DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA:

"IMPLEMENTACIÓN DE UNA AUTORIDAD CERTIFICADORA NO ACREDITADA EN AMBIENTE SMART GRID"

AUTORES: QUINTANILLA VITERI, JUAN PABLO
SÁNCHEZ PERUGACHI, ADRIÁN MAXIMILIANO

DIRECTOR: ING. GALARRAGA, FERNANDO
CODIRECTOR: ING. CAIZAHUANO, CARLOS

SANGOLQUÍ
2015

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Señor QUINTANILLA VITERI JUAN PABLO y el Sr. SÁNCHEZ PERUGACHI ADRIÁN MAXIMILIANO, como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA.

Sanqolquí, Noviembre 2015

Ing. Fernando Galarraga.
DIRECTOR DE TESIS

Ing. Carlos Caizaguano
CODIRECTOR DE TESIS

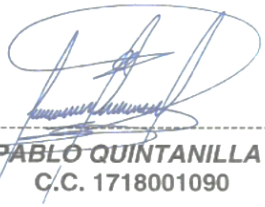
AUTORÍA DE RESPONSABILIDAD

Nosotros, QUINTANILLA VITERI JUAN PABLO y SÁNCHEZ PERUGACHI ADRIÁN MAXIMILIANO, declaramos que el presente trabajo es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación personal y que he consultado las referencias bibliográficas que se incluyen en el documento.

La Universidad de las Fuerzas Armadas ESPE puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual por su reglamente y por la normativa institucional vigente.

Sangolquí, Noviembre 2015

ADRIÁN MAXIMILIANO SÁNCHEZ PERUGACHI
C.C. 1003061965



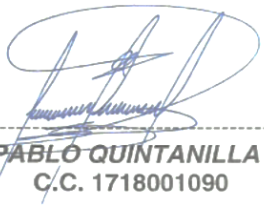
JUAN PABLO QUINTANILLA VITERI
C.C. 1718001090

AUTORIZACIÓN

Nosotros, QUINTANILLA VITERI JUAN PABLO y SÁNCHEZ PERUGACHI ADRIÁN MAXIMILIANO, autorizamos a la Universidad de las Fuerzas Armadas ESPE la publicación, en la biblioteca virtual de la institución, del trabajo de titulación "IMPLEMENTACIÓN DE UNA AUTORIDAD CERTIFICADORA NO ACREDITADA EN AMBIENTE SMART GRID", cuyo contenido, ideas y criterios son de nuestra responsabilidad y autoría.

Sangolquí, Noviembre 2015

ADRIÁN MAXIMILIANO SÁNCHEZ PERUGACHI
C.C. 1003061965



JUAN PABLO QUINTANILLA VITERI
C.C. 1718001090

DEDICATORIA

Esta tesis la dedico a Dios todopoderoso, por ser mi mano derecha, mi sustento, el que me ha dado la capacidad, la valentía y la fortaleza para que este sueño se hiciera realidad.

A mis padres, Luis y Ximena, regalo maravilloso que Dios me ha dado, por su apoyo incondicional, por sus esfuerzos y sacrificios que han hecho por mí, para que este sueño hoy fuera una realidad.

Juan Pablo Quintanilla Viteri

DEDICATORIA

El resultado consecuente de este trabajo está dedicado a la memoria de mi padre Julio Aníbal Sánchez.

Adrián Sánchez

AGRADECIMIENTO

Gracias a todas las personas de la Universidad de las Fuerzas Armadas, por su atención y amabilidad en todo lo referente a mi vida como alumno.

Ante el gran número de personas que de diferente forma me han ayudado en realizar el esfuerzo de comprender un tema cuya importancia se manifiesta en varios escenarios.

Son muchos a quienes les debo reconocer su contribución. Algunos tal vez ni lo recuerden, incluso no han sido conscientes de su aporte. Pero, yo les guardo un recuerdo y un agradecimiento muy particular, por su colaboración.

Gracias, muchas gracias.

Juan Pablo Quintanilla Viteri

AGRADECIMIENTO

Los fracasos y las derrotas suelen materializarse por causa de no haber actuado o tomado decisiones en el tiempo adecuado, pertinente, oportuno. En ocasiones, nos dejamos motivar y convencer por nuestros impulsos, por nuestros instintos, y acabamos por desarrollar esfuerzos tras el intenso deseo de lograr cosas, ignorando que todo tiene su tiempo y que por más que se desee alcanzar algún objetivo, este no se obtendrá, si las cosas no se hacen bien y además en su debido momento.

Agradezco a todas las personas que aparecieron en mi vida en el momento adecuado.

Adrián Sánchez

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

RESUMEN

El propósito de este trabajo fue crear una Infraestructura de Clave Pública basado en Smart Grid para el Sistema Nacional de Educación Superior del Ecuador SENECYT; bajo un marco investigativo, se utilizó las herramientas provistas por parte de Globus Alliance, "Globus Toolkit"; La cual permite la construcción de Grids computacionales, y provee herramientas para su administración y configuración, tanto en ambientes reales, como de investigación. Esta investigación fue ejecutada, conjuntamente con una recopilación de los conceptos básicos de certificación digital, elementos y mecanismos básicos de seguridad de una Infraestructura de clave pública, elementos propios que intervienen en un ambiente Grid.

Palabras Clave:

- PKI
- AC
- AR
- Smart Grid
- Globus Toolkit
- X509
- SENECYT.

ABSTRACT

The purpose of this work was to create a Public Key Infrastructure based on Smart Grid for the National System of Higher Education of Ecuador SENECYT; under a research framework, the tools provided by the Globus Alliance, "Globus Toolkit," which allows the construction of computational grids, and provide tools for administration and configuration, both in real environments, such research was used. This research was carried out, together with a compilation of the basics of digital certification, basic elements and security Public Key Infrastructure, elements involved in Grid environment mechanisms.

KeyWords:

- PKI
- AC
- AR
- Smart Grid
- Globus Toolkit
- X509
- SENECYT.

CAPÍTULO 1

MARCO METODOLÓGICO

El intercambio de información día a día está relacionada más con la realidad de cualquier institución, de esta manera es importante poseer un certificado digital que acredite la veracidad de una manera irrefutable, de esta manera permita garantizar tramites seguros y mucho más rápidos, contando con los elementos principales de la autenticidad, integridad, confidencialidad y no repudio.

El Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE) permite la planificación institucional, que incluye el diseño del desarrollo de ciertas políticas y la monitoreo de los objetivos del Plan Nacional mediante la gestión de datos y la difusión de información.

1.1 Antecedentes

La consolidación de la arquitectura orientada a servicios OGSA (Open Grid Service Architecture), llevada a cabo orientada mente por el grupo del trabajo en el global Grid Forum (GGF), en la actualidad OGF (Open Grid Forum), ha permitido el desarrollo del modelo de computación distribuida y de nuevos espacios de colaboración para equipos de trabajo internacionales y multidisciplinares en diversos sectores como la ingeniería aeroespacial, diseño automovilístico, investigación, educación superior, energías renovables, industria farmacéutica e incluso otros como la banca, la industria de entrenamiento y multimedia. Mientras que el Grid Computing había sido tradicionalmente descrito en términos de procesamiento de gran volumen de datos, en la actualidad el Grid Computing se enmarca en los conceptos de espacio de colaboración y organización virtual (VO) abierto sobre internet.

Son varias las empresas que han adoptado un Gestor de Contenidos, facilitando la creación de nuevas oportunidades de negocios electrónicos obteniendo así el máximo provecho de sus sistemas de información.

1.2 Planteamiento del Problema

Actualmente la información no tiene por qué ser aislada para el beneficio de una sola institución sino que debe ser difundida de manera segura para que otras instituciones se puedan beneficiar y a la vez aportar con conocimiento para que unificando esfuerzos se logre un crecimiento mutuo como formadoras de nuevos profesionales del Ecuador.

Hoy en día el Sistema Nacional Educación Superior no cuentan con ningún sistema que garantice la validez jurídica de los documentos debido a que no disponen de herramientas informáticas que les ayude a agilizar procesos electrónicamente, mucho menos para poder compartir dicha información.

Los sistemas de redes inteligentes y las redes, tales como inteligencia distribuida y capacidades de banda ancha, pueden mejorar enormemente la eficiencia y fiabilidad de cualquier tipo de trabajo, así también empiezan a aparecer nuevas vulnerabilidades, bajo este contexto si no son trabajadas con todos los controles de seguridad apropiados, no serán optimizados y aprovechados al máximo de su capacidad.

