Grid para poder procesar sus trabajos. Dichos certificados tienen las siguientes características:

- Algoritmo del certificado SHA-256 (Secure Sash Slgorithm)
- Firma digital
- Sin repudio
- Cifrado de clave
- Cifrado de datos
- Autenticación del cliente
- Correo seguro
- Firma de código
- CRL
- Vigencia 1 año

En la Ilustración III. 5, se muestra un certificado de usuario, esta información se obtuvo con un comando de OpenSSL.

```
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number: 516 (0x204)
  Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=MX, O=UNAMgrid, OU=UNAM, CN=CA
      Validity
          Not Before: Aug 31 18:56:51 2015 GMT
          Not After : Aug 30 18:56:51 2016 GMT
      Subject: C=MX, O=UNAMgrid, OU=DGSCA UNAM CU, CN=Fernando Ortiz
      Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
              Public-Key: (2048 bit)
              Modulus:
                  00:bb:ad:76:55:52:7c:86:bf:01:ca:ae:3f:72:f5:
                  6f:21
              Exponent: 65537 (0x10001)
      X509v3 extensions:
          X509v3 Basic Constraints: critical
              CA:FALSE
          Netscape Cert Type:
              SSL Client, S/MIME, Object Signing
          X509v3 Key Usage: critical
              Digital Signature, Non Repudiation, Key Encipherment,
              Data Encipherment
          X509v3 Extended Key Usage:
              TLS Web Client Authentication, E-mail Protection,
              Code Signing
          Netscape Comment:
              User Certificate
          X509v3 Subject Key Identifier:
              23:20:55:61:C4:A2:2B:C3:30:A1:F8:49:5E:FA:86:84:AE:ED:2C:F7
          X509v3 Authority Key Identifier:
              keyid:73:35:B7:8F:77:27:F2:6C:4E:EE:E7:5C:61:35:31:AF:F0:04:AF:99
          X509v3 Subject Alternative Name:
              email:luis_saldierna@yahoo.com.mx
          X509v3 Issuer Alternative Name:
              email:camanager@ca.unamgrid.unam.mx
          Netscape CA Revocation Url:
              http://ca.unamgrid.unam.mx/pub/crl/cacrl.crl
          Netscape Revocation Url:
              http://ca.unamgrid.unam.mx/pub/crl/cacrl.crl
          X509v3 CRL Distribution Points:
              Full Name:
                URI:http://ca.unamgrid.unam.mx/pub/crl/cacrl.crl
          X509v3 Certificate Policies:
              Policy: 1.2.840.113612.5.4.2.5.2.2.1.1.0
  Signature Algorithm: sha256WithRSAEncryption
```

Ilustración III. 5 Certificado de usuario, revisado con OpenSSL

III.7.3.3 CERTIFICADOS DE SERVIDOR

Los certificados de servidor sólo se expiden a los administradores para que la grid pueda identificar los servidores que comparten sus recursos, así como para autenticar a los usuarios. Dichos certificados tienen las siguientes características:

- Algoritmo del certificado SHA-256
- Firma digital
- Cifrado de clave
- Cifrado de datos
- Autenticación del servidor
- Autenticación del cliente
- Correo seguro
- Firma de código
- CRL
- Vigencia 1 año

En la Ilustración III. 6, se muestra un certificado de tipo servidor con OpenSSL:

```
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number: 506 (0x1fa)
  Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=MX, O=UNAMgrid, OU=UNAM, CN=CA
      Validity
          Not Before: Mar 27 19:14:22 2015 GMT
          Not After : Mar 26 19:14:22 2016 GMT
      Subject: C=MX, O=UNAMgrid, OU=DGSCA UNAM CU, CN=fesc06.lemdist.unam.mx
      Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
              Public-Key: (2048 bit)
              Modulus:
                  00:d2:13:53:0a:9d:2a:a3:0e:06:fc:ea:75:9f:15:
                  2b:21
              Exponent: 65537 (0x10001)
      X509v3 extensions:
          X509v3 Basic Constraints: critical
              CA:FALSE
          X509v3 Key Usage: critical
              Digital Signature, Key Encipherment, Data Encipherment
          X509v3 Extended Key Usage:
              TLS Web Server Authentication, TLS Web Client Authentication,
              E-mail Protection, Code Signing
          X509v3 Subject Key Identifier:
              DF:48:CD:7D:7B:6A:2A:82:78:D3:93:12:ED:4B:E1:FB:0A:D0:D2:5D
          X509v3 Authority Key Identifier:
              keyid:73:35:B7:8F:77:27:F2:6C:4E:EE:E7:5C:61:35:31:AF:F0:04:
          X509v3 Subject Alternative Name:
              DNS:fesc06.lemdist.unam.mx
          X509v3 Issuer Alternative Name:
              email:camanager@ca.unamgrid.unam.mx
          X509v3 CRL Distribution Points:
              Full Name:
                URI:http://ca.unamgrid.unam.mx/pub/crl/cacrl.crl
          X509v3 Certificate Policies:
              Policy: 1.2.840.113612.5.4.2.5.2.2.1.1.0
  Signature Algorithm: sha256WithRSAEncryption
```

Ilustración III. 6 Certificado de servidor, revisado con OpenSSL

III.7.3.4 CERTIFICATE REVOCATION LIST

Certificate Revocation List (CRL) es la lista de certificados revocados, que revocan los administradores o los mismos usuarios. Un usuario podrá revocar su certificado si ve comprometido su certificado, o por suplantación de identidad. Dicha lista tiene las siguientes características:

- Algoritmo del certificado SHA-256
- Versión 2
- Vigencia 30 días

En la Ilustración III. 7, se muestra la CRL, vista desde comandos de OpenSSL, donde se muestra la información antes mencionada:

```
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=MX/O=UNAMgrid/OU=UNAM/CN=CA
        Last Update: Mar 18 15:17:35 2016 GMT
        Next Update: Apr 17 15:17:35 2016 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:73:35:B7:8F:77:27:F2:6C:4E:EE:E7:5C:61:35:31:AF:F0:04:AF:99

            X509v3 CRL Number:
                272
Revoked Certificates:
    Serial Number: 23
        Revocation Date: Nov 19 18:20:35 2014 GMT
    Signature Algorithm: sha256WithRSAEncryption
         7f:05:ad:cb:f9:7c:c4:00:8b:7b:23:bc:bc:e0:df:b1:0e:1d:
         31:d9:c0:c8
```

Ilustración III. 7 CRL vista con comandos OpenSSL

III.7.4 INFRAESTRUCTURA

A continuación de muestra las especificaciones de cada servidor tanto en software como hardware.

III.7.4.1 AUTORIDAD DE REGISTRO

Registration Authority (RA) es una máquina virtual que se encuentra alojada en las oficinas del Departamento de Firma Electrónica Avanzada.

Sus características tanto en hardware como en software son:

- Red Hat Enterprise 3 (Taroon Update 9)
- OpenCA Server Versión 0.9.2
- Postgres[27] 8.1.2
- OpenSSL 0.9.8e 23 Feb 2007
- Apache2[28]
- Máquina Virtual (MV)
    - Virtualizador: VMware[29]
    - 1 Gb de RAM

III.7.4.2 AUTORIDAD CERTIFICADORA

La AC es la autoridad que procesa las solicitudes de los usuarios en ésta se encuentra alojada la llave que firma los certificados, esta autoridad no cuenta con conexión a internet. La AC está en una computadora de escritorio que se encuentra alojada en las oficinas del Departamento de Firma Electrónica Avanzada.

Sus características tanto en hardware como en software son:

- Ubuntu Desktop 7.10
- OpenCA Server Versión 0.9.2
- Postgres 8.2.6
- OpenSSL 0.9.8e 23 Feb 2007
- Apache 2
- Computadora de escritorio
    - Procesador pentium 4
    - 512 Mb RAM

[27] PostgresSQL, Recuperado 25 de mayo de 2016. https://www.postgresql.org/
[28] Apache 2, Recuperado 25 de mayo de 2016. https://httpd.apache.org/
[29] VMware, Recuperado 25 de mayo de 2016. http://www.vmware.com/mx

III.7.5 PROCESO DE CERTIFICACIÓN

Para el proceso de certificación los líderes de proyecto, tienen que capacitar a los usuarios finales (Investigadores, Académicos, Alumnos), para poder utilizar los recursos grid y solicitar un certificado a la UNAMgrid. Una vez terminado el curso de capacitación los usuarios finales, tienen que realizar su solicitud personal de un certificado. A continuación, veremos el procedimiento para generar un certificado.

III.7.5.1 SOLICITUD DE UN CERTIFICADO

La solicitud de un certificado se realiza en la RA que es la autoridad que registra las peticiones de los usuarios, esta autoridad es del dominio público. Para solicitar un certificado se realizan los siguientes pasos:

1. Primeramente, se accede al sitio web de UNAMgrid CA https://ca.unamgrid.unam.mx/
   En la Ilustración III. 8, se muestra la página de inicio de la versión actual de UNAMgrid.

Ilustración III. 8 Página de inicio UNAMgrid actual

2. Una vez que se entra a la página, se va al menú, se busca el apartado “Users” y se selecciona “Request Certificate”
   El usuario seleccionará el tipo de certificado que necesite, que es certificado de usuario o certificado de servidor

III.7.5.1.1 SOLICITUD DE CERTIFICADO DE USUARIO

En la Ilustración III. 9, se muestra el formulario para solicitar un certificado de usuario, a continuación de describen los campos que deberá llenar el usuario:

- *Name.* En este campo el usuario tecleará su nombre completo tal y como viene en su identificación oficial que presentará junto con la carta de intención.
- *ID Card Number.* En este campo el usuario pondrá el número de su identificación oficial (por ejemplo, su número de cuenta de la UNAM, o el número de identificación del INE).
- *Address.* En este campo el usuario tecleará su dirección personal o la dirección del proyecto donde labora el usuario.
- *E-Mail.* En este campo el usuario tecleará una dirección valida de correo electrónico.
- *Common Name (CN).* Este campo no acepta acentos, caracteres especiales y deberá ser alusivo al nombre de usuario final.
- *PIN.* Este campo debe tener al menos 12 caracteres, una mayúscula y un número.

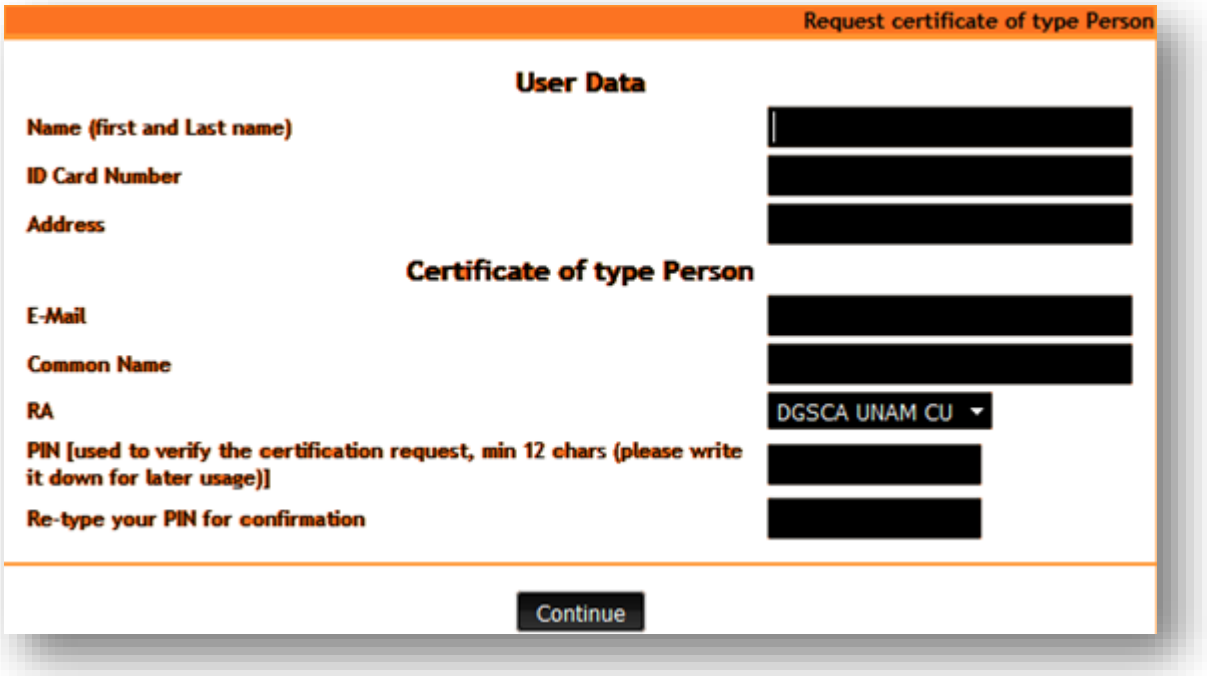


Ilustración III. 9 Formulario para solicitar un certificado de usuario.