1.3 Justificación

Grid Computing son parte de las 10 tecnologías más estratégicas a nivel mundial. Estos paradigmas aplicados al estudio de la interoperabilidad basada en Grid Computing y aplicados a una PKI fiable y segura que prometen cambiar radicalmente la forma de trabajar de las empresas, la manera de hacer negocios, la forma de relacionarse entre las personas y en definitiva cambiar la sociedad tal y como en su día supuso la aparición del e-mail o Internet. Por lo tanto, las empresas ecuatorianas no pueden adoptar una actitud pasiva ante la tecnología Grid.

En los últimos años, la tecnología Grid ha evolucionado de ser una tecnología diseñada principalmente para cubrir las necesidades de la comunidad de computación de altas prestaciones, hacia un marco abierto para los dominios orientados al soporte y desarrollo de negocios en las empresas. Esta evolución del Grid de la "e-ciencia" hacia el Grid de "negocio" ha sido complementada por los esfuerzos que permitan aumentar la automatización y reducir la complejidad de los sistemas con el objetivo de establecer una completa integración de los recursos heterogéneos y distribuidos que son ofrecidos como servicios de certificación digital.

1.4 Objetivos

1.4.1 Objetivo General

- Desarrollar una PKI basado en Grid Computing para el Sistema Nacional de Educación Superior del Ecuador.

1.4.2 Objetivos Específicos

- Instituir un marco conceptual uniforme para establecer las interacciones y los roles entre los componentes de una infraestructura de certificación digital.
- Identificar los servicios de certificación digital basadas en una PKI en Smart Grid.
- Definir las posibles aplicaciones seguras basadas en una PKI en Smart Grid.

1.5 Alcance

La infraestructura de seguridad de mayor uso en Grid Computing es GSI (Grid Security Infrastructure), la misma utiliza certificados X.509 para identificar entidades en el Grid, en ella cada usuario es identificado por un único certificado digital y los procesos que el usuario lanza utilizan ese mismo certificado, pero para efectos prácticos, los usuarios esperan autenticarse utilizando una combinación de cuenta de

usuario y palabra clave. Para cumplir simultáneamente con ambos requisitos, los portales Grid operan utilizando mecanismos que automáticamente suplen las credenciales reconocidas en la Organización Virtual (VO) luego de que el usuario logra autenticarse utilizando una combinación de cuenta de usuario y palabra clave que coincide con una combinación almacenada en la base de datos de cuentas del dominio de seguridad al que el usuario pertenece.

GSI es, tal vez, la infraestructura que más dificultad ofrece por el carácter distribuido y heterogéneo de sus componentes que forman parte de la tecnología Grid. Un Grid Computing se basa en la criptografía de clave pública; los conceptos de clave pública y privada y el de firma digital, son básicos dentro de Grid Computing, y de hecho, la implementación de una PKI en un entorno de Grid Computing requiere una CA (Certification Authority) y una RA (Registration Authority), dependiendo del marco legal existente.

Las necesidades de seguridad en una Grid Computing son las siguientes:

1. Comunicaciones seguras (autenticación, confidencialidad e integridad de datos) entre los componentes del Grid.
2. La necesidad de soportar un modelo de seguridad por encima de los límites Organizacionales.
3. La necesidad de un Logon Único (Single Sign On) con delegación de credenciales y un sistema adecuado de control de acceso a los recursos sin la necesidad de múltiples autenticaciones.

CAPÍTULO 2

MARCO TEÓRICO

En este capítulo se pone a consideración sobre los conceptos de seguridad de la información y seguridad informática y se establece una explicación sobre los pilares sobre los que se basa la seguridad de la información. También sobre los Sistemas de Altas Prestaciones, describiendo los principales paradigmas y objetivos de la programación paralela. Además, se destaca la optimización a múltiples niveles como mecanismo para obtener las máximas prestaciones de un sistema de computación. Posteriormente, se detallan la Grid Computing, los cuales se toman en cuenta junto con la estructura del SENECYT para establecer bajo términos lógicos las normas y procedimientos para el Sistema Nacional de Educación Superior.

2.1 Seguridad de la Información

La seguridad de la información indica que "un sistema está libre de todo peligro, daño o riesgo" y dicha información tiene notabilidad en un contexto determinado que por tanto, hay que resguardarlo.

Al especificar la seguridad de la información determina que es un conjunto de medidas técnicas, organizativas y legales que consienten en la organización protegiendo la confidencialidad, integridad y disponibilidad de su sistema de información.

Permite además la digitalización de información reduciendo el espacio ocupado, facilitando su análisis y proceso. Se obtiene ganancia en espacio, acceso, rapidez en el procesamiento de dicha información.

De la misma manera aparecen dificultades ligadas a esas disposiciones. Si es más fácil trasladar la información también hay más posibilidades de que en el camino desaparezca.

"La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad

de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.” (Trejo, s.f.) .

2.1.1 Seguridad Informática

Es la protección de una gama de amenazas para salvaguardar el proceso de las operaciones del negocio las cuales pueden ser ocasionadas dentro o fuera de la organización, disminuyendo los daños que estas amenazas causarían ampliando las oportunidades de negocios.

“Seguridad de los Sistemas de Información consiste en la protección de los sistemas de información respecto al acceso no autorizado o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicio para los usuarios autorizados, incluyendo a que las medidas necesarias para detectar, documentar y contrarrestar dichas amenazas.” (Valera)

La seguridad de la información se obtiene desarrollando mediante un conjunto de controles efectivos, que se dividen en políticas, prácticas, manual de funciones, procedimientos, estructuras organizativas, planes de contingencia y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, para asegurar que se cumplan los objetivos.

“La Seguridad de la Información está apoyada en 3 pilares fundamentales de la seguridad estos son:” (García, 2009)

1. **Confidencialidad:** Se refiere a la limitación de acceso a la información y divulgación a los usuarios autorizados "personas adecuadas" y prevenir el acceso o divulgación a los no autorizados "gente equivocada."

2. **Integridad:** Implica mantener la consistencia, precisión y fiabilidad de los datos a través de todo su ciclo de vida. Los datos no se debe cambiar en tránsito, y se deben tomar medidas para asegurar que los datos no pueden ser alterados por personas no autorizadas.

3. **Disponibilidad:** Disponibilidad de la información se refiere a garantizar que las personas autorizadas puedan acceder a la información cuando sea necesa-

rio. La información sólo tiene valor si la gente adecuada puedan acceder a él en los momentos adecuados.

Figura 1. Pilares de la Seguridad Informática

Fuente *(Sasia, 2011)*

Las características de la seguridad informática son:

- **Autenticidad**: Asegura el origen de la información, la identidad de usuarios al momento de un acceso debe ser validada, de modo que se puede demostrar que es quien dice ser.
- **No repudio:** Consiste en que a los emisores o a los receptores para negar un mensaje transmitido, el receptor puede probar que el mensaje fue enviado por el presunto emisor.
- **Trazabilidad:** Conjunto de acciones, medidas y ordenamientos técnicos que autoricen la autentificación y el registro de la información desde que esta es enviada hasta llegar a su destino.

2.1.2 Mecanismos de Seguridad

Herramienta que se utiliza para fortalecer la confidencialidad, la integridad y la disponibilidad de cualquier tipo de sistema informático.

- **Preventivos:** Se refiere a los controles que impiden la pérdida o daños de la información que se produzcan.
- **Detectivos**: Son los responsables de vigilar la actividad para identificar las anomalías en las prácticas o procedimientos.
- **Correctivos:** Es el que encargado de restaurar el sistema o proceso de volver al estado anterior a un hecho que produjo daño.

a) Mecanismo de Seguridad "Confidencialidad"

- **Cifrado de datos:** Es el proceso encargado que se sigue para enmascarar los datos, con el objetivo de ser enigmáticos para cualquier agente no autorizado.

  Al usar una clave especial y siguiendo una secuencia de pasos pre-establecidos, los datos se enmascaran usando un "algoritmo de cifrado".

b) Mecanismo de Seguridad "Integridad"

- **Software anti-virus:** Su función específica es de ejercer el control preventivo, detectivo y correctivo sobre el virus infectado en el sistema.
- **Software "firewall":** Es el encargado de ejercer el control preventivo y detectivo sobre intromisiones no deseadas a los sistemas.
- **Software para sincronizar transacciones:** Su función es ejercer el control los servicios que se aplican a los datos.

c) Mecanismo de Seguridad "Disponibilidad"

- **Planes de contingencia:** Es en que se encarga de especificar los pasos a seguir en caso de que se interrumpa la actividad del sistema, enfocándose en la recuperación de la funcionalidad.

  Depende el tipo de contingencia los pasos que puedan ejecutarse, siendo personas entrenadas, sistemas informáticos especialmente programados en ambos elementos.