III.7.5.1.2 SOLICITUD DE CERTIFICADO DE SERVIDOR

En la Ilustración III. 10, se muestra el formulario para solicitar un certificado de servidor, a continuación de describen los campos que deberá llenar el usuario:

- *E-Mail.* En este campo el usuario tecleará una dirección valida de correo electrónico.
- *Hostname. (Common Name CN).* En este campo el usuario pondrá el nombre del servidor, este campo no acepta espacios, mayúsculas, caracteres especiales.
- *PIN.* Este campo debe tener al menos 8 caracteres, una mayúscula y un número.

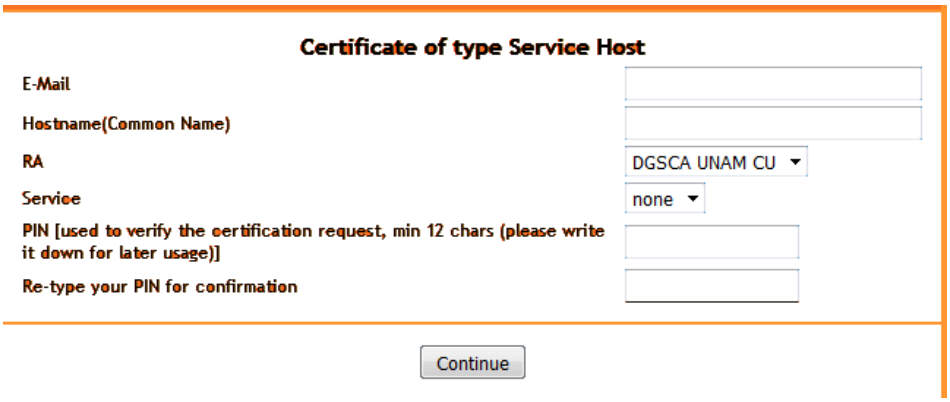


Ilustración III. 10 Formulario para solicitar un certificado de servidor.

III.7.5.2 REQUISITOS PARA PROCESAR LA SOLICITUD

Una vez realizada la solicitud el sistema notifica a los administradores mediante un correo electrónico automático, que contiene los datos del solicitante: Nombre del Usuario, correo electrónico, tipo de certificado, DN (Nombre de Dominio) del usuario que es la unión de todos los campos que lleno previamente en el formulario, así como la información del nombre de la AC y la fecha de solicitud que viene implícita en el correo electrónico, (véase Ilustración III. 11).

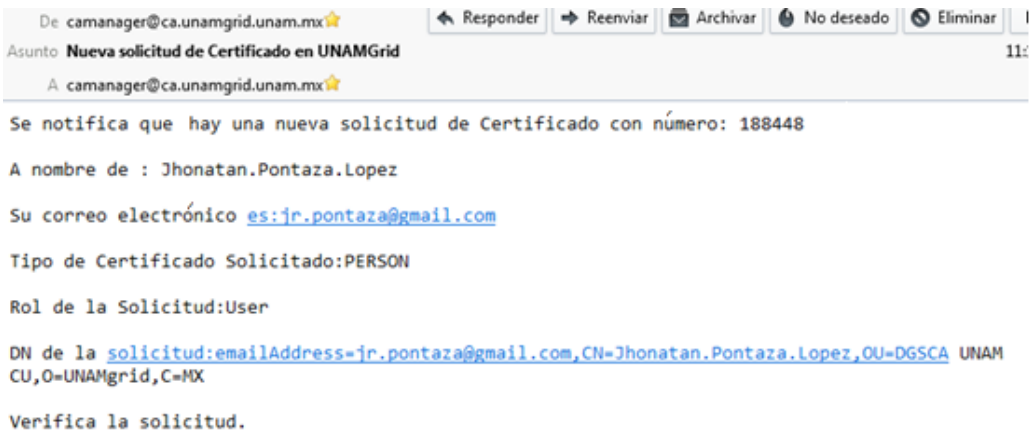
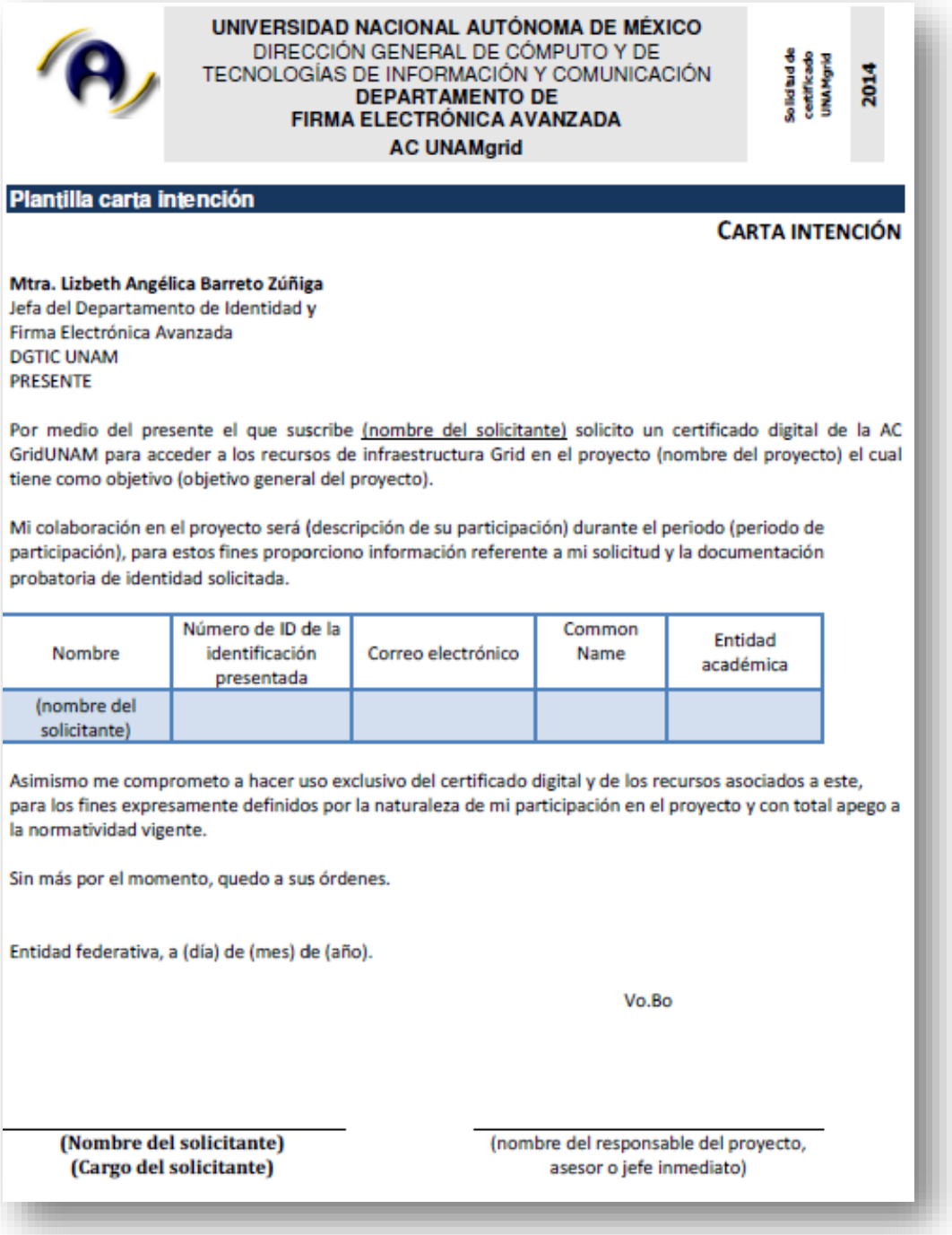


Ilustración III. 11 Correo electrónico que le llega al administrador.

Una vez que el administrador recibió el correo, éste le manda un correo electrónico manual al usuario para pedirle una carta de intención (ésta tiene el objetivo de saber el proyecto en el cual están involucrados los usuarios, así como su permanencia dentro del mismo. Este documento deberá de ser firmado por el responsable del proyecto) y una identificación oficial (INE, pasaporte, credencial de la UNAM u otra institución educativa). En la Ilustración III. 12, se muestra el cuerpo base del documento.



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
DEPARTAMENTO DE FIRMA ELECTRÓNICA AVANZADA
AC UNAMgrid

Solicitud de certificado UNAMgrid 2014

Plantilla carta intención

CARTA INTENCIÓN

Mtra. Lizbeth Angélica Barreto Zúñiga
Jefa del Departamento de Identidad y
Firma Electrónica Avanzada
DGTIC UNAM
PRESENTE

Por medio del presente el que suscribe (nombre del solicitante) solicito un certificado digital de la AC GridUNAM para acceder a los recursos de infraestructura Grid en el proyecto (nombre del proyecto) el cual tiene como objetivo (objetivo general del proyecto).

Mi colaboración en el proyecto será (descripción de su participación) durante el periodo (periodo de participación), para estos fines proporciono información referente a mi solicitud y la documentación probatoria de identidad solicitada.

Nombre	Número de ID de la identificación presentada	Correo electrónico	Common Name	Entidad académica
(nombre del solicitante)				

Asimismo me comprometo a hacer uso exclusivo del certificado digital y de los recursos asociados a este, para los fines expresamente definidos por la naturaleza de mi participación en el proyecto y con total apego a la normatividad vigente.

Sin más por el momento, quedo a sus órdenes.

Entidad federativa, a (día) de (mes) de (año).

Vo.Bo

(Nombre del solicitante)
(Cargo del solicitante)

(nombre del responsable del proyecto, asesor o jefe inmediato)

Ilustración III. 12 Formato carta intención

III.7.5.3 SOLICITUD DE RENOVACIÓN DEL CERTIFICADO

Un certificado puede ser renovado si no ha llegado al término de su periodo de validez, si no ha sido revocado y si el nombre del titular (suscriptor) y atributos aún son correctos.

Únicamente cuando la RA verifica que el certificado no ha sido revocado, la AC acepta y procesa la solicitud de renovación. UNAMgrid CA puede decidir rechazar esa renovación por motivos de seguridad. La RA deberá validar que el solicitante todavía esté trabajando en el proyecto original. El solicitante de la renovación debe preguntar al líder de proyecto que originariamente confirmó la necesidad del usuario de un certificado, para informar a la RA que el usuario todavía tiene derecho a un certificado.

El periodo para realizar la solicitud de renovación de un certificado será 30 días antes del vencimiento del mismo.

El titular del certificado puede pedir la renovación de su certificado digital, antes de que éste expire a través de la interfaz web, utilizando su DN.

Para los certificados de servidor (host), éstos pueden ser solicitados por los responsables del servidor o servicio y deben presentar el certificado que se solicita renovar como medio de autenticación.

La renovación de certificados digitales podrá hacerse vía remota a través de la interfaz web del sitio de la UNAMgrid AC

- http://ca.unamgrid.unam.mx/

Si se cuenta con certificado aún vigente, utilizando la interfaz web, en el menú, Renovar certificado, se podrá solicitar la renovación. Una vez que el certificado haya perdido vigencia no podrá ser renovado.

En la Ilustración III. 13, se muestra el formulario para solicitar la renovación de un certificado sin importar si es de usuario o servidor, el usuario tiene que buscar su certificado ya sea por CN, e-mail o número de serie que tiene el certificado a renovar.

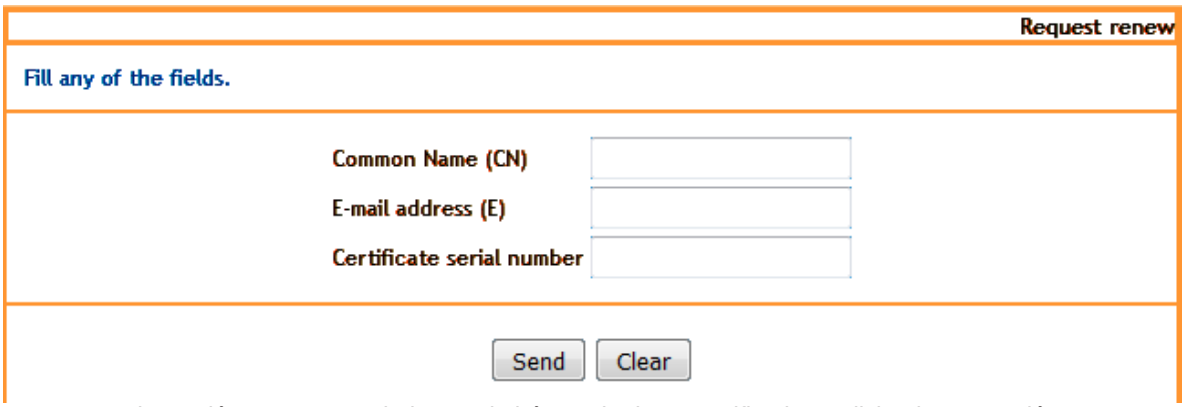


Ilustración III. 13 Formulario para la búsqueda de un certificado y solicitar la renovación

Una vez que el sistema encuentra coincidencias dependiendo del criterio de búsqueda, deberá seleccionar su certificado buscando que sea el más nuevo o el más reciente. En la Ilustración III. 14, se muestra el resultado de la búsqueda. El usuario deberá seleccionar “Request renew” y el sistema mandará un correo al administrador para poder procesar la solicitud.