- **Respaldo de los datos:** Es un proceso importante en el que se encarga de copiar los elementos de información que pueden ser recibidos, transmitidos, almacenados, procesados o generados por el sistema.

Entre los mecanismos de seguridad más avanzados se cuenta con:

- **Certificado Digital**

El certificado digital es el que permite autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones a través de las redes abiertas de comunicación, por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación.

La entidad lleva como nombre "Autoridad Certificadora" el cual puede ser una empresa o un organismo público reconocida en Internet.

"El certificado digital tiene como función principal la autentificación al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información sensible entre las partes." (Certificado Digital, 2008)

Los certificados digitales permiten:

- Identificarnos.
- Firmar digitalmente un Documento Digital.
- Seguridad de que un Documento Digital no ha sido alterado.

- **Firma Electrónica**

Una firma electrónica es una huella digital de un documento cifrado con una clave, cuyo objetivo principal es el enviar un documento firmado a través de medios electrónicos de manera que ese documento cuente con las mismas características, técnicas de seguridad y legales el mismo que proporciona un documento firmado hológrafamente.

La huella digital se obtiene aplicando un algoritmo a un mensaje el cual tiene dos características fundamentales que son:

- Es imposible volver a obtener el mensaje iniciando de la huella digital generada.
- Al cambiar el mensaje la huella digital será distinta.

Al cumplir estas características se garantiza la integridad y el no repudio del mensaje. Si el contenido del mensaje es cambiado, el indicado de verificar la firma lo va a conocer.

"La huella digital se cifra con la clave privada del certificado de la persona que firma. Aplicando los mecanismos de verificación, el receptor va a conocer quién firmó y esa persona no puede repudiar la autoría del mensaje." (Digital, 2000)

a) Amenaza

Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño (material o inmaterial) sobre los elementos (activos, recursos) de un sistema.

- **Autenticidad**: Credibilidad de una persona, servicio o elemento el cual debe ser comprobable.
- **Confidencialidad**: Protección de la información de su divulgación a terceros no autorizados.
- **Disponibilidad**: Garantizar que las personas autorizadas puedan acceder a la información cuando sea necesario.

b) Vulnerabilidades

Al ser expuestos los puntos débiles afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa. Una de las principales importancias en la implementación de la seguridad es rastrear los puntos débiles de un ambiente que se encuentra la tecnología de la información.

Una vez identificados los puntos débiles, será posible dimensionar los riesgos en el que el ambiente está expuesto definiendo las medidas de seguridad convenientes para su corrección.

De la forma en que se organizó el ambiente depende los puntos débiles en las que se maneja la información y del medio en que la misma se está utilizando.

2.2 Grid Computing

La idea específica de la tecnología en Grid Computing es aprovechar los recursos distribuidos, conectados a una red de banda ancha, mediante la utilización de un software adecuado para planificar su utilización que tenga en cuenta las prioridades de demanda de los usuarios.

Incluye mecanismos de autentificación basados en certificados digitales, y contar con una gestión basada en una instalación automatizada, flexible y dinámica.

Es importante mencionar cuales son las capas de la arquitectura Grid, estableciendo en cada capa la correspondencia con la herramienta Globus Toolkit.

2.2.1 Capa de Tejido

Es la que proporciona el recurso compartido que se accederá a través de los protocolos Grid, recursos computacionales, recursos de red. Los recursos se establecen como un sistema de ficheros distribuidos, Clúster u ordenador que genera una implementación de recursos.

- **Recursos Computacionales**

  Son los encargados de ejecutar programas para monitorizar y controlar la ejecución de los procesos. Dispone de mecanismos avanzados los indicados de determinar las características de hardware y software así como información relevante de estado actual de carga y colas de procesamiento en el caso de recursos gestionados por colas.

- **Recursos de Almacenamiento**

  Su trabajo es el transferir ficheros, que permitan el control de los recursos así como los mecanismos avanzados de reserva en los recursos. Re requiere consultas para determinar las características de hardware y software así como información relevante de carga como utilización de ancho de banda y espacio disponible.

- **Recursos de red**

  Es el mecanismo de gestión que facilita control sobre los recursos localizados para la transferencia de los datos en la red.

- **Colecciones de Código**

  Establece el almacenamiento de recursos que requiere el mecanismo para gestión de versiones de código fuente.

- **Catálogos**

  Se encarga de almacenar los recursos que requieran mecanismos para la implementación de operaciones de consulta de catálogos y sus actualizaciones.

- **Globus Toolkit**

  Fue creada principalmente para usar los componentes existentes de protocolos e interfaces de otros fabricantes, incluyendo los mecanismos necesarios que no estén proporcionados.

2.2.2 Capa de Conectividad

Define los protocolos de comunicación y autentificación necesarios para las transacciones de la red específicas de Grid. Los requerimientos de comunicación, incluyen el transporte y resolución de nombres. Los mecanismos están incluidos en el protocolo TCP/IP, en concreto las capas y aplicaciones (DNS, OSPF, RSVP), Internet (IP y ICMP) y transporte (TCP, UDP).

Las capas de conectividad, al igual que con los protocolos de comunicación, cualquier estándar de seguridad desarrollado dentro del contexto del protocolo Internet es aplicable.

Las características de autentificación para entornos son:

- Integración con varias soluciones de seguridad local.
- Entorno de seguridad común para el uso de recursos en otro Grid.
- Delegación de un conjunto de derechos de acceso de un recurso a otro.
- Única autentificación para el acceso a todos los recursos Grid definidos en la paca de tejido.

Las soluciones de seguridad proporcionan protección de la comunicación y habilitando el control sobre las decisiones de autorización.

2.2.3 Capa de Recursos

Define sobre la implementación de protocolos que realizan peticiones a las funciones de capa de tejido con la finalidad de obtener el control local de los recursos. Los protocolos se dedican exclusivamente a recursos individuales ignorando cualquier repetición y acción dirigida a colecciones distribuidas de recursos. Se puede distinguir dos clases primarias de protocolos:

- **Protocolos de Información**
  Se utilizan para obtener información sobre la estructura y el estado de un recurso, (configuración, carga actual, política de uso.)
- **Protocolos de Gestión**
  Se utiliza para negociar el acceso a un recurso compartido, especificando requerimientos de recursos (incluyendo reserva avanzada y calidad de servicio) y la operación u operaciones a ser realizadas, tales como creación de procesos o acceso a datos.
- **Lightweight Directory Access Protocol (LDAP)**
  Protocolo de acceso a catálogos.
- **Grid Resource Information Protocol (GRIP)**
  Su función es definir un protocolo estándar de información del recurso y el modelo de información asociado.
- **Grid Resource Access and Management (GRAM)**
  Protocolo basado en HTTP, utilizado para monitorizar y realizar un control computacional en dicho recurso.
- **Grid FTP**
  Es un protocolo de gestión para acceso a datos.

2.2.4 Capa Colectiva

Esta capa se encarga en la mayor parte de la coordinación de múltiples recursos, a partir de ello se puede implementar una amplia variedad de servicios de compartición

sin la necesidad de establecer nuevos requerimientos.
Los servicios que se encuentran en la capa colectiva son los siguientes:

- **Servicios de directorio**
  Permite a los usuarios realizar consultas de recursos.
- **Servicios y agentes de localización y planificación**
  Permite realizar peticiones de localización de uno o más recursos.
- **Servicios de replicación de datos**
  Brinda soporte de gestión de recursos de almacenamiento para maximizar el rendimiento en el acceso a los datos.
- **Servicio de monitorización y diagnóstico**
  Permite la monitorización de recursos cuyo objetivo es la detección de intrusos, sobrecarga.
- **Seguridad de programación Grid**
  Permite habilitar modelos de programación que se puedan integrar en entorno Grid.
- **Gestión de carga de trabajo y colaboración de entornos de trabajo**
  Permite resolución de entorno, proporcionado para la descripción, uso y gestión de flujos asíncronos de múltiples componentes.
- **Servicios de detección de Software**
  Selecciona la mejor implementación software y plataforma de ejecución.
- **Servidores de autorización de VO**
  Asegura que se cumplen las políticas comunitarias que gobiernan.
- **Servicios de contabilidad y pago VO**
  Reúne la información de recursos con el objetivo de contabilizar, establecer la cuota y limitar el uso por los miembros de la comunidad.

2.2.5 Capa de Aplicaciones

Estas aplicaciones están construidas en términos de servicios definidos específicamente para cada capa de la arquitectura Grid.

En cada capa, los protocolos establecidos, facilitan el acceso gestión de recursos, acceso a datos y detección. Las interfaces de cada capa de programación de aplica-

ciones (APIs) están implementadas desde los protocolos de intercambio de mensajes hasta las acciones determinadas. Los APIs se implementan como herramientas de desarrollo software (SDKs), el cual tiene como prioridad el utiliza protocolos para interactuar con servicios de red.

2.3 TTP

La TTP (Trusted Third Party) permite obtener una amplia gama de servicios de seguridad siendo estos representados como (servicios de confianza). Por este motivo existen varios tipos de TTPs. Los usuarios de servicios tienen dificultades cuando trabajan con diferentes de TTP siendo aquí donde depositan gran parte de confianza dentro de los procedimientos. El rol de la TTP dentro de protocolo de seguridad es determinar el rendimiento del protocolo. Por este motivo existe métodos para que pueda ser clasificados y analizados, con este fin se puede medir la confianza que los usuarios ponen en un TTP.

Por esta razón será de gran ayuda, evaluar el papel del TTPs y que a su vez los usuarios puedan escoger la entidad de confianza que sea más conveniente. Clasificar estos servicios también será útil para identificar sus requisitos y características.

Un TTP es una autoridad de seguridad de confianza para otras entidades que refieren a las actividades de seguridad, esto se explica a que una entidad deposita confianza en otra entidad cuando una anterior asume que la segunda entidad se comportara como la anterior lo espera, es decir depositando un grado de confianza en una TTP.

Una TTP es una organización con niveles de seguridad, prestando estos servicios para que sea de confianza de otras organizaciones con respecto a los servicios que presta. Las clases que se proponen para analizar el servicio de una TTP son:

- **Confianza**

  Verificable: el usuario puede demostrar el incumplimiento del servicio esto quiere decir, cuando una TTP rompe dicha confianza puesta por el usuario en la TTP.

No verificable: el usuario no puede demostrar que existe incumplimiento por parte de la TTP, cuando brinde su servicio.

- **Intervención en el protocolo**

  Optimista: Una TTP está involucrada en el protocolo en casos solamente excepcionales.
  Arbitrado: Los usuarios finales deben tener contacto con la TTP siempre.

- **Confidencialidad**

  Operacional: Una TTP no puede obtener datos confidenciales.
  Incondicional: Una TTP puede obtener datos confidenciales.

- **Usuario del servicio**

  Soporte: La comunicación entre TTPs con los usuarios se llevan a cabo fuera de línea, siendo interacciones separadas.
  Final: Una TTP da cobertura al servicio de manera directa

- **Organización de la TTP**

  Colegiado: Un grupo de TTPs está involucrado siempre en el protocolo.
  No colegiado: Una TTP toma las decisiones que se encuentran relacionadas al servicio.

- **Equidad**

  Transparente: La TTP no puede realizar procesos erróneos con un usuario, ya que el usuario se dará cuenta.

CAPÍTULO 3

PKI

Es la infraestructura de hardware y software, que se apoya con políticas y procedimientos necesarios para crear, gestionar, distribuir, utilizar, almacenar y revocar certificados digitales; con la finalidad de establecer acceso fiable y consistente cumpliendo con los principios de Seguridad Informática.

Conocido como criptografía de clave pública; determinada así por su Algoritmo Criptográfico basado básicamente en Cifrar y descifrar mensajes utilizando dos claves o también denominadas claves diferentes: clave pública, clave privada; las claves están relacionadas con un algoritmo matemático, con el fin de establecer un acuerdo entre las claves públicas con las respectivas identidades de usuario por medio de una autoridad de certificación AC.

Los conceptos de clave pública y privada y el de firma digital, son básicos dentro de Smart Grid; la implementación de una PKI en un entorno de Grid Computing requiere una AC, una AR (Registration Authority) y un Sistema de Distribución de Certificados, dependiendo del marco legal existente.

PKI, al ser una infraestructura que establece comunicación entre varias entidades la necesidad de seguridad que esta requiere deberá cumplir con los principios básicos de seguridad, además de establecer normas acordadas, establecer métodos para descubrir y validar las rutas de certificación, protocolos operativos, protocolos de gestión y Legislación de soporte o apoyo.

La seguridad en el uso de la infraestructura PKI depende en cierta medida de cómo se guarden las claves privadas. Existen dispositivos especiales denominados tokens de seguridad diseñados para mantener la integridad y seguridad de la clave privada, así como evitar que ésta pueda ser exportada.

La clave privada es utilizada en el proceso de generación de la firma y la clave pública (Certificado Digital) es utilizada en el proceso de verificación de dicha firma. Un intruso, que no tenga conocimiento de la clave privada del Firmante, no

puede generar la Firma correcta de dicho firmante, las Firmas no pueden ser falsificadas. Sin embargo, utilizando la clave pública del Firmante, cualquier persona puede verificar un mensaje debidamente firmado. El destinatario requiere contar con la certeza que la clave pública representa al propietario del par de claves estableciendo la existencia de un vínculo confiable entre la identidad del usuario y la clave pública. Este vínculo de confianza mutua se logra por parte de una tercera persona con la formulación de un certificado de clave pública autorizada para tales efectos por una Autoridad Certificadora que cumpla con las normas ANSI X9.57-1997 de Administración de Certificados.

3.1 PKIx

El sector de normalización de las telecomunicaciones o sus siglas en ingles ITU-T, para validar las rutas de certificación de una PKI desarrolla el estándar X.509, para luego el Grupo de Trabajo en Ingeniería de Internet (IETF) se base en este, para el desarrollo de normas independientes diseñadas para atender los requerimientos de PKI basada en X.509 en la Internet.

Generando así; formatos estándar para certificados de claves públicas y definiendo una estructurada fuente de parámetros o normas a seguir cuyo principal objetivo es proporcionar la administración de certificados de protocolos orientados a Internet. Las especificaciones PKIx definen el comportamiento que se espera de la PKI.

3.1.1 X.509

Define un algoritmo de validación de la ruta de certificación para una infraestructura de clave pública PKI.

Es expedido por una Autoridad de Certificación (AC), Autoriza al portador del proxy a actuar en nombre del usuario que lo ha firmado, Con el fin de autenticarse para utilizar los recursos Grid.

El formato de certificados X.509 se especifica en un sistema de notación denominado sintaxis abstracta uno (Abstract Sintax One o ASN-1). Para la transmisión de los datos se aplica el DER (Distinguished Encoding Rules) que son las reglas de

codificación distinguible, que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales.

Los certificados X.509 han estado presentes desde hace varios años en la cotidianidad de los usuarios de internet como una forma de autenticación de usuarios, además es una forma electrónica de identificación. Su aparición surge de elevar y sofisticar el grado de seguridad que se utiliza en la autenticación simple, debido a que existen diversas razones que demuestran que la autenticación simple no es un método lo suficientemente robusto para proteger adecuadamente un recurso o servicio, como por ejemplo el Robo de contraseñas, que puede derivarse de conductas inseguras que los usuarios pueden adoptar con respecto al manejo de contraseñas, hacen que existan diversidad de métodos o ataques específicos para obtener datos de autenticación.

Figura 2. Autenticación Simple Usuario/Contraseña

Para robustecer los métodos de Autenticación Simple, la Unión internacional de Telecomunicaciones UIT por sus siglas en el idioma inglés propone un método; es el crear un certificado electrónico que será capaz de permitir la autenticación mutua y además que esta se encuentre cifrada, a la cual la denominarían Certificado X.509.

Se basa en claves cifradas para la comunicación, e internamente está estructurada por un conjunto de campos que contienen información acerca del titular del certificado. Están diseñados para que un tercero pueda dar fe del usuario en cuestión, esta tercera parte se llama una Autoridad de Certificación este modelo de seguridad es denominado Infraestructura de Clave Pública PKI pos sus siglas en el idioma inglés,

con el fin de solicitar un certificado, un numero de detalles se envían a un determinado AC para asegurarse de que es usted el usuario que se supone que sea.

Para confirmar la identidad de un usuario en cuestión depende de las políticas de seguridad presente en la AC. El usuario hace el papel de emisor luego con un certificado que contiene los detalles envían la petición, firmada digitalmente por esa AC. El AC también proporciona un conjunto de claves pública y privada para su uso en el proceso de autenticación mutua.

Los certificados X.509 fueron diseñados para ser modificables, ampliables, utilizables bajo variadas circunstancias y niveles de seguridad.

3.1.2 Componentes

La estructura PKI puede ayudar a dividir en dos grupos Básicos de los componentes de toda la infraestructura, como muestra la figura:

Figura 3. PKI X.509 Componentes básicos

A continuación se detalla las principales tareas de cada componente:

- AC Autoridad de Certificación.- Generación de Claves y Certificados Digitales; Emisión y distribución de certificados, Revocación, Certificación cruzada, Respaldo de claves y Sistema de Recuperación.
- AR Autoridad de Registro.- Registro cara a cara, registro remoto, registro automático, revocación.