Ilustración III. 14 Selección de certificado a renovar

El sistema le manda un correo automático al administrador para dar conocimiento de la solicitud. En este caso yo como el administrador tengo que mandarle un correo manual a usuario para solicitarle la carta intención (véase Ilustración III. 12), esto es para tener los datos actualizados.

Una vez validada la documentación se procederá a renovar el certificado.

III.7.5.4 SOLICITUD DE REVOCACIÓN Y SUSPENSIÓN DE UN CERTIFICADO

La revocación de un certificado digital implica la baja permanente del par de claves y la pérdida de sus privilegios de acceso y uso en los sistemas grid. Esta baja no libera la responsabilidad sobre el uso de éste, mientras estuvo vigente.

Circunstancias de revocación

Las principales razones para solicitar una revocación serán:

- ✓ Debido a que el titular (suscriptor) ha dejado de ser un miembro o asociado de un programa o actividad de UNAMgrid CA.
- ✓ La clave privada del titular (suscriptor) se extravía o se sospecha está comprometida.
- ✓ No se necesita más.
- ✓ La información en el certificado del titular (suscriptor) es incorrecta o imprecisa.
- ✓ El titular (suscriptor) no cumplió con las reglas del presente documento.
- ✓ El sistema (host) para el cual fue emitido el certificado, fue dado de baja.
- ✓ La clave privada de la AC se ha extraviado o se encuentra comprometida.
- ✓ A solicitud del titular (suscriptor)

Quién puede solicitar revocación

Una revocación certificada puede ser pedida por:

- ✓ El propietario de la clave certificada.
- ✓ La UNAMgrid CA o la RA que tenga prueba de clave comprometida.
- ✓ La organización o entidad que desea revocar su consentimiento a estar incluida en un certificado.
- ✓ La RA que autenticó al propietario del certificado.
- ✓ El titular (suscriptor) del certificado.
- ✓ Cualquier persona que presente prueba de conocimiento de que la contraseña del titular (suscriptor) está comprometida o que los datos del titular (suscriptor) han cambiado.

A menos que la UNAMgrid CA realice directamente la revocación, la solicitud de revocación debe ser efectuada por:

- ✓ El titular (suscriptor) del certificado, debidamente autenticado, usando las opciones de revocación dispuestas en la página web. En caso de emergencia o no contar con pérdida de la llave privada del certificado, deberá informar a la RA tan pronto como sea posible y solicitarle realice la revocación.
- ✓ El administrador de la AC usando una interfaz web segura, solamente en el caso de pérdida de la llave privada del certificado por parte del usuario.
- ✓ Antes realizar la revocación, la UNAMgrid CA deberá verificar la fuente de la solicitud de acuerdo con los procedimientos para el registro inicial.

- ✓ Asimismo, el titular (suscriptor) deberá confirmar un correo de solicitud de revocación para que ésta se lleve a cabo.

En la Ilustración III. 15, se muestra el formulario para solicitar la revocación, de un certificado, a continuación de describen los campos que deberá llenar el usuario:

- *Certificate Serial Number.* El usuario tendrá que poner el número de serie del certificado a revocar.
- *Reason.* El usuario tendrá que dar una breve explicación de los motivos para la revocación.
- *CRIN.* El usuario tendrá que teclear el PIN que ingreso al llenar el formulario para la solicitud de su certificado.
- *Retype CRIN code.* El usuario repetirá el PIN.

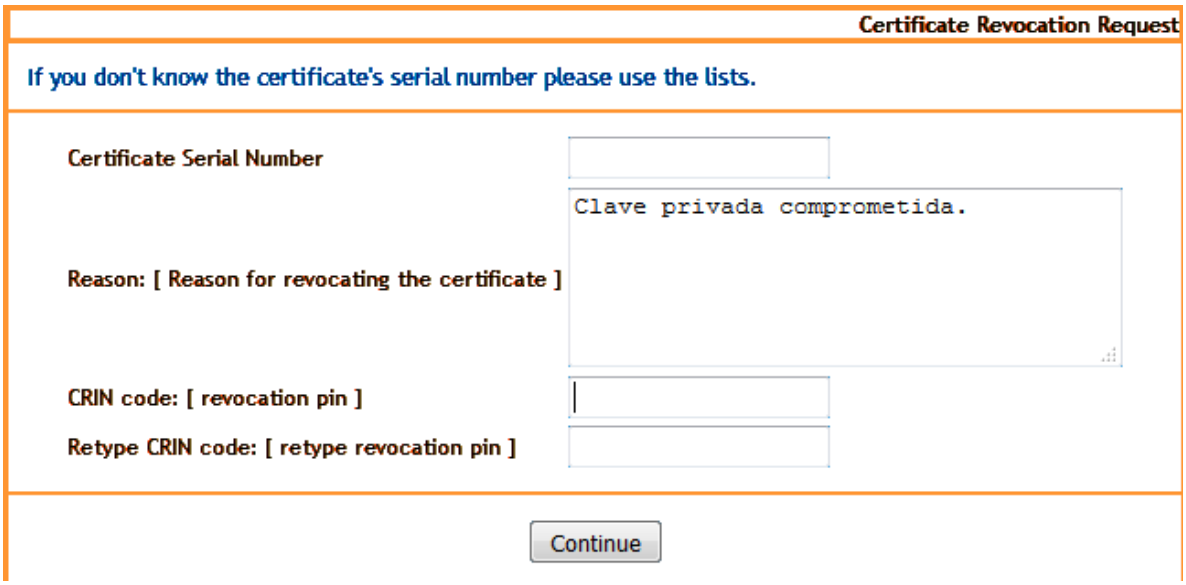


Ilustración III. 15 Formulario para solicitar la revocación de un certificado

Una vez que el usuario solicita la revocación el sistema manda un correo al administrador y procedo a revocar el certificado.

Ya que tengo conocimiento de cualquier tipo de solicitud el proceso para aprobar es el mismo.

III.7.5.5 APROBAR SOLICITUDES

El usuario tiene que acudir a presentar de manera personal la documentación solicitada para poder procesar su solicitud al Departamento de Firma Electrónica Avanzada. Una vez recibida y aprobada la documentación se archiva y proceso la solicitud de la siguiente manera.

En la Ilustración III. 16, se muestra el acceso a la página de administración de la RA para buscar, aprobar y exportar la solicitud.

Ilustración III. 16 Proceso de aprobación y exportación en la página de administración de la RA

Una vez que exporte la solicitud, tengo que ingresar al servidor de manera remota para poder extraer el archivo que lleva consigo la o las solicitudes, descargarlas en una USB o algún medio de almacenamiento para guardarlas y llevarlas a la AC.

Tengo que ingresar a la AC de manera física para descargar las solicitudes, acceso vía consola a la AC para darle permisos al archivo, copiarlas a una carpeta en específico para que se puedan importar y firmar las solicitudes, cada que se procesa una solicitud se tiene que generar una CRL.

En la Ilustración III. 17, se muestra el procedimiento para firmar las solicitudes, primeramente, tengo que acceder a la página de administración de la AC para importar las solicitudes.

Después de importar las solicitudes busco y apruebo las solicitudes pendientes, el sistema me pide la clave de 16 dígitos de la AC para poder firmar y almacenar el registro de los certificados, una vez firmados todos los certificados pendientes, se tiene que generar una nueva CRL, para generar dicha CRL, la AC pide que se ingrese el periodo de validez que por normas de TAGPMA es de 30 días naturales, ingresa la contraseña de la autoridad.

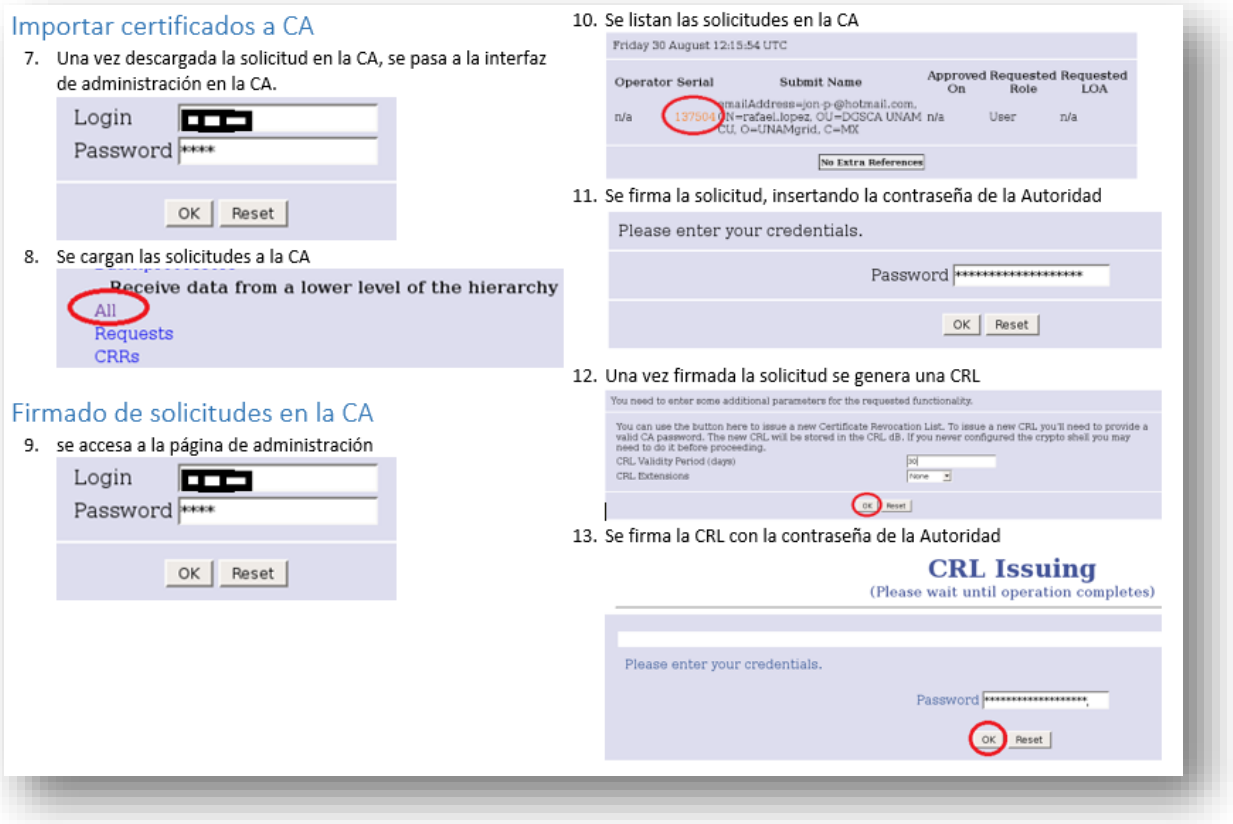


Ilustración III. 17 Proceso de importación y firmado de las solicitudes en la AC

Una vez firmados los certificados y generada la nueva CRL se pasa a exportar los nuevos certificados generados, en la Ilustración III. 18, se muestra el proceso para la exportación.

Ya que se hizo la importación en el panel de administración de la AC, acceso vía consola para extraer el archivo y los diferentes tipos de CRL. Lo almaceno en una USB.

Ya que se tiene los archivos me conectó a la RA de manera remota para descargar el archivo, hay que otorgar permisos y moverlos a sus carpetas correspondientes para que en el panel de administración se pueda hacer la importación.

Acceso a la página de administración de la RA para que se puede hacer la importación, el sistema de manera automática lanza un evento de correo electrónico para que le envíe a los usuarios una notificación y éstos puedan descargar su certificado.

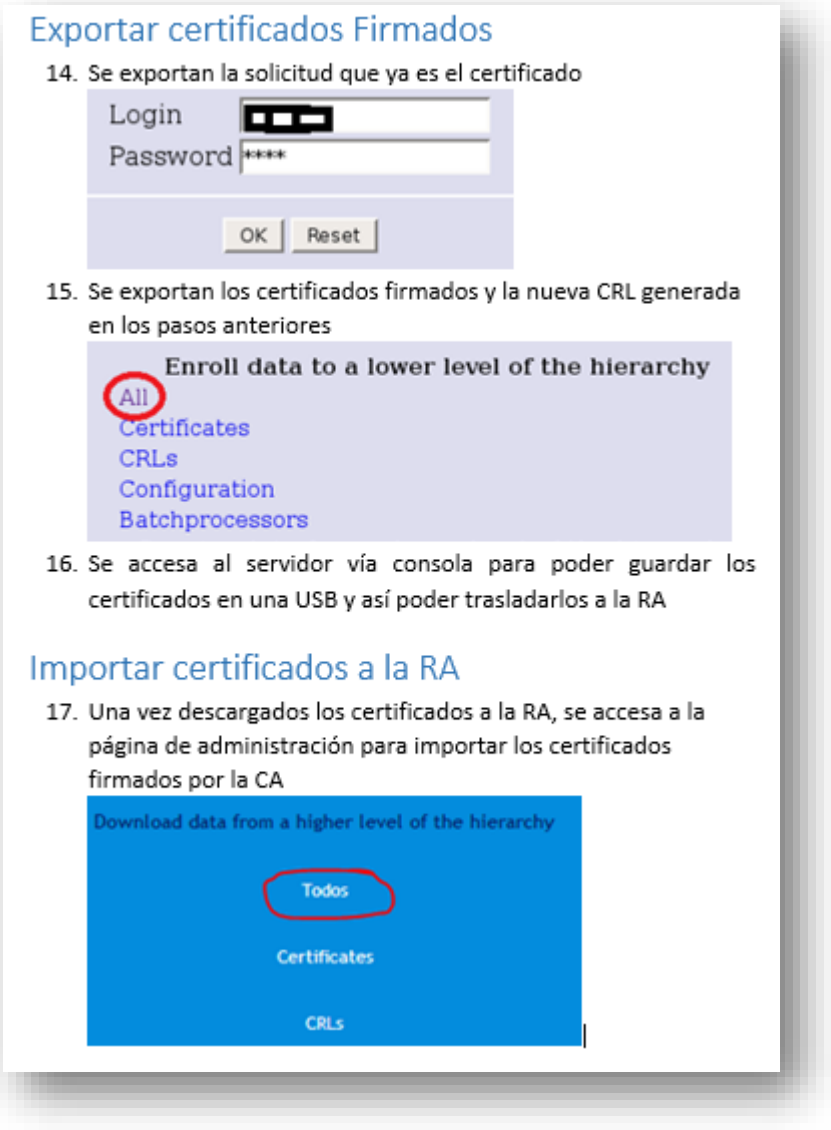


Ilustración III. 18 Importación de certificados en la RA

El sistema manda de manera automática un correo electrónico al usuario informándole que ya está listo para descargar su certificado digital, el cual contiene la URL de descarga y los pasos para realizar la descarga de manera manual.