- Sistema de distribución de certificados.- Proporciona repositorio para Certificados Digitales y Listas de revocación de certificados; Base de Datos para propósitos especiales, directorios LDAP.

- PKI aplicaciones habilitadas.- requiere de cierta funcionalidad como funcionalidad criptográfica, Almacenamiento seguro de información personal, Certificado digital de acceso a directorios, Instalaciones Comunicación.

3.1.3 Funciones de Administración de PKIx

PKIx identifica una serie de funciones de gestión, que potencialmente necesita ser apoyada por protocolos de gestión y la relación entre los diversos componentes del PKI, resume los tipos de funciones de gestión que podría ocurrir entre estos componentes.

Las funciones que se identifican son:

- **Registro.-** Para aprovechar de las aplicaciones habilitadas en la estructura PKI, es necesario que las entidades finales deban inscribirse, a esta función se la denomina Registro, es el primer paso en el proceso de inscripción de la entidad final.

  El primer paso del registro es la verificación inicial de la identidad, es el proceso mediante una entidad final se hace conocida ante una AC. El nivel de seguridad asociada con el proceso de registro tenderá a variar basado en el entorno de destino, uso previsto del certificado, y las políticas asociadas.
  El proceso de registro podría lograrse directamente con la Autoridad Certificadora o a través de una Autoridad De Registro intermedio, este proceso también puede llevarse a cabo en línea o fuera de línea o una combinación de los dos.

- **Inicialización.-** Este paso se asocia generalmente con la inicialización de la Entidad final con su par de claves asociadas. Para la generación de claves incluye la creación de la división, público / privado par de claves aso-

ciado con una entidad final. Para la generación de claves puede ocurrir antes del proceso de inscripción de entidad final o puede llevarse a cabo en respuesta a la misma. Las parejas de claves puede ser generada por el sistema cliente entidad final, AR, AC o algún otro componente tal como un módulo de seguridad de hardware. La ubicación de la generación del par de claves está dictada por las limitaciones operativas y políticas aplicables.

Es posible que determinadas partes de este paso puedan ocurrir en momentos diferentes. En Internet, por ejemplo, los navegadores se inicializan con las claves públicas de numerosas entidades de certificación raíz que podría ser utilizado como anclas de confianza. Sin embargo, la parte del usuario final de la inicialización no ocurriría hasta que se realice una solicitud de certificado explícito.

- **Certificación.-** Es la conclusión para el proceso de inscripción de una entidad final; este paso implica la emisión del certificado de clave pública de entidad final por la AC. Si el par de claves es generado externamente a la AC, la clave pública debe ser transportado a la AC de una manera que se garantice la integridad de los datos.

  Una vez generado, el certificado se devuelve a la entidad final para que proceda a publicarlo en un repositorio de certificados.
  Existe la posibilidad que la inicialización y la certificación trabajen como un solo proceso, es necesario rescatar que dos o más de éstas funciones descritas anteriormente se pueden combinar en una sola.

- **Recuperación de claves.-** Permite a las entidades Finales restaurar sus claves de cifrado /descifrado, con la instalación de una copia de seguridad emitido por una clave autorizada por lo general, la AC que expedido un certificado.

También es posible que la asociación de una entidad final con una organización pueda cambiar por ejemplo, en el caso de renuncia del empleado, despido, o lesiones personales, y la organización tiene una necesidad legítima para recuperar datos que han sido cifrados por la entidad final.

- **Actualización de clave.-** Los certificados son emitidos con período de validez por lo tanto es evidente que el certificado finalmente vencerá. La actualización de las claves es necesaria como consecuencia de la revocación de certificados esto implica la generación de un nuevo par de claves, y la emisión de una nueva clave pública.

  La actualización de claves puede ocurrir antes de la expiración de un par de claves determinado. Esto ayudará a garantizar que la entidad final siempre tendrá en posesión un par de claves legítimas.

  El uso de esta función no es recomendada en estructuras web debido a que es posible establecer diferentes períodos de validez para las claves públicas y privadas que se utilizan para firmar digitalmente y verificar. Este obligaría a una actualización de las claves antes que la clave pública asociada expire en realidad. Ella También ofrece una ventana de tiempo en el que el certificado de clave pública no puede ser vencida utilizado para verificar las firmas digitales que se crearon con la clave privada ahora expirada. Esto ayudará a minimizar los mensajes de advertencia irrelevantes que de otro modo serían mostrados a la entidad final.

- **Solicitud de revocación.-** Los certificados de clave pública se emiten con tiempos de vida bastante extensos. Sin embargo, las circunstancias que existían cuando se emitió el certificado pueden cambiar antes de que el certificado expire naturalmente o por diferentes razones.

  Por lo tanto, en ocasiones es necesario revocar un certificado antes de su fecha de caducidad. Aparece un nuevo término como lo es el CRL, por

sus siglas en el idioma ingles de Certificate Revocation List, la traducción a nuestro idioma es Lista de Certificados Revocados.

La información de revocación de certificados debe estar a disposición de la autoridad competente que emitió dicho certificado o por el CRL Emisor a que los delegados AC esta función. X.509 define un método para la publicación de esta información a través de las listas de revocación de certificados (CRL). La frecuencia de publicación y el tipo de CRLs utilizados son una función de la política local.

El grupo de trabajo PKIx también ha introducido varios protocolos que están diseñados para proporcionar información de estado de certificados en línea. Y recomiendan tener en cuenta que las entidades finales, o de terceros de confianza que operan en su nombre, debe comprobar el estado de revocación de todos los certificados en una ruta de certificación dada.

- **Certificación cruzada.-** Se produce entre las entidades emisoras. Un certificado cruzado es un certificado de clave pública que se emite por una AC a otra AC. Un certificado cruzado es un certificado de clave pública que contiene la clave pública de una AC que ha sido firmado digitalmente por otra AC.

  La certificación cruzada puede ser bidireccional o unidireccional. Bidireccional a la certificación cruzada se produce normalmente entre las entidades emisoras. Certificación cruzada unidireccional se produce típicamente en un modelo de confianza jerárquico donde la emisión esta remitida por un ente superior en este caso un AC.

3.1.4 Estructura

Cada aplicación de X.509 podría incluir diferentes campos o asignar diferentes significados para ellos. Para referencia algunos de los campos X.509 estándar se visualiza a continuación.

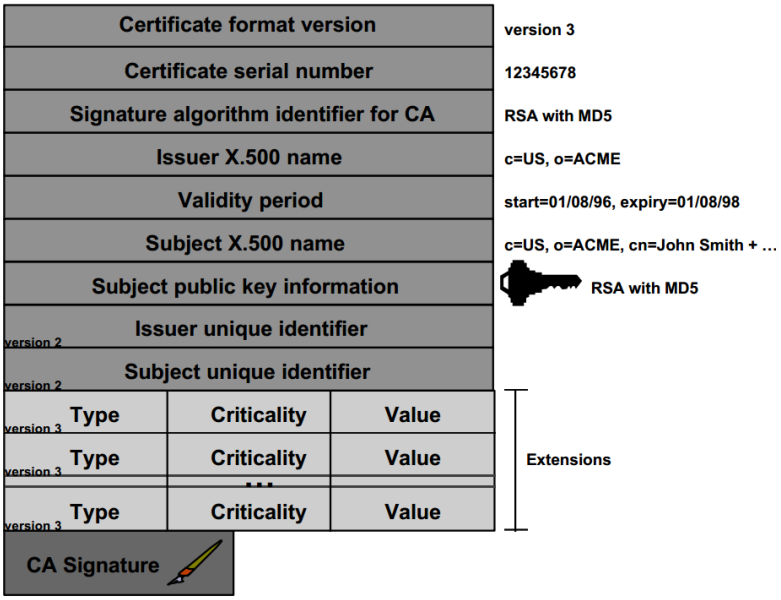


Figura 4. Estructura de un certificado X.509

X.509 se encuentra actualmente en V3. Y su estructura está conformada por:

- Número De Serie.- Los números de serie se utilizan para hacer el certificado De revocación más manejable.
- Algoritmo de firma Identificador.- Esto es importante ya que no todos los utilizan los mismos algoritmos de firma.
- Nombre emisor.- Identifica la AC de que se trate.
- Período de validez.- Para ayudar en la seguridad de los certificados que permanezca valida por un periodo determinado.
- Nombre del sujeto.- Este consta de los siguientes subcampos en la estructura Globus.
    - Nombre
    - Unidad Organizacional
    - Organización.