III.8 PROPUESTA DE INFRAESTRUCTURA

Como se observa en el proceso anterior, para la aprobación de solicitudes de un certificado digital, ya sea generación, renovación o revocación yo tengo que hacer todo el procedimiento.

Esto provocaba que los usuarios dependan de mí, si por alguna razón el usuario olvidó hacer su renovación a tiempo o solicita un certificado de urgencia en la madrugada o en fin de semana, tendrían que esperar a que llegara a la oficina para poder procesar su solicitud.

Los certificados de servidor tienen un nivel de prioridad muy alto ya que el IGTF monitorea de manera continua cada servidor, por lo que si un administrador habla a cualquier hora solicitando un certificado tenemos la obligación de generarlo.

Como se observa yo como administrador tengo que estar en todo momento conectado a la UNAMgrid, por este inconveniente y dado que la versión en producción ya no podía cumplir con los requerimientos de TAGPMA, se decidió migrar a una plataforma que tiene soporte para cumplir con los requerimientos solicitados.

Este nuevo software permite procesar las solicitudes en el mismo servidor sin la necesidad de exportar ni importar las solicitudes de los usuarios. También como es software libre se puede modificar sin restricciones para poder hacer procesos nuevos o lo más parecidos a los procesos actuales y así los usuarios no tengan problemas para poder realizar peticiones de certificados.

III.8.1 ENTERPRISE JAVA BEANS CERTIFICATE AUTHORITY

EJBCA[30] (*Enterprise Java Beans Certificate Authority*) es una autoridad certificadora creada en java basada en JEE (*Java Platafform, Entreprise Edition*).

EJBCA es un software libre, que permite la creación de Autoridades Certificadoras mediante su interfaz gráfica. Este software permite crear AC´s con llaves generadas y almacenadas por el propio software y llaves en dispositivos criptográficos.

III.8.2 INFRAESTRUCTURA

Uno de los aspectos que se tiene que respetar es que la nueva AC tenga los conceptos básicos de una PKI tradicional, como se muestra en la ilustración III. 19, la RA y la AC están en un mismo servidor, y para mitigar el problema de clonación o robo de la llave, se adquirió un HSM FIPS 140-2 nivel 3, que es un dispositivo especializado para resguardar la llave de la AC.

[30] EJBCA - Open Source PKI Certificate Authority – Home. Recuperado 26 de mayo de 2016. https://www.ejbca.org/

También se muestra que se tienen servidores dedicados para la Base de Datos, así como un servidor dedicado al envío de correos.

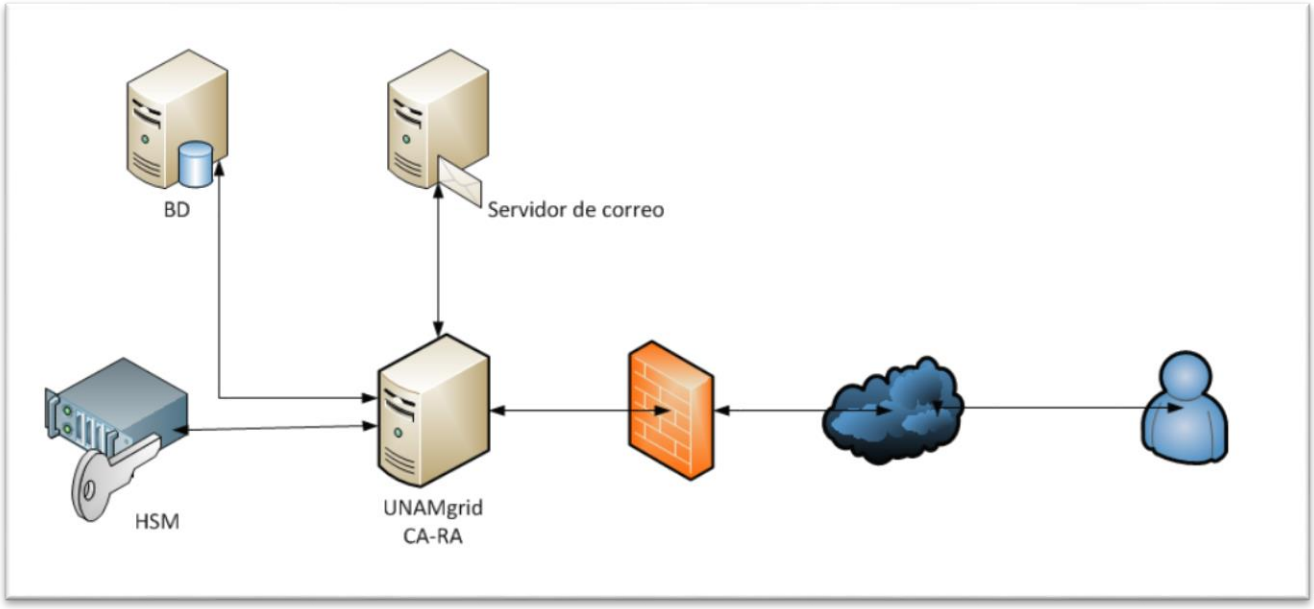


Ilustración III. 20 Infraestructura para la nueva versión de UNAMgrid

Autoridad Certificadora y Autoridad Registradora

- Red Hat[31] Enterprise Linux Server release 6.6 (Santiago)
- EJBCA 6.1.1
- PostgreSQL 8.4
- OpenSSL 1.0.1e-fips 11 Feb 2013
- apache-ant[32] 1.9.4
- Jboss[33] 7.1.1
- Máquina Virtual (MV)
  - Virtualizador: QUEMU[34]
  - 8 Gb Memoria RAM

La propuesta para migrarse a la plataforma EJBCA contiene mejoras en la infraestructura:

- Configuración de servidor dedicado a bases de datos.

[31] Red Hat SUMMIT Recuperado 26 de mayo de 2016. https://www.redhat.com/es
[32] Apache Ant™, Recuperado 26 de mayo de 2016. http://ant.apache.org/
[33] JBossDeveloper, Recuperado 26 de mayo de 2016. http://www.jboss.org/
[34] QEMU open source machine processor emulator, Recuperado 26 de mayo de 2016. http://wiki.qemu.org/Main_Page

- Integración de un dispositivo criptográfico de alto nivel FIPS 140-2[35] nivel 3 para almacenar la llave raíz de la autoridad certificadora, garantizando la integridad de la información.
- Máquina virtual resguardada en un centro de datos con altos niveles de seguridad lógica, física y perimetral.
- Utilización de una plataforma de autoridad certificadora más robusta, confiable y actualizada (EJBCA v. 6.1.1.).

III.8.2.1 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 140-2

Norma Federal para el procesamiento de información 140-2 (FIPS 140-2) es una norma gubernamental de E.U.A, que describe el cifrado y los requisitos de seguridad relacionados que los productos de Tecnologías de la Información deben cumplir para el uso con datos sensibles, pero no clasificados.

Niveles[36] asociados con FIPS 140-2

FIPS 140-2 define cuatro niveles de seguridad. La validación de FIPS 140-2 especificará el nivel de seguridad que el producto deberá cumplir.

- **El nivel 1** típicamente se usa para productos de cifrado sólo para software, impone requisitos de seguridad muy limitados. Todos los componentes deben ser de *nivel de producción* y los diversos tipos flagrantes de inseguridad deben estar ausentes.
- **El nivel 2** requiere la autenticación *basada en la función*. (No se necesita la autenticación de usuario particular.) También requiere la capacidad de detectar la violación física mediante el uso de bloqueos físicos o sellos a prueba de violaciones.
- **El nivel 3** agrega violación física *resistencia* al desmontaje o modificación, haciéndolo extremadamente difícil para sabotear. Si se detecta una violación, el dispositivo debe ser capaz de borrar los parámetros de seguridad críticos.
- El nivel 3 también incluye una sólida protección de cifrado y administración de claves, autenticación *basada en la identidad,* así como la separación física o lógica entre las interfaces mediante el ingreso y la salida de los *parámetros de seguridad críticos*.
- **El nivel 4** incluye una protección avanzada contra violación y está diseñado para ser utilizado con productos que operan en ambientes desprotegidos físicamente.

[35] SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, Recuperado 23 de mayo de 2016. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[36] Tecnología estándar FIPS 140-2 y unidad de cifrado automático, Recuperado 23 de mayo de 2016. http://www.seagate.com/la/es/tech-insights/fips-140-2-standard-and-self-encrypting-drive-technology-master-ti/

III.8.3 MEJORAS EN LA PARTE OPERATIVA

- Creación de nuevos procesos para la certificación de usuarios y proceso de recertificación de usuarios con certificados vigentes.
- Gestión para el proceso de aprobación por TAGPMA e IGTF para ser una AC reconocida internacionalmente.
- Se generaron nuevos formularios para la solicitud de certificados.
- Se creó un certificado de acceso para que el usuario pueda realizar sus peticiones de certificados.
- Se optimizó el proceso de certificación para que no se dependa de mí para la aprobación de certificados.

III.9 IMPLEMENTACIÓN

III.9.1 INSTALACIÓN BÁSICA

Primeramente, instalé una MV (Máquina Virtual) con los elementos básicos, S.O. (Sistema Operativo) Red Hat con los siguientes programas:

- Servidor de SSH (Secure SHell)[37]
- Cliente de NTP (Network Time Protocol)[38]
- OpenSSL (Secure Sockets Layer)

Concluida la instalación básica de la MV preparé los elementos necesarios para la instalación de EJBCA.

- EJBCA
- Apache ant
- Jboss
- Java jdk (Java Development Kit)[39]

Descargué e instalé el software necesario para poder levantar el servicio web de Jboss. Así mismo configuré los parámetros básicos necesarios para generar una AC que se genera al momento de compilar el software de EJBCA. Los requerimientos básicos para levantar una AC son:

- Indicar la ubicación del directorio Jboss.
- Instalar el controlador de la base de datos PostgreSQL en Jboss.
- Generar una base de datos en el servidor dedicado para el proyecto.
- En los parámetros de EJBCA de configuración indicar la dirección IP (Internet Protocol) y el manejador de base de datos que se utilizará.

---

[37] Red Hat Enterprise Linux 4: Manual de referencia, Recuperado 26 de mayo de 2016. http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

[38] NTP: The Network Time Protocol, Recuperado 26 de mayo de 2016. http://www.ntp.org/

[39] Java SE Documentation, Recuperado 26 de mayo de 2016. http://www.oracle.com/technetwork/java/javase/documentation/index.html

- Indicar que puertos se utilizaran puerto 80 (página pública del sitio) y puerto 443 (página de administración).

Al terminar de configurar los parámetros, procedí a compilar el software de EJBCA con la herramienta de apache ant.

Una vez terminada la instalación básica de EJBCA con una AC de prueba, revisé si en su estado nativo podría cumplir con lo solicitado, después de varios días revisando las funcionalidades algunas si cumplían y otras no por completo.

Uno de los grandes problemas a los que me enfrente es que el sistema tiene que tener un formulario para que los usuarios se puedan registrar, EJBCA tiene la funcionalidad de generar formularios de registro, con la desventaja de que el sistema autogenera las contraseñas y las envía vía correo electrónico.

Para el desarrollo del proyecto se tuvieron varias sesiones de trabajo con TAGPMA, se les mostró el formulario y varias propuestas del nuevo sistema con los nuevos procesos, que trae el propio sistema, ellos realizaron observaciones; entre las cuales la más significativa es que la contraseña la tiene que ingresar el propio usuario y de ninguna manera se tendría que transmitir la contraseña.

Para dar solución al problema de la contraseña, reutilice código para cumplir con los requerimientos, lo adapte y compile, este código es una porción de la página de administración, lo extraje y lo coloqué en el sitio público.