- Nombre de dominio completo (necesario para algunos tipos de certificado)

Además los certificados X.509 están diseñados de manera tal que pueden trabajar con los siguientes estándares y protocolos:

- TLS/SSL
- S/MIME (Secure Multipurpose Internet Mail Extensions)
- IPsec
- SSH
- Single sign-on
- HTTPS
- LDAP
- Timestamping

3.2 Autoridades de Certificación

Como se mencionó antes el termino AC, viene derivado de las siglas en el idioma ingles de "Certification Authority", Autoridad de Certificación; Es un componente fundamental dentro de la estructura PKI y necesaria dentro de un ambiente Smart Grid.

Basado en criptografía de clave pública es un ente que debe cumplir estrictamente con las normativas vigentes de cada país para obtener un título habilitante que la acrediten, dentro de la cual se establecen requisitos legales y técnicos nuestro país ha tomado como referencia la Ley Modelo de CNUDMI-UNCITRAL. Dentro de las obligaciones que la ley refiere establece que la AC deberá ser una entidad de confianza cuyo objetivo es garantizar la identidad de los titulares de certificados y su correcta asociación a las claves de firma electrónica, es responsable de emitir y revocar los certificados digitales o certificados utilizados en la firma electrónica.

3.2.1 Autoridades de Certificación Nacionales

La Ley de Comercio Electrónico de Ecuador , ha puesto especial énfasis, para que dichas Entidades además de cumplir con todos los requisitos legales y técnicos que exige la normativa vigente, cumpla con ciertos requisitos que demuestren solvencia técnica, logística y financiera.

Respecto a la capacidad económica y financiera suficiente para prestar los servicios autorizados como Autoridad de Certificación, se entendería como la liquidez o solvencia que debe tener la persona jurídica, para que en un futuro, si llegare a presentarse una eventual responsabilidad civil, contractual o extracontractual se cubra con su patrimonio.

Otro requisito muy importante, es contar con la capacidad técnica necesaria para la emisión de certificados sobre la autenticación de las firmas electrónicas.

Sobre este punto, la AC utilizará tecnología de punta y lo más importante debe tener altos índices de seguridad, pero para que aquello se cumpla, toda Entidad de Certificación debe basarse y acatar la Declaración de Prácticas de Certificación.

Es importante manifestar, que las Entidades de Certificación, son aquellas que dan fe, que una determinada clave pública corresponde a un sujeto específico, mediante la expedición de un certificado.

Dentro de la legislación ecuatoriana, al referirse a las Entidades de Certificación, se ha tomado como referencia la Ley Modelo de la CNUDMI/UNCITRAL, dentro de la cual, establece obligaciones que se debe cumplir, dentro de las cuales se encuentran las siguientes:

“Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) Actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) Actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;

c) Proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

1. La identidad del prestador de servicios de certificación;
2. Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;
3. Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella"

Dentro de las principales obligaciones que debe cumplir una AC se encuentran las siguientes:

- Garantizar al usuario la prestación permanente, inmediata, oportuna, ágil y segura del servicio de certificación.
- Tener un respaldo de información relativo a los certificados, incluyendo un sitio seguro. Debe proteger las claves privadas contra el peligro de usurpación.
- Mantener una publicación del estado de los certificados emitidos y una página web actualizada, para que los usuarios lo puedan utilizar.
- Emitir certificados de acuerdo a las Políticas de Certificación que le sean aplicables.
- Conservar registrada toda la información y documentación relativa a un certificado emitido por la (AC) por un plazo no inferior a 4 años contando desde la fecha de caducidad del mismo.
- La información sobre los programas o equipos requeridos para acceder a registros o mensajes de datos deberá ser proporcionada a los usuarios de dichos registros o mensajes de datos, mediante medios electrónicos o físicos.

En tal virtud, una vez que obtenga el título habilitante, la AC está autorizada para emitir certificados en relación a claves criptográficas, ofrecer y facilitar los servicios de registro y recepción de datos, entre otras. Dicha Entidad expedirá certificados, producto del resultado de verificación que efectúa sobre la autenticidad, veracidad y legitimación de las claves criptográficas y la integridad de un mensaje de datos.

La institución encargada de acreditar un AC en Ecuador es el CONATEL Consejo Nacional de Telecomunicaciones hoy por hoy miembro de la Secretaria Nacional de Telecomunicaciones, la misma que avala como autoridades acreditadas a :

- Autoridad de Certificación Pública
    - Banco Central Del Ecuador.- es la Entidad de Certificación de Información y servicios relacionados o la contracción por sus siglas ECIBCE, acreditada en el 2008 por el Consejo Nacional de Telecomunicaciones.

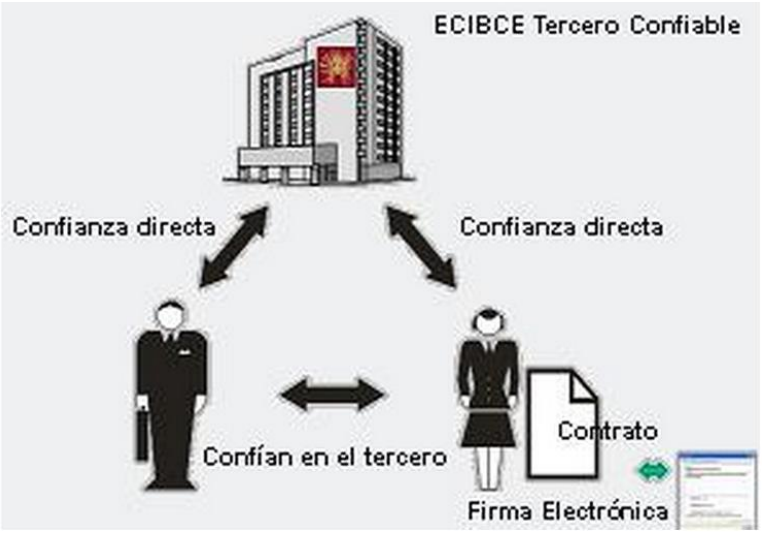


Figura 5. Diagrama ECIBCE

Entre sus principales funciones, emite certificados digitales de firma electrónica y otros servicios relacionados con la certificación electrónica para el Sector Público, Personas Jurídicas y Personas Naturales; garantizando la seguridad jurídica y tecnológica en entornos electrónicos cumpliendo

el marco legal, las normas y estándares nacionales e internacionales de certificación electrónica.

- Autoridades de Certificación Privadas
    - Security Data.- parte del grupo Telconet, acreditada por el CONATEL para emitir Certificados de Firma Electrónica, permite interactuar con las aplicaciones de Gobierno como SRI, INCOP, INEN, sistema Ecuapass de la Aduana.
    - ANF Ecuador.- Entidad de Certificación de Información y Servicios Relacionados, filial de la española Distribución MCP 2000 SL, oficialmente acreditada para operar en Ecuador, ofrece servicios para las operaciones de e-Commerce que engloba la emisión de certificados de identidad y entrega de dispositivos de firma electrónica a empresas y profesionales.

Los costos por servicios de certificación electrónica en Ecuador se encuentran dentro de un rango de precio de entre $20 A $100 y tienen vigencia entre un año y tres años, y su respectiva renovación representa un costo adicional. Donde se puede percatar de un precio más elevado es en los aplicativos para firma y sellado o dispositivos que soportan a los servicios de certificación como los tokens de seguridad.

3.2.2 Autoridades de Certificación Internacionales

La certificación del ente que pretende ser una Autoridad de Certificación AC, se llama acreditación, por lo tanto a nivel mundial existen diversidad de encargados de autorizar la creación de una autoridad de certificación o prestador de servicios de certificación. Para lograr la acreditación existen diversos entes reguladores que se encargan de verificar que se cumplan con las normativas propias de cada país, La mayoría de países delegan a entidades gubernamentales para que brinden el servicio como Autoridades de Certificación Pública, en el caso de Ecuador está el Banco Central, en España está el Ministerio de Industria, Turismo y Comercio; en México la Secretaría de Economía, por citar algunos ejemplos.

Un ejemplo es, España donde existen dos Entidades que gestionan todo lo que se refiere a firma electrónica y son las Entidades de Certificación y Autoridades de Registro AR .A su vez las dos se incluyen en una clase más general de instituciones destinadas a generar confianza en todo el sistema de relaciones telemáticas conocidas como "Terceras partes de confianza" y abreviadamente por sus siglas inglesas TTP (Trusted Third Party) además estas incluyen las Autoridades de sellado de tiempo.

Una AC internacional, actúa como fedatarios de los certificados que firman, responsabilizándose de su generación, publicación, revocación y suspensión, de dichos certificados.