El usuario tiene todo el control sobre su o sus certificados, para cualquier acción sobre éste, requiere la aprobación del dueño para poder revocar o renovar, se activó el módulo para la renovación de un certificado, así como adaptación para la revocación.

Para poder revocar o renovar, el usuario tendrá que autenticarse ante el sistema con su certificado vigente y cumplir con las políticas de certificación que se crearon.

III.9.2 SOLICITUD DE CERTIFICADOS

Generé una nueva página de inicio que fuera similar a la página que se tiene en producción, para que el usuario final no tuviera problemas al presentarle un cambio muy drástico, los cambios como se nota en la siguiente ilustración fueron la posición de los menús (véase Ilustración III. 21 Página de inicio de la nueva versión de UNAMgrid)

Ilustración III. 21 Página de inicio de la nueva versión de UNAMgrid

El sitio es de dominio público (https://ca.unamgrid.unam.mx), cualquier persona podrá acceder a la página y navegar por todo el sitio.

Para evitar solicitudes de personas ajenas a algún proyecto decidimos restringir el formulario para poder obtener un certificado digital.

Como medida de seguridad generé un certificado de acceso para el formulario que está en el sitio, el usuario final lo tendrá que descargar e instalar en su navegador para que pueda hacer su solicitud de certificado. Sólo los responsables de los

proyectos tendrán la clave del certificado de acceso, así se garantiza que sólo los usuarios autorizados puedan realizar solicitudes válidas. En la Ilustración III. 22, se muestran los datos del certificado de acceso que se llama ***PKIStep***.

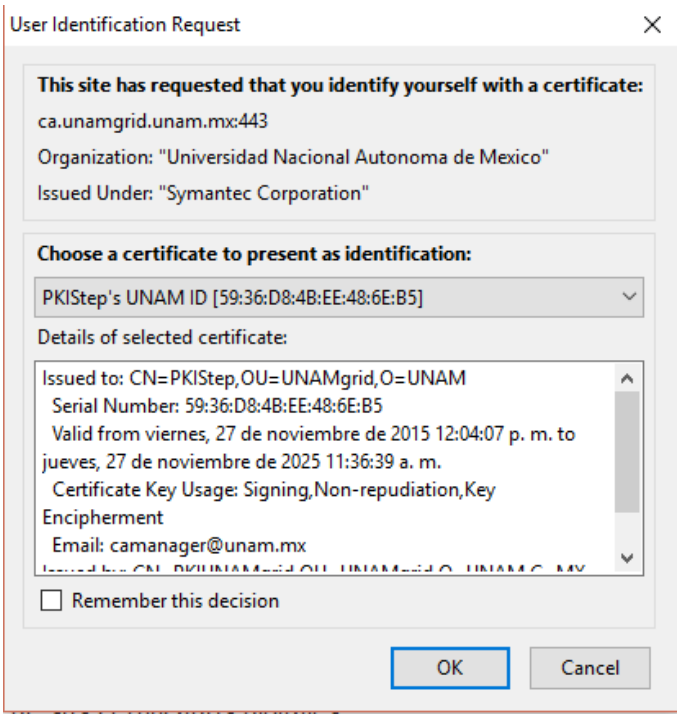


Ilustración III. 22 Datos generales del certificado de acceso PKIStep

PKIStep, es un certificado de administración con privilegios para poder solicitar un certificado. Para poder agilizar el proceso y no depender de estar físicamente donde se encuentra la AC, generé certificados de administración (uno para la Jefa del Departamento, otro para el deje de aplicaciones), para que puedan aprobar cualquier solicitud, en la Ilustración III. 23, se muestra el diagrama de los certificados.

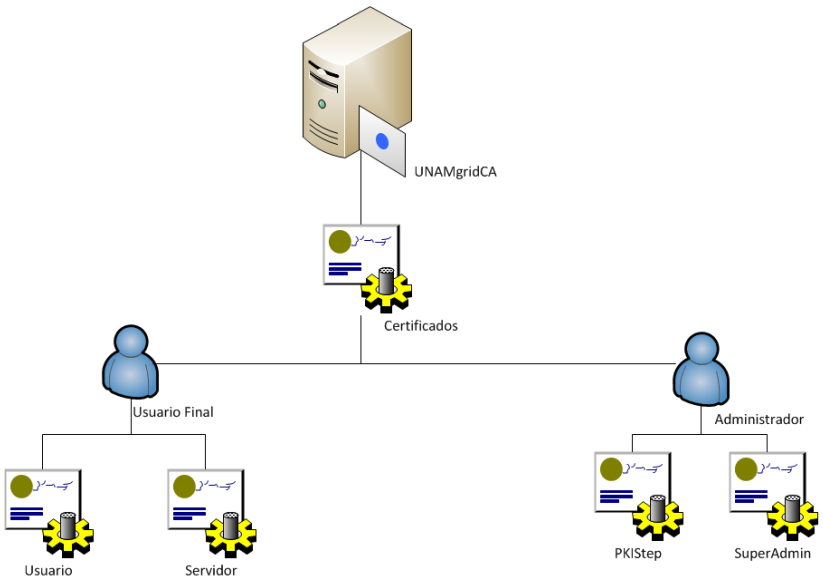


Ilustración III. 23 Diagrama de certificados que emite UNAMgridCA

Una vez que el sistema validó el certificado PKIStep, le permitirá visualizar el formulario para poder hacer la solicitud. En la Ilustración III. 24, se muestra el formulario para solicitar un certificado de usuario, a continuación, se describen los campos que deberá llenar el usuario:

- *CN, Nombre Común.* Este campo no acepta espacios, acentos, caracteres especiales y deberá ser alusivo al nombre de usuario final.
- *Password.* Este campo debe tener al menos 8 caracteres, una mayúscula y un número.
- *Dirección de E-mail.* El usuario deberá ingresar un correo valido, ya que será la forma de comunicarse con el administrador.
- *Nombre.* El usuario en este campo deberá poner su nombre completo tal y como viene en su identificación que presentará para terminar el proceso.

- *Entidad.* El usuario ingresará su entidad a la que pertenece ya sea en la UNAM o en su defecto la universidad a la que pertenece.

Ilustración III. 24 Formulario para solicitar un certificado de usuario

Para poder acceder al formulario de solicitud de certificado de tipo servidor, el usuario tendrá que presentar el certificado de PKIStep para poder realizar la solicitud correspondiente. En la Ilustración III. 25, se muestra el formulario para solicitar un certificado de servidor, a continuación, se describen los campos que deberá llenar el usuario:

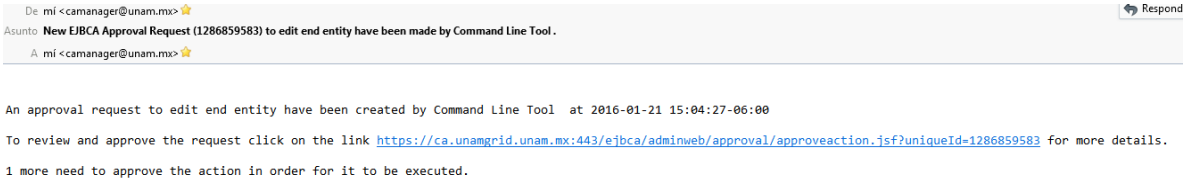
- *CN, Nombre Común.* En este campo el usuario pondrá el nombre del servidor, este campo no acepta espacios, mayúsculas, caracteres especiales.
- *Password.* Este campo debe tener al menos 8 caracteres, una mayúscula y un número.
- *Dirección de E-mail.* El usuario deberá ingresar un correo valido, ya que será la forma de comunicarse con el administrador
- *Nombre.* El usuario deberá poner el nombre completo del responsable de dicho servidor tal y como viene en su identificación que presentará para terminar el proceso.
- *Entidad.* El usuario ingresará su entidad a la que pertenece ya sea en la UNAM o en su defecto la universidad a la que pertenece.

Ilustración III. 25 Formulario para solicitar un certificado de servidor

III.9.3 APROBACIÓN DE SOLICITUD DE CERTIFICADOS

Creé certificados de administración para poder entrar a la página de administración de la nueva AC, a continuación, se describen los pasos para poder aprobar una solicitud:

- Una vez llenado el formulario el sistema manda un correo electrónico a la cuenta de e-mail de UNAMgrid para poder pre-aprobar la solicitud (véase Ilustración III. 26).
- Yo siendo el administrador acceso a la página de administración apruebo la solicitud.
- El sistema le manda un correo al usuario para solicitarle su documentación y tener actualizado su registro ver Ilustración III. 27 (se utilizará el mismo formato de la carta de intención que se tiene actualmente. Véase Ilustración III. 12).

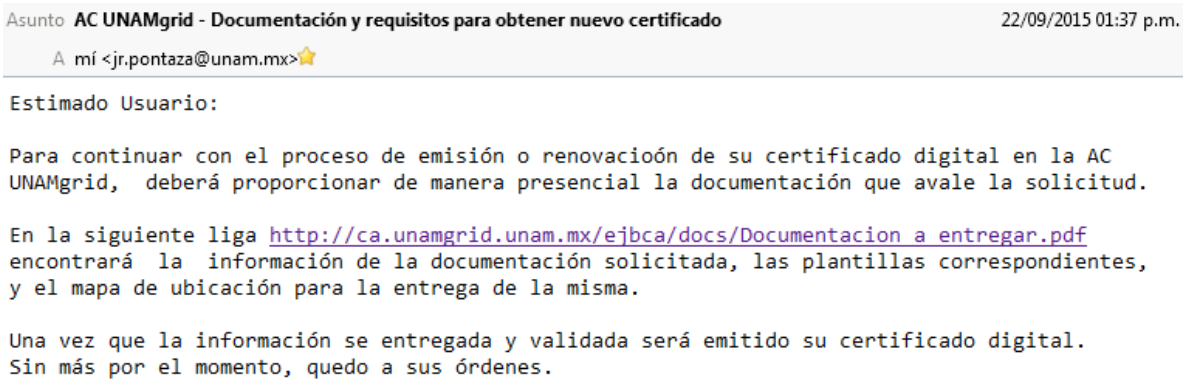

De mí <camanager@unam.mx>
Asunto **New EJBCA Approval Request (1286859583) to edit end entity have been made by Command Line Tool .**
A mí <camanager@unam.mx>

An approval request to edit end entity have been created by Command Line Tool at 2016-01-21 15:04:27-06:00

To review and approve the request click on the link https://ca.unamgrid.unam.mx:443/ejbca/adminweb/approval/approveaction.jsf?uniqueId=1286859583 for more details.

1 more need to approve the action in order for it to be executed.

Ilustración III. 26 Correo enviado a la cuenta de administración de UNAMgrid


Asunto **AC UNAMgrid - Documentación y requisitos para obtener nuevo certificado** 22/09/2015 01:37 p.m.

A mí <jr.pontaza@unam.mx>

Estimado Usuario:

Para continuar con el proceso de emisión o renovacioón de su certificado digital en la AC UNAMgrid, deberá proporcionar de manera presencial la documentación que avale la solicitud.

En la siguiente liga http://ca.unamgrid.unam.mx/ejbca/docs/Documentacion_a_entregar.pdf encontrará la información de la documentación solicitada, las plantillas correspondientes, y el mapa de ubicación para la entrega de la misma.

Una vez que la información se entregada y validada será emitido su certificado digital.
Sin más por el momento, quedo a sus órdenes.

Ilustración III. 27 Correo enviado por el sistema al usuario solicitando documentación

- Una vez que el usuario entrega la documentación solicitada, se le envía un correo manual al usuario para notificarle que su solicitud ha sido aprobada, en la Ilustración III. 28, se muestra el correo enviado al usuario para la descarga de su certificado.


Información de Certificado UNAMgrid

Autoridad Certificadora UNAMgrid <camanager@unam.mx>

Para luis_saldierna@yahoo.com.mx

Estimado usuario de AC UNAMgrid:

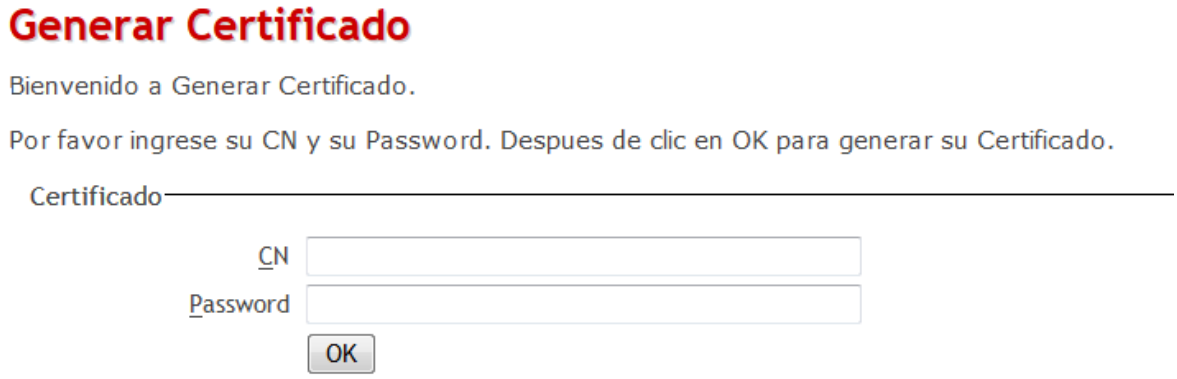
Su certificado con CN=fernando fue aprobado. Puede descargarlo desde nuestro servidor en la URL:

http://ca.unamgrid.unam.mx/ejbca/enrol/browser.jsp

1. Ingresar su Username
2. Teclear su contraseña y dar clic en generar

Ilustración III. 28 Correo enviado al usuario para descargar su certificado

- El usuario tiene que ingresar a la página que se le envía a través del correo electrónico, al ingresar a la página, tiene que teclear su CN y su contraseña que ingresó en el formulario de registro (véase Ilustración III. 29).


Generar Certificado

Bienvenido a Generar Certificado.

Por favor ingrese su CN y su Password. Despues de clic en OK para generar su Certificado.

Certificado

CN

Password

OK

Ilustración III. 29 Página para la descarga de su certificado

III.9.4 REVOCAR CERTIFICADO

Para revocar un certificado, se mejoró el proceso ya que los usuarios en el proceso actual tienen que ingresar su pin (contraseña), el cual los usuarios no lo recordaban. Este proceso consiste en que para hacer la revocación tiene que ingresar con su certificado al apartado de revocación en la página de UNAMgrid, al ser reconocido por el sistema le mostrará sus datos, número de serie, DN del usuario y DN del emisor (véase Ilustración III. 30) sólo bastará con dar clic en el botón de revocar.

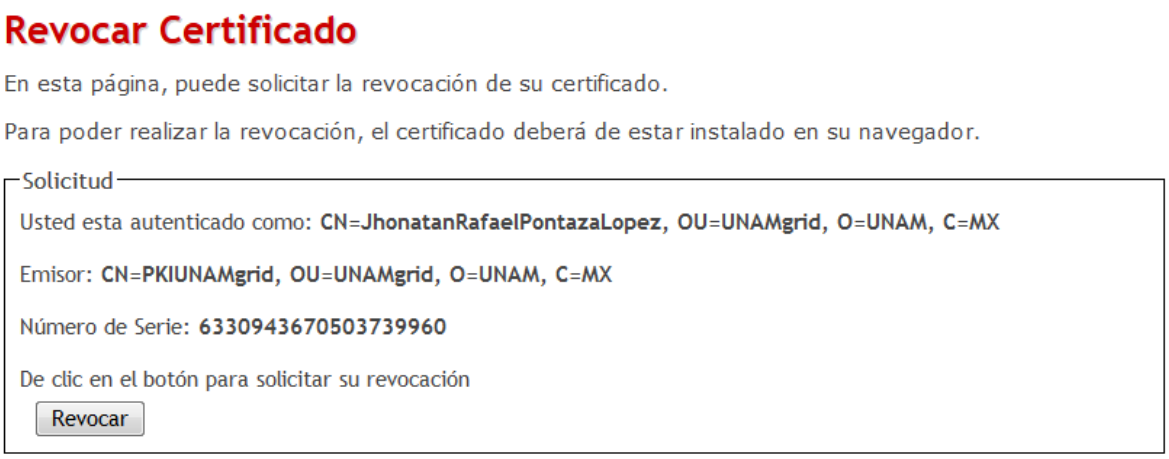


Ilustración III. 30 Solicitud de revocación de un certificado

Una vez que el usuario solicitó la revocación, el sistema manda un correo a la cuenta de administración de la AC, tengo que pre-aprobar la solicitud para que se interactúe con el usuario solicitando la confirmación vía correo electrónico, ya que una vez revocado el certificado ya no es posible deshacer el cambio. En la Ilustración III. 31, se muestra el cuerpo del correo enviado al usuario para confirmar la solicitud.

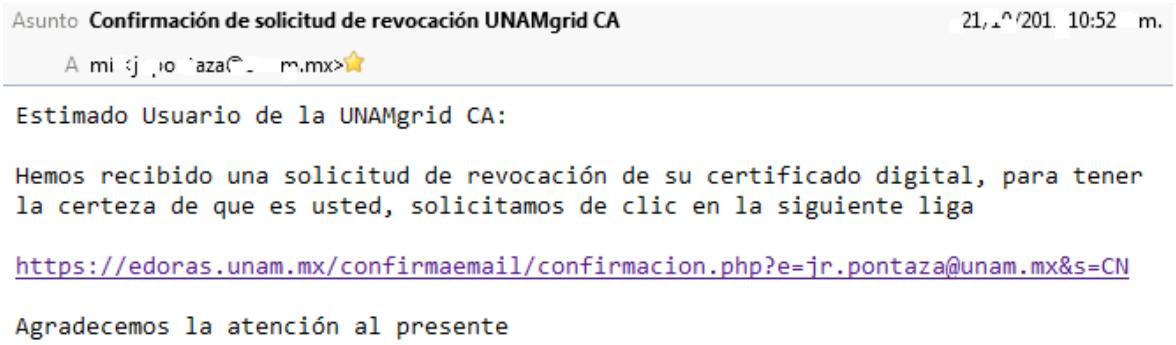


Ilustración III. 31 Correo enviado al usuario para la confirmación de revocación

Ya que se tiene la confirmación del usuario, tengo que hacer la petición de revocación del certificado para esto, sólo basta ingresar al panel de administración y uno de los administradores realice la solicitud, para concluir con la revocación se necesita la intervención de otro administrador para que se revoque de manera permanente el certificado, este proceso se realizó para tener la garantía de que siendo administrador de sitio no revoque certificados por equivocación.

III.9.5 RENOVACIÓN DE CERTIFICADOS

Para que un usuario pueda hacer la renovación de su certificado tiene que acceder a la página de la UNAMgrid y en el apartado de renovación, el sistema solicitará el certificado a renovar. Una vez que el sistema verifica tu información, verificando que dicho certificado no esté vencido o revocado, se mostrará la información del usuario. En la Ilustración III. 32, se muestran los datos del usuario que son el número de serie, datos del usuario y datos de la Autoridad Certificadora.

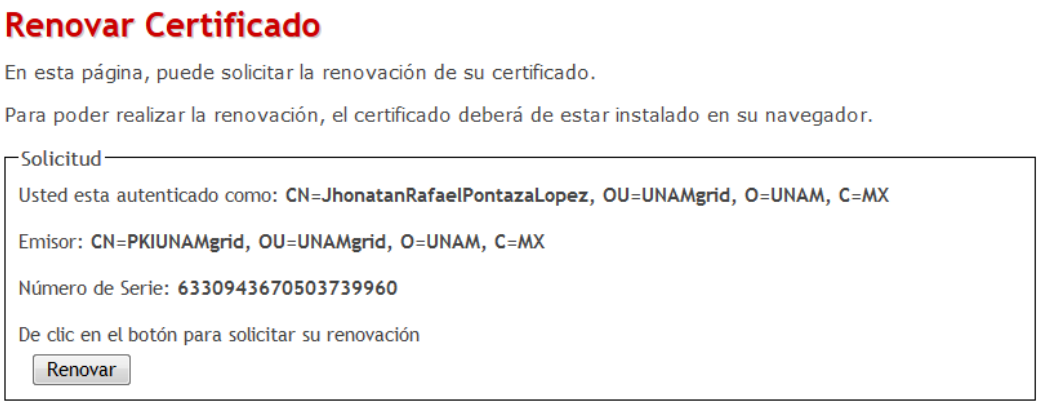


Ilustración III. 32 Solicitud de renovación de un certificado

Una vez que el usuario realiza su petición, el sistema envía un correo a la cuenta oficial de UNAMgrid, verifico sus datos y si es válida, procedo a su aprobación.

La apruebo en la página de administración. En automático el sistema le manda un correo al usuario solicitando que renueve la documentación. En este caso sólo se solicitará la carta de intención (véase Ilustración III. 12). Una vez que el usuario entregó personalmente dicho documento se le envía un correo al usuario indicándole la página web, para que realice la descarga de su nuevo certificado.

III.10 PRUEBAS

Una vez que terminé de configurar y revisar los procesos, la AC está en revisión, para garantizar la compatibilidad con los sistemas de producción le pedí a los administradores de la grid me ayudaran con las pruebas operativas.

Tuve que aprender el funcionamiento completo, una vez que el usuario obtiene su certificado tiene que acceder a la página de Organización Virtual (VO).

Una VO es la organización que está a cargo de la administración de los proyectos, México actualmente está en dos VO, una que es el proyecto EELA (E-Infrastructure shared between Europe and Latin America), que es para proyectos académicos y de investigación. El segundo proyecto al que México está adherido es el Proyecto ALICE que se definió en la introducción.

Cada servidor que aporta recursos a la grid, tiene instalados todos los certificados de las AC's y la información de ellas como son su vigencia, la dirección del sitio, la dirección la CRL y el número de serie del certificado, toda esta información es empaquetada en un archivo RMP (Red Hat Package Manager). Este archivo está en repositorio público del IGTF[40].

[40] International Grid Trust Federation IGTF Recuperado 26 de mayo de 2016. https://dl.igtf.net/distribution/igtf/

Generé el archivo RPM, con toda la información necesaria se lo instalé a los servidores de la UNAM, una vez instalado el archivo accedí a la VO. Para ingresar al sitio tienes que presentar un certificado de una AC válida por el IGTF, (por eso se generó y se instaló el RMP para que los servidores reconocieran los certificados véase III.10.1).

Una vez que el sitio reconoce los nuevos certificados pude hacer mi solicitud para formar parte de la grid y así poder mandar un job, el administrador de la grid en México aceptó mi solicitud y continúe con las pruebas operativas.

El administrador de los recursos grid me facilitó un programa para que la grid procesará un job, cada usuario tiene un cliente para poder enviar los trabajos.

Un usuario puede instalar y configurar el cliente, o los administradores te facilitan una cuenta en la que te logueas vía SSH, y envías tu trabajo.

En este caso los administradores me facilitaron una cuenta para poder enviar jobs, (en el cliente también instale el RPM, realicé la conexión y envíe el job al cabo de unos minutos la Grid proceso y me devolvió el resultado.

Al terminar las pruebas concluí que las pruebas operativas fueron exitosas y no habría ningún problema al poner en producción UNAMgrid en su nueva versión.

III.10.1 MANDAR UN TRABAJO "JOB"

Un usuario final debe tener conocimientos avanzados en sistemas computacionales, el usuario diseña y programa sus códigos en el lenguaje de programación JDL (Job Control Language). La interfaz para lanzar un 'Job' en la grid es una consola de un sistema Linux.

En la Ilustración III. 33, se muestra el procedimiento para enviar un trabajo en la grid. Adicionalmente en la Tabla III. 3 se describe el procedimiento.