Los procedimientos de seguridad que todas las Autoridades de Certificación deben poseer para evitar falsificaciones de certificados. Deben contener la Declaración de Prácticas de Certificación (Certification Practice Statement o CPS), el mismo que indica sus políticas y prácticas relativas a la seguridad y mantenimiento de los certificados, responsabilidades de la AC y obligaciones de los suscriptores de certificados de firma.

Dentro de las Autoridades de Certificación reconocidas a nivel Internacional:

- Banesto AC
- Comodo CA Limited
- DigiCert Inc
- EADTrust
- EDICOM
- Equifax Secure Inc.
- Entrust.net
- GlobalSign nv-sa
- GoDaddy.com, Inc.
- Network Solutions L.L.C.

- Starfield Technologies, Inc.
- Thawte Consulting cc
- UTN-USERFirst-Hardware
- VeriSign, Inc.
- VeriSign Trust Network

Los costos por servicios de certificación electrónica se encuentran dentro del mismo rango que los establecidos por los de las Autoridades de certificación Nacionales, cabe mencionar que los precios vienen a ser parametrizados por las AC de nivel público pertenecientes al estado. Donde se puede notar de un precio más elevado es en los aplicativos para firma y sellado o dispositivos que soportan a los servicios de certificación como los tokens de seguridad.

3.3 GSI

Dentro del marco de seguridad, es el más usado para sistemas del tipo Smart Grid, el mismo que amerita un estricto nivel de seguridad. Sobre todo con el manejo de Claves públicas para establecer comunicaciones seguras, la autenticidad y confidencialidad entre los elementos que forman parte del Grid debe dar las debidas garantías, todo este conjunto de infraestructura de seguridad forma el denominado GSI abreviación de Grid Security Infraestructure.

Dentro de la estructura Globus Project se encuentra ubicado en la segunda capa dedicada a los servicios de seguridad.

Es la Infraestructura de seguridad que hace uso de certificados proxy como el X.509 para identificar a las entidades, utiliza SSLv3 para realizar el proceso de autenticación mutua; permite que los recursos puedan especificar sus propias políticas de autorización, permite la delegación de privilegios a otras entidades y además se integra con los sistemas locales de seguridad de cada organización.

3.3.1 Componentes

Los usuarios se identificarán en el Grid mediante las credenciales de autenticación del GSI, el mismo que ofrece los siguientes servicios de seguridad:

- Un sistema de criptografía de clave pública (Public Key System)
- Autenticación mutua mediante certificados x509
- Delegación de credenciales y "single sign-on".

GSI está compuesto de:

- Comandos para gestionar certificados.
- Clases Java para integrar y configurar la seguridad tanto en los Grid Services como en sus clientes.

Configuración de GSI básicamente se reduce a conseguir uno o varios certificados digitales. Para obtener un certificado se tiene que:

- Conseguir el certificado del AC al que se quiere solicitar un certificado.
- Generar una petición de certificado.
- Enviársela al AC.
- El AC devolverá el certificado firmado.
- Instalar el certificado

3.3.2 Herramienta Globus Toolkit

La infraestructura de red de seguridad (GSI) implementa certificados proxy para proporcionar capacidades de autenticación y de delegación de Globus Toolkit. La aplicación permite a los usuarios emplear certificados de proxy para autenticar a los servicios basados en GSI y delegar Certificados de proxy a esos servicios para que puedan actuar en nombre del usuario.

GSI está pensado principalmente para trabajar con sistemas de autorización basados en la identidad y, como tal, devuelve a la aplicación que llama una identidad para el cliente remoto. Asimismo, se pretende que ser utilizado principalmente con los certificados de proxy que tienen las políticas de delegación de la serie completa de su los derechos del emisor a su portador. En este caso se devuelve el nombre del sujeto de la X.509 certificado de clave pública que emitió el certificado original de proxy en la cadena.

GSI incluye una biblioteca GSS-API, que controla la autenticación y la delegación utilizando Certificados Proxy. Esta biblioteca se basa en gran medida en la biblioteca OpenSSL, un código abierto de implementación de protocolo SSL. OpenSSL proporciona compatibilidad, protección del mensaje y la validación de rutas X.509 básica. Se añade al OpenSSL código personalizado para el manejo de los certificados de proxy, además de público normal de X.509 certificados de clave y delegación de realizar.

El kit de herramientas Globus son un conjunto de herramientas orientadas al Grid de primera generación, diseñado para fomentar la investigación en la mejora de las Grid en general. Es un proyecto de código abierto que ha ganado un amplio apoyo en todo el mundo y se ha convertido en líder de desarrollo de Grid.

- **Single Sing On en Grid**

Inicio de sesión único también denominado por sus siglas en inglés como SSO, es una arquitectura de sistemas que permite al usuario acceder a diferentes aplicaciones con una sola validación de acceso.

Esta técnica se ha popularizado con el auge de las redes sociales, las aplicaciones web y la computación en la nube. Grandes compañías han querido simplificar la vida de sus usuarios permitiéndoles tener acceso a sus distintos productos con una misma cuenta, Un ejemplo conciso sería Google Apps, donde con una sola cuenta, se puede acceder a Gmail, Google Calendar, Google Maps, Google Play, YouTube, Google Docs.

Inicio de sesión único es característica importante para aplicaciones en GSI, Permite una fácil coordinación de los múltiples recursos, donde el usuario se autentica una vez, entonces puede llevar a cabo múltiples acciones sin Re autenticación.

Una ventaja más del SSO en GSI es el permitir que los procesos puedan actuar en su nombre. Para apoyar el inicio de sesión único en GSI añade la siguiente funcionalidad para SSL como es las Credenciales de proxy y la Delegación de Credenciales.

- **Certificados Digitales en Grid**

El acceso a los recursos del GRID se hace a través de un certificado digital que ha de solicitarse a la Autoridad Certificadora, gracias a este certificado los usuarios pueden enrolarse en alguna Organización Virtual y comenzar a utilizar el Grid.

Un certificado de clave pública es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada.

Los certificados de clave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado. La entidad identificada se denomina sujeto del certificado o subscriptor (si es una entidad legal como, por ejemplo, una persona).

Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca.

Figura 6. Diagrama acceso al Grid.

El correo electrónico es muy vulnerable a los hackers. Los mensajes pueden ser leídos o modificados sin que el emisor ni el receptor detecten las alteraciones. Una infraestructura de correo electrónico que no utilice internet, dedicada especialmente para el intercambio de mensajes confidenciales no es viable económicamente ni fácil de utilizar. Una solución más eficiente y rentable es la utilización de Certificados Digitales que funcionen como un pasaporte electrónico asegurando así la integridad de los mensajes remitidos como recibidos, a este nivel de seguridad se lo conoce como Correo Seguro.

- Correo seguro.- existen varios componentes que de Certificación Digital para establecer un nivel de seguridad confiable, se puede agregar la firma digital y la encriptación de los datos, Los certificados digitales permiten el cifrado de documentos y mensajes, además de los anexos, de forma que sólo pueden ser leídos sólo por los destinatarios autorizados.

- Firma Digital.- las cuales también se sostienen en el cifrado de clave pública proporcionan un medio más seguro de probar la identidad de uno cuando se envía un mensaje. Permite que el destinatario compruebe que el mensaje no fue modificado en el camino y que lo que lee es exactamente lo que redacto.

3.3.3 Ventajas

Existe el manual de usuario para Globus Toolkit publicado por IBM, el cual será nuestra pauta para seguir paso a paso con la actividad post- instalación de globus toolkit, que será la configuración de GSI, y consta básicamente en usar los comandos adecuados para el setup de GSI.

Establecer comunicación segura entre elementos del Grid para ofrecer seguridad a través de diversos dominios administrativos. No debe haber un sistema de seguridad centralizado.

CAPÍTULO 4

AUTORIDAD CERTIFICADORA NO ACREDITADA EN AMBIENTE SMART GRID

Un Smart Grid es un sistema de red evolucionado que gestiona la demanda de una manera sostenible, y fiable para facilitar la integración de todos los involucrados, constituye nuevas soluciones tecnológicas orientadas a la optimización.

Obedece a un modelo computacional destinado a integrar recursos distribuidos en la forma de un recurso único, la tecnología Grid pretende aunar recursos separados o no geográficamente, incluso pertenecientes a diferentes organizaciones o dominios administrativos. Por lo cual, surge la necesidad de implementar una infraestructura de seguridad que permita a aquellos participantes del Grid controlar el uso de sus recursos (donados al Grid) y, además, que dé al usuario confianza, acerca de la autenticidad de los recursos a los cuales puede acceder a través del Grid.