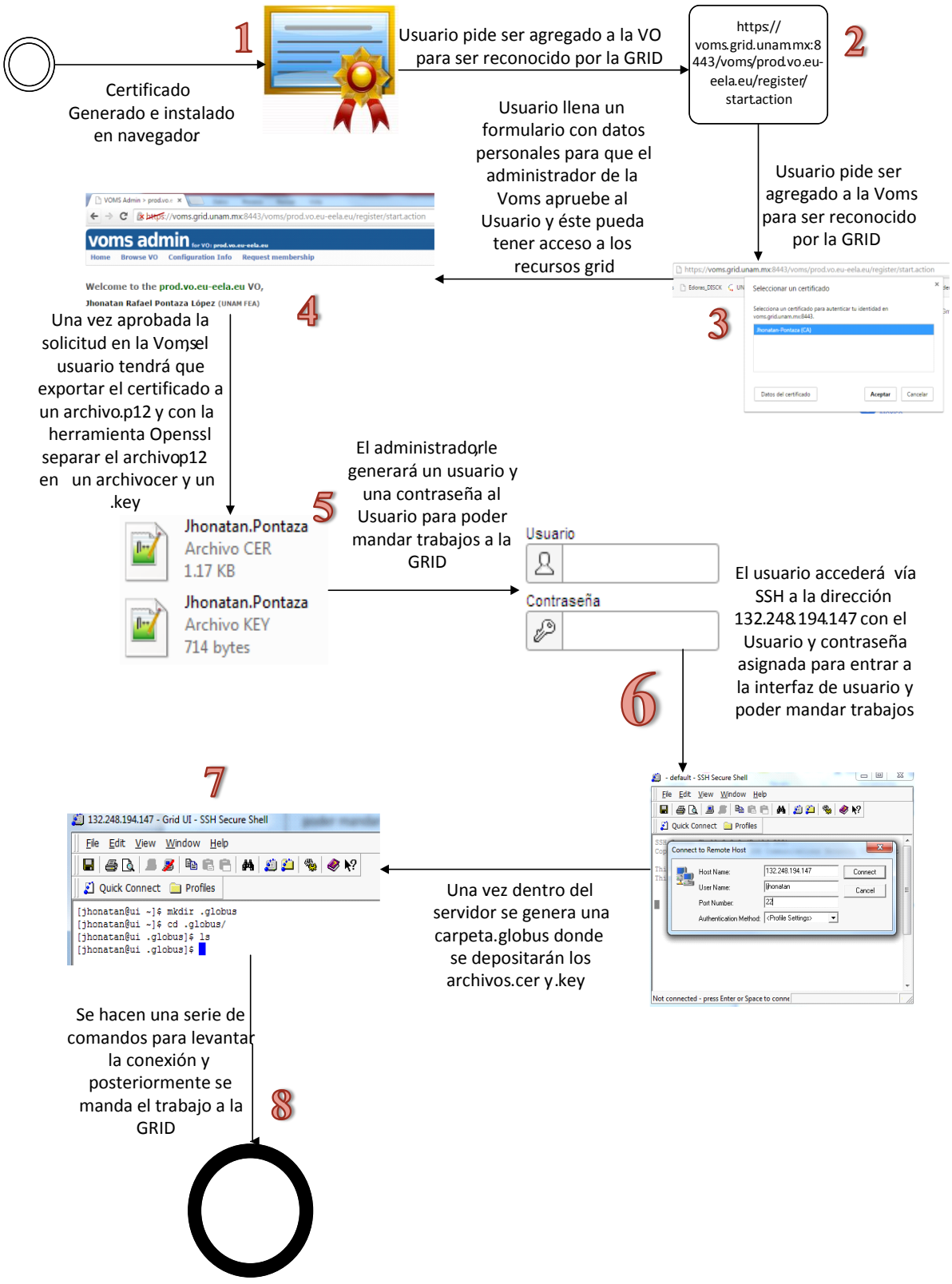


Ilustración III. 33 Envío de Jobs a la Grid

Tabla III. 3 Descripción de Envío de Jobs

ID	Etapa	Descripción
1	Certificado Generado	En esta etapa el usuario ya tiene su certificado instalado en el navegador.
2	Solicitud al Administrador de proyectos	Página para solicitar ingresar al administrador de proyectos.
3	Sistema valida usuario	El sistema valida al usuario, con el certificado previamente solicito a UNAMgrid, el usuario llena un formulario y espera la notificación de aprobación
4	Notificación de aprobación	El usuario recibirá un correo de aprobación por parte del administrador de proyectos.
5	Exportación de certificado	El usuario tiene que exportar su certificado y separar el certificado en la llave pública y privada correspondiente.
6	Acceso al cliente	El usuario ingresara al cliente para poder enviar los trabajos
7	Configuración del cliente	El usuario configurará su cliente con su certificado para poder crear la conexión.
8	Envío de trabajos	Una vez creada la conexión con la grid el usuario podrá enviar sus trabajos

III.11 RESULTADOS

III.11.1 CERTIFICADO DE AC

Como se mencionó anteriormente este certificado es público y se encontrará en el sitio web de UNAMgrid. https://ca.unamgrid.unam.mx. Para poder visualizarlo hay que modificar el archivo hosts de nuestro equipo "***200.53.148.157 ca. unamgrid.unam.mx***"

Cabe mencionar que, para el proceso de recertificación de todos los usuarios, deberán descargar e instalar este certificado, para que se construya de manera correcta la cadena de certificación. Así mismo para que se realice la descarga correcta de los certificados ya que algunos navegadores no lo descargan por que no está instalado en el almacén de certificados correspondiente.

Las mejoras que se implementaron según el calendario de TAGPMA fue generar dicha AC con un algoritmo mejor que el que se tiene en producción, así como el incremento de la llave que es a 4096 bits, un cambio importante es que esta autoridad ya nace con el servicio de OCSP para que los sistemas de la grid lo empiecen a consultar de cualquier momento.

- Algoritmo de cifrado SHA-256 (4096).
- Atributo de AC que permite el firmado de certificados.
- Firma de CRL.
- Duración de la AC 10 años.
- Cambio del CN de la AC por PKIUNAMgrid.

En la Ilustración III. 34, se muestra el certificado de la AC visto con la herramienta de OpenSSL

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4002123767724990828 (0x378a665cd265616c)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=MX, O=UNAM, OU=UNAMgrid, CN=PKIUNAMgrid
        Validity
            Not Before: Nov 27 17:36:39 2015 GMT
            Not After : Nov 27 17:36:39 2025 GMT
        Subject: C=MX, O=UNAM, OU=UNAMgrid, CN=PKIUNAMgrid
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:c3:e3:0f:7d:b4:f0:84:50:08:93:c7:dc:f1:40:
                    7b:41:fd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                16:69:77:92:0A:97:01:04:11:2E:BE:21:5E:CF:C4:7C:78:B9:79:2E
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:
                keyid:16:69:77:92:0A:97:01:04:11:2E:BE:21:5E:CF:C4:7C:78:B9:79:2E

            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
         11:ed:86:7e:c1:c5:1f:e3:c3:7b:d9:bf:a1:b5:6f:5b:00:e4:
```

Ilustración III. 34 Certificado de la nueva AC

III.11.2 CERTIFICADO DE USUARIO

Los certificados de usuario y servidor conservan la misma estructura, el único cambio es la dirección URL del servicio de OCSP

- Algoritmo del certificado SHA-256 (2046).
- Firma digital.
- Sin repudio.
- Cifrado de clave.
- Cifrado de datos.
- Autenticación del cliente.
- Correo seguro.
- Firma de código.
- CRL.

- Vigencia 1 año.
- OCSP.

En la Ilustración III. 35, se muestra el certificado de usuario con los cambios establecidos por TAGPMA visto con la herramienta de OpenSSL.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8952523678913863583 (0x7c3dc0da7cef1f9f)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=MX, O=UNAM, OU=UNAMgrid, CN=PKIUNAMgrid
        Validity
            Not Before: Jan  8 20:11:34 2016 GMT
            Not After : Jan  8 20:11:34 2017 GMT
        Subject: C=MX, O=UNAM, OU=UNAMgrid, CN=VomsUserFinal
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c0:8f:9f:5a:df:31:84:8d:b2:62:a0:c7:ab:f7:
                    b7:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                OCSP - URI:http://ca.unamgrid.unam.mx/ejbca/publicweb/status/ocsp

            X509v3 Subject Key Identifier:
                DE:34:13:65:0C:B4:B7:B9:D9:8B:A9:0F:BE:E4:A2:DE:42:FB:BF:C2
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:16:69:77:92:0A:97:01:04:11:2E:BE:21:5E:CF:C4:7C:78:B9:79:2E

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://ca.unamgrid.unam.mx/ejbca/publicweb/webdist
                /certdist?cmd=crl&issuer=C=MX,O=UNAM,OU=UNAMgrid,CN=PKIUNAMgrid
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment,
                Data Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, Code Signing, E-mail Protection
            X509v3 Subject Alternative Name:
                email:dudas_firma@unam.mx
    Signature Algorithm: sha256WithRSAEncryption
         7f:3f:ab:14:22:c9:36:0a:e0:1e:5a:12:08:45:58:d2:4d:ba:
```

Ilustración III. 35 Certificado de usuario UNAMgrid nueva versión

III.11.3 CERTIFICADO DE SERVIDOR

Así como en el certificado de usuario se agregó el atributo de OCSP, y la única diferencia que tiene con el certificado de usuario es el atributo extendido que es autenticación de servidor.

En la Ilustración III. 36, se muestra el certificado de servidor visto con la herramienta de OpenSSL

```
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number: 2504621123034517989 (0x22c233a42f6991e5)
  Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=MX, O=UNAM, OU=UNAMgrid, CN=PKIUNAMgrid
      Validity
          Not Before: Jan 15 18:54:48 2016 GMT
          Not After : Jan 15 18:54:48 2017 GMT
      Subject: C=MX, O=UNAM, OU=UNAMgrid, CN=pruebas.host.unamgrid.mx
      Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
              Public-Key: (2048 bit)
              Modulus:
                  00:b1:57:c4:7d:df:fc:ff:69:d7:23:4a:c6:05:f5:
                  fc:15
              Exponent: 65537 (0x10001)
      X509v3 extensions:
          Authority Information Access:
              OCSP - URI:http://ca.unamgrid.unam.mx/ejbca/publicweb/status/ocsp

          X509v3 Subject Key Identifier:
              66:61:A2:DC:0F:23:5A:61:43:11:0E:15:18:06:A0:07:E2:09:26:3B
          X509v3 Basic Constraints: critical
              CA:FALSE
          X509v3 Authority Key Identifier:
              keyid:16:69:77:92:0A:97:01:04:11:2E:BE:21:5E:CF:C4:7C:78:B9:79:2E

          X509v3 CRL Distribution Points:

              Full Name:
                URI:http://ca.unamgrid.unam.mx/ejbca/publicweb/webdist/certdist
                ?cmd=crl&issuer=C=MX,O=UNAM,OU=UNAMgrid,CN=PKIUNAMgrid
          X509v3 Key Usage: critical
              Digital Signature, Non Repudiation, Key Encipherment,
              Data Encipherment
          X509v3 Extended Key Usage:
              TLS Web Server Authentication, TLS Web Client Authentication,
              Code Signing, E-mail Protection
          X509v3 Subject Alternative Name:
              email:dudas_firma@unam.mx
  Signature Algorithm: sha256WithRSAEncryption
       06:0e:df:0d:50:97:cb:98:dc:82:a0:7b:e9:c9:b8:b6:38:c4:
```

Ilustración III. 36 Certificado de usuario UNAMgrid nueva versión

III.12 ESTADO ACTUAL DE LA NUEVA VERSIÓN

Actualmente la nueva versión de UNAMgrid está a la espera de la revisión de TAGPMA y el IGTF, a continuación, se describen los pasos para ponerla en producción:

- TAGPMA hará una revisión de la operación del UNAMgrid en donde dará por acreditada la AC.
- TAGPMA hará una revisión de la nueva versión del CPS
- Una vez que sea acreditada la AC UNAMgrid, se actualizarán los repositorios y la información en las oficinas de TAGPMA, así como en el IGTF se publicará el nuevo rpm para la su distribución.
- De acuerdo a lo estipulado en el actual CPS la lista de revocación de certificados (CRL) deberán ser en versión 2.
- Se publicarán video tutoriales que ayuden en el procedimiento de solicitud y obtención de un certificado.
- Se les enviará un correo a los usuarios para notificarles la migración de plataforma, por lo que tendrán un mes para el proceso de recertificación.

CONCLUSIONES

Al término del proyecto, se cubrieron todos los requerimientos establecidos por TAGPMA, al mismo tiempo se aprovechó el poder actualizar toda la infraestructura tanto el hardware y el software, así como robustecer el resguardo de la llave raíz de la Autoridad Certificadora con el dispositivo de seguridad.

El proyecto al día 09 de junio de 2016, está en la etapa final de revisión, por lo que en un plazo de un mes máximo se tiene previsto liberar el mismo, así mismo el 01 de junio de 2016 se realizó la presentación oficial ante los administradores de la grid, por lo que sólo estamos a la espera de la última revisión de TAGPMA para poner en línea la nueva UNAMgrid CA.

Uno de los beneficios adicionales fue la integración del módulo criptográfico que garantiza el resguardo de la llave privada de la AC, que es la que firmará los certificados tanto de usuario como de servidor. Adicionalmente se integró el protocolo de OCSP, para que los sistemas grid puedan consultar el estatus de un certificado de manera individual, sin la necesidad de la descarga y la lectura de la CRL convencional, por lo que el proceso de verificación de estatus será más rápido. La ventaja más importante es que se acortó el tiempo de respuesta de solicitud, ya que se puede aprobar una solicitud casi en cualquier lado con una simple conexión a internet.

El proyecto no termina en la generación de certificados, ya que hay que estar actualizados en materia de Autoridades Certificadoras, por lo que, conforme salgan actualizaciones se evaluarán y se implementarán, para que UNAMgrid CA este actualizada. Algunos miembros de TAGPMA quieren migrar de plataforma a EJBCA por lo que el Departamento de Firma Electrónica les brindará asesoría y la transferencia de conocimiento para sus migraciones.

El proyecto de migración de plataforma me permitió profundizar en conocimientos y buscar soluciones para resolver la compatibilidad de servicios con los sistemas que nos consumen. Al principio sólo fue el proyecto de generar una nueva AC, pero conforme se avanzaba en el proyecto había factores como el funcionamiento de una grid que debí de resolver.

También considero relevante el desarrollo de este proyecto, porque me brindó la oportunidad de destacar mis habilidades en planeación de proyectos de ingeniería de cómputo.

Finalmente, cabe mencionar que el proyecto requirió de un conocimiento especializado en materia de AC´s, grid y la investigación a fondo de todos los procesos que intervienen, no sólo en la emisión y entrega de certificados digitales, sino también en los sistemas que lo validan, este proyecto me permitió profundizar en estos conceptos y lograr el objetivo encomendado de proveer a la UNAM de una AC para recursos grid.

GLOSARIO
DEFINICIONES

Autenticación
El proceso en el que se establece que los individuos, organizaciones o cosas son quien o lo que dicen ser. En el contexto de una PKI, autenticación puede ser el proceso de establecer que un individuo u organización que solicite o que pretenda ingresar a algo bajo un cierto nombre es, de hecho, el individuo u organización identificada.

Autenticación también puede referirse a un servicio de seguridad que proporciona garantías de que las personas, organizaciones o cosas son quien o lo que dicen ser, o que un mensaje u otros datos se originaron a partir de un individuo, organización o dispositivo específico.

Certificado personal
Un certificado utilizado para la autenticación, que permite establecer una identidad como persona en la grid. Siempre representará a un individuo.

Certificado servidor
Un certificado para la certificación del servidor y el cifrado de las comunicaciones (SSL / TSL). Cada certificado representa a una sola máquina. Los certificados de host se utilizan internamente por el servicio PKI y no se emiten a otros sitios.

Cliente OCSP
Aplicación (cliente) que permite la verificación del servicio OCSP, su implementación y operación es responsabilidad del tercero (parte confiada) y deberá cumplir con el RFC 2560.

Identificación
El proceso de establecer la identidad de un individuo u organización, es decir, para demostrar que un individuo u organización es un individuo u organización específica. En el contexto de una PKI, la identificación se refiere a dos procesos: (1) establecer que un nombre dado de un individuo u organización corresponde a una identidad real mundo de un individuo u organización, y (2) determinar que un individuo u organización que solicite o la búsqueda de acceso a algo bajo ese nombre es, de hecho, el nombre individuo u organización.

Una persona que busca la identificación puede ser un solicitante de certificado, o una persona que busca el acceso a una aplicación de red o software, como un administrador de AC que solicite el acceso a los sistemas de AC.

Organización Virtual (VO)
Una organización que se ha creado para representar un esfuerzo de investigación o desarrollo en particular independiente de los sitios físicos en que el científico o ingenieros trabajan (por ejemplo, PPDG, FNC, EDG, etc).

Repositorio

Un área de almacenamiento, por lo general en línea, que contiene listas de certificados emitidos, CRL, documentos de política, etc.

RFC 3280
Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002.

RFC 1778
The String Representation of Standard Attribute Syntaxes.

Servicio Consulta de Certificados en Línea (OSCP Responder)
Servicio que permite conocer el estado de vigencia de los certificados en línea en tiempo real.

Suscriptor (Titular)
A veces llamado entidad final, es una persona o servidor a quien se expide un certificado digital.

X.509 versión 3
Estándar desarrollado por la Unión Internacional de Telecomunicaciones (organización internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Llave Pública y los Certificados digitales.

Acrónimos

AC (Autoridad de Certificación)
Una autoridad de confianza para uno o más usuarios (suscriptores) que crea y asigna certificados de llave pública y es responsable de ellos durante toda su vida útil. Certificados de identidad X.509 que emite la entidad / sistema (coloca un nombre de objeto y la llave pública en un documento y luego firma digitalmente el documento utilizando la llave privada de la AC).

CENAM (Centro Nacional de Metrología)
Laboratorio nacional de referencia en materia de mediciones. Es responsable de establecer y mantener los patrones nacionales, ofrecer servicios metrológicos como calibración de instrumentos y patrones. Proporciona servicios de sincronía y calibración de sistemas informáticos con la hora oficial de los Estados Unidos Mexicanos.

CPS (Certificate Practice Statement)
Una declaración de las prácticas, que una autoridad de certificación emplea en la emisión de certificados.

CRL (Certificate Revocation List)
Listado de los certificados revocados o suspendidos que es firmada con la llave privada de la CA.

CSR (solicitud de firma de certificado)
Un mensaje enviado a una AC con el fin de solicitar un certificado digital. Contiene información de identificación del solicitante y la llave pública elegida por el

solicitante. Si se aprueba la solicitud, el AC devolverá un certificado que ha sido firmado digitalmente con la llave privada de la AC.

DRP (Disaster Recovery Plan)
Plan de recuperación ante desastres, proceso que permite mantener la continuidad de los servicios mediante el establecimiento de medidas para recuperar los datos, hardware y software crítico de la aplicación o sistema en caso de un desastre natural, evento inesperado o error humano.

HSM (Hardware Security Module)
Dispositivo criptográfico basado en hardware que genera, almacena y protege llaves criptográficas, garantizando la unicidad e integridad de la llave raíz.

IGTF (International Grid Trust Federation)
Comunidad científica internacional de Grids computacionales cuyo principal objetivo es el avance de la ciencia y la ingeniería. La promesa de Grids computacionales globales requiere de políticas y procedimientos que identifiquen de forma fiable a los titulares (suscritores) y los recursos Grid. Se han establecido Policy Management Authorities (PMA), cada una es responsable de la gestión y autenticación en sus grids.

NTP (Network Time Protocol)
Protocolo de internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

OCSP (Online Certificate Status Protocol)
Protocolo para verificación de estatus de certificados en línea.

RA (Autoridad de Registro)
Entidad responsable de la identificación y autenticación de los titulares del certificado, pero no firma o emite certificados.

RFC (Request for comments)
Publicación que recopila las mejores prácticas, procesos, procedimientos avalados por la IETF y que son convención a nivel internacional.

TAGPMA (The Americas Grid PMA)
Federación de entidades de certificación de grid y anexos que operan en la región conocida como las Américas. Se regirá por una Policy Management Authority (PMA), que está formada por miembros con responsabilidades en grid en las Américas. El objetivo de la federación es facilitar las relaciones de confianza necesarias entre dominios para desplegar las redes en las Américas y en el mundo.

UNAM
Universidad Nacional Autónoma de México.

REFERENCIAS

Universidad Nacional Autónoma de México (UNAM). 2016. *Firma Electrónica Avanzada*. Recuperado el 12 de mayo de 2016, de http://sistemas.tic.unam.mx/?q=firma_electronica

IGTF Distribution of Authority Trust Anchors (PKI Certificate format). 10 May, 2016 *Acuerdo de implementación de Firma Electrónica Avanzada*, Recuperado 12 de mayo de 2016, de http://www.fea.unam.mx/sites/default/files/archivos/acuerdo_para_la_implementacion.pdf

Universidad Nacional Autónoma de México (UNAM). 19 de abril de 2012.*Universidad Nacional Autónoma de México. ¿Quiénes Somos?* Recuperado 12 de mayo de 2016, de http://www.tic.unam.mx/mision.html

Universidad Nacional Autónoma de México. 30 de noviembre de 2015, *Organigrama* Recuperado 12 mayo de 2016 http://www.tic.unam.mx/organigrama.html

Sintesis UNACAR. 2015. *Firma electrónica Avanzada, una realidad en la UNCAR*, Recuperado 19 mayo de 2016, de http://www.unacar.mx/comunicacion_social_unacar/unacar/noticia.php?id=891

Coordinación de Seguridad de la información. 2015 *Coordinación de Seguridad de la información*, Recuperado 22 de mayo de 2016, de http://www.seguridad.unam.mx/index.html

TAGPMA. 02 de septiembre 2009. *TAGPMA Welcome*, Recuperado 22 de mayo de 2016, de http://www.tagpma.org/

NICKHEF. 11 de mayo de 2016. *IGTF: Interoperable Global Trust Federation*, Recuperado 22 de mayo de 2016, de https://www.igtf.net/

UNAMgridCA. 14 de mayo de 2014. *UNAMgridCPSv0.1a*, Recuperado 22 de mayo de 2016, de https://ca.unamgrid.unam.mx/grid/pdf/UNAMgridCPSv1a.pdf

UNAMgridCA. 14 de mayo de 2014. *Certificado CA en formato CRT (browser import)*, Recuperado 22 de mayo de 2016, de https://ca.unamgrid.unam.mx/pub/cacert/cacert.crt

Instituto de ciencias nucleares UNAM. Secretaría Técnica de Cómputo, Redes y Telecomunicaciones, Recuperado 23 de mayo de 2016, de http://www.nuclecu.unam.mx/secretaria_de_computo_redes_y_telecomunicaciones.php

escience MÉXICO. 26 de junio de 2009. *Proyectos instruccionales y aplicaciones*, Recuperado 23 de mayo de 2016, de http://www.e-science.unam.mx/index.jsp

EUGridPMA. *Building Trust for Distributed IT Infrastructures for Research*, Recuperado 22 de mayo de 2016, de https://www.eugridpma.org/

CNIC/SDG Grid CA. 9 de noviembre de 2012. *Asia Pacific Grid Policy Management Authority*, Recuperado 22 de mayo de 2016, de http://www.apgridpma.org/

Main.TagPmaTv160511r1.8. 11 de mayo de 2016. *TAGPMA Agenda 11 May 2016*, Recuperado 23 de mayo de 2016, de http://tagpma.es.net/wiki/bin/view/Main/TagPmaTv160511

EUgridpma. *IGTF time line statement on SHA-2 Secure Digest Mechanisms*, Recuperado 22 de mayo de 2016, de https://www.eugridpma.org/documentation/hashrat/sha2-timeline

rfcmarkup 1.118. Junio de 2013 *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, Recuperado 23 de mayo de 2016, de https://tools.ietf.org/html/rfc6960

OpenCA Group. 5 de agosto de 2005.*OpenCA Guide for Versions 0.9.2*+, Recuperado 25 de mayo de 2016, de http://www2.openxpki.org/docs/guide/html_chunked/

OpenCA PKI. 8 de agosto de 2013. *OPEN SOURCE PKI MANAGEMENT SOFTWARE*, Recuperado 25 de mayo de 2016, de https://www.openca.org/projects/openca/

PrimeKey Solutions AB. EJBCA®. 13 de mayo de 2016. *EJBCA PKI CA, Recuperado 25 de mayo de 2016*, de https://www.ejbca.org/

RFC 3280. Abril 2012. *Internet X.509 Public Key Infrastructure*, Recuperado 24 de mayo de 2016, de https://www.ietf.org/rfc/rfc3280.txt

OpenSSL Software Foundation. 2015. *OpenSSL*, Recuperado 25 de mayo de 2016, de https://www.openssl.org/

The PostgreSQL Global Development Group. 1996-2016*. PostgresSQL*, Recuperado 25 de mayo de 2016, de https://www.postgresql.org/

The Apache Software Foundation. 1997-2016. *Apache 2*, Recuperado 25 de mayo de 2016, de https://httpd.apache.org/

Mware, Inc. 2016. *VMware*, Recuperado 25 de mayo de 2016, de http://www.vmware.com/mx

Red Hat, Inc. 2016. *Red Hat SUMMIT*. Recuperado 26 de mayo de 2016, de https://www.redhat.com/es

Red Hat, Inc. 2016. *JBossDeveloper*, Recuperado 26 de mayo de 2016, de http://www.jboss.org/

OSUOSL. Noviembre 2002. *QEMU open source machine processor emulator*, Recuperado 26 de mayo de 2016, de http://wiki.qemu.org/Main_Page

FIPS PUB 140-2. 25 de mayo de 2001. *SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*, Recuperado 23 de mayo de 2016, de http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Seagate Technology LLC. 2016. *Tecnología estándar FIPS 140-2 y unidad de cifrado automático*, Recuperado 23 de mayo de 2016, de http://www.seagate.com/la/es/tech-insights/fips-140-2-standard-and-self-encrypting-drive-technology-master-ti/

Red Hat Enterprise Linux 4: Manual de referencia, Recuperado 26 de mayo de 2016, de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

www.ntp.org. 27 de abril de 2017. *NTP: The Network Time Protocol*, Recuperado 26 de mayo de 2016, de http://www.ntp.org/

©Oracle. *Java SE Documentation*, Recuperado 26 de mayo de 2016, de http://www.oracle.com/technetwork/java/javase/documentation/index.html

EELA. 23-de abril de 2014. *E-Infrastructure shared between Europe and Latin America*. http://www.eu-eela.eu/first-phase.php

R. Housley, W. Ford, W. Polk and D. enero 1999 *Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 2459, Recuperado 08 febrero de 2016 http://www.ietf.org/rfc/rfc2459.txt

R. Housley, W. Polk, W. Ford and D. Solo. Abril 2002. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280*. Recuperado 10 de febrero de 2016 http://www.ietf.org/rfc/rfc3280.txt

S. Chokani and W. Ford. Marzo 1999. *"Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework", RFC 2527*. Recuperado 10 de febrero de 2016. De http://www.ietf.org/rfc/rfc2527.txt

S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu. Noviembre 2003. "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, [reemplaza a RFC 2527].* Recuperado 24 de marzo de 2016 http://www.ietf.org/rfc/rfc3647.txt

Entérate en línea. Septiembre de 2006. *Tutorial en grids computacionales en la UNAM*. Recuperado 8 de abril de 2016 http://www.enterate.unam.mx/Articulos/2006/septiembre/grids.htm

Entérate en línea. Noviembre de 2004. *Internet 2*. Recuperado 04 de febrero de 2016 http://www.enterate.unam.mx/Articulos/2004/noviembre/internet2.htm

Universidad Nacional Autónoma de México (UNAM). 2010-2016. *Ciencia UNAM Colabora la UNAM en megaproyecto internacional de computación*. Recuperado 04 abril de 2016 http://ciencia.unam.mx/leer/89/Colabora_la_UNAM_en_megaproyecto_internacional_de_computacion

Universidad Nacional Autonóma de México -- Centro de Ciencias Genómicas. 13 de febrero de 2009. *Tutorial EELA-2 en el Centro de Ciencias Genómicas*. Recuperado 04 de abril de 2016 http://www.ccg.unam.mx/es/news/tutorial_eela_2_en_el_centro_de_ciencias_gen%C3%B3