El capítulo medular de este proyecto es establecer un AC no acreditado donde se simulará un Smart Grid con la herramienta software Globus Toolkit y se procederá a configurar la estructura de una Autoridad Certificadora que permitirá identificar de manera segura a los miembros de la infraestructura, garantizando la validez de los certificados que están implícitos en las operaciones y cubrirán la necesidad de establecer una infraestructura de seguridad basada en el modelo PKI.

Para la implantación de políticas y procedimientos de seguridad de Globus Toolkit, además para la creación del modelo PKI este proyecto se soporta en el modelo previamente establecido, Para llevar un proceso alineado y optimo en la creación y puesta en marcha de una Autoridad Certificadora No Acreditada en ambiente SMART GRID.

4.1 Preparación del ambiente de trabajo

Para la configuración tanto en software como hardware, para simular el Grid y para configurar la infraestructura PKI a ser utilizada, se cuenta con la siguiente infraestructura tecnológica:

- Hadware

  Computador ASUS Slim Core i7 8gb en memoria RAM (host)

- Software

  Sistema Operativo Windows 7 (host)

  VirtualBox 4.3.2

  Sistema Operativo Ubuntu 12.04

  Globus Toolkit 5.2.5

Se cuenta con la ventaja y el aprovechamiento del software de virtualización VirtualBox, para las respectivas instalaciones de los servidores; que simularan el Grid donde se implantará la PKI, para la gestión de Certificados.

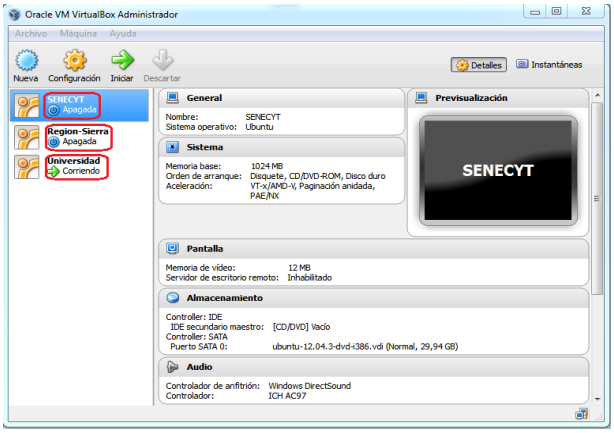


Figura 7. Infraestructura Virtualizada del Grid

La puesta en marcha de este proyecto viene establecida por la utilización de máquinas virtuales previamente instaladas con el sistema Operativo de distribución

Unix Ubuntu 12.04, el proyecto inicialmente cuenta con tres máquinas virtuales a las cuales se las denomina.

SENECYT, en esta máquina se procederá a instalar la AC Puente, en orden respectivo se cuenta con la máquina virtual denominada Región-Sierra, la tercera maquina con nombre Universidad, cada uno de los comandos ejecutados para las configuraciones necesarias se ha dividido en grupos las siguientes nomenclaturas:

Comandos de usuario común:

- adminuser@SENECYT-AC:~$
- adminuser@Region-Sierra:~$
- adminuser@Universidad-Sierra:~$

Comandos de usuario root:

- root@SENECYT-AC:~#
- root@Region-Sierra:~#
- root@Universidad-Sierra:~#

Las tres máquinas virtuales cuentan con la instalación previa de Globus Toolkit, su instalación funcionamiento de pertenencia a un GRID previamente detallado y demostrado; para verificar que Globus Toolkit se encuentra en las máquinas virtuales, se puede hacerlo buscando en el centro de programas de Ubuntu denominado Ubuntu Software Center, como se puede apreciar en la Figura 0.8, se observa la leyenda Installed, herramienta instalada.

Figura 8. Verificación Globus Toolkit

El procedimiento se repite para las máquinas virtuales Región-Sierra y Universidad; el resultado ha obtenerse será el mismo.

Para asegurar el funcionamiento de la herramienta se puede ejecutar un comando que indique el status de un servicio exclusivo de Globus Toolkit , haciendo uso del comando UNIX "service" este comando permite iniciar, detener, verificar servicios de herramientas, su funcionamiento es la abstracción de ejecutar toda la ruta completa hacía el directorio init.d; ejemplo: service globus-gridftp-server status

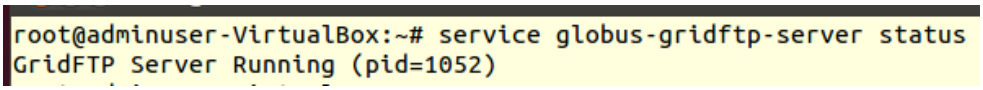


Figura 9. Verificación del servicio GridFTP

La Figura 0.9 identifica que un servicio exclusivo de la herramienta principal de simulación de Grid; otra forma de verificar que se cuenta con la herramienta previamente instalada es ejecutar un comando propio del Grid, en este caso puede digitar como usuario root, la sentencia grid-, para activar la opción de auto completado pulsa dos veces la tecla Tab, obteniendo como resultado:

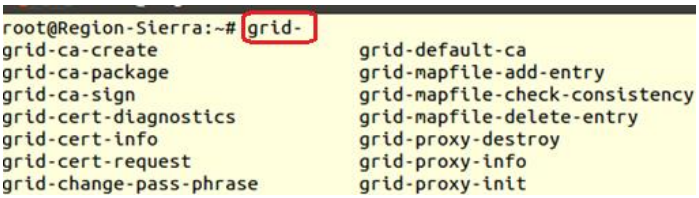


Figura 10. Opciones del Comando grid

La opción de autocompletación del terminal de Ubuntu, despliega las diferentes opciones de comandos propios del Grid, de los que se hará uso para futuras configuraciones.

4.2 Implementación del Modelo

Como antecedentes es necesario destacar que la herramienta que permite simular un ambiente Grid es el software de código abierto Globus Toolkit, esta herramienta incluye varios servicios de software y bibliotecas para el control de los recursos, la gestión de archivos, infraestructura de la información, gestión de datos, la comunicación, la detección de fallos, y la portabilidad. Formando un conjunto de componentes que se pueden utilizar de forma independiente o en conjunto para la creación de diferentes aplicaciones.

Es así como se va utilizar este conjunto de componentes para la consecución de este proyecto, donde se debe preparar todo el ambiente de trabajo que simulará el ambiente Smart Grid, para la configuración de un AC raíz que será la parte inicial de la estructura PKI.

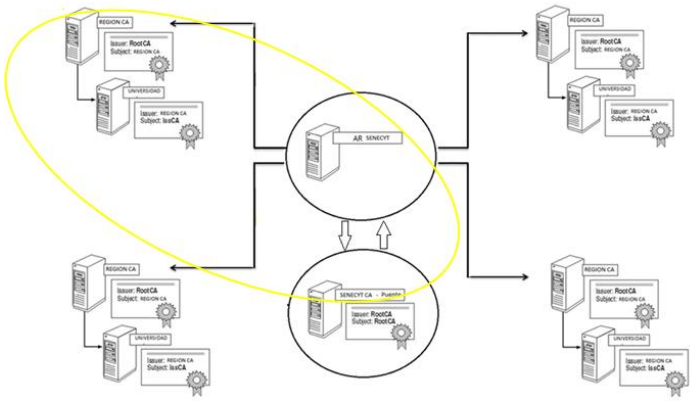


Figura 11. Modelo PKI.

La figura 11 establece el modelo al cual se rige el proyecto a implementarse, concentrándose a la parte encerrada en color amarrillo, donde se cuenta con la AC Puente, que hará de puente para el resto de la Infraestructura del modelo.

La estructura de un PKI se organiza en función de una Autoridad de Certificación raíz que se conecta con un nodo denominado AC-Región, entidad certificadora de la

región a la cual pertenece una AC-Universidad , basado en el seccionamiento por región geográfica establecido en las políticas a las cuales se está rigiendo este trabajo y será la responsable de:

- Identificar las entidades que solicitan certificados.
- Emitir, remover y archivar certificados.
- Proteger el servidor de la AC.
- Mantener un espacio de nombres único para los propietarios de certificados.
- Proporcionar certificados firmados de entidad final.

En este punto ese necesario destacar el trabajo de una Autoridad Registrante AR, será la responsable de aprobar o rechazar solicitudes de certificados de claves públicas, además validará la información enviada por el usuario con el fin de procesarla de manera segura hacia la Infraestructura, antes que la AC correspondiente pueda firmar cualquier certificado. Este proceso se ejecutará bajo un ambiente web, donde la gestión de solicitudes, la definición de una solicitud si es válida o no, debe cumplir los requisitos documentados en las políticas establecidas, es decir debe establecer si es un ente es válido para solicitar un certificado Grid.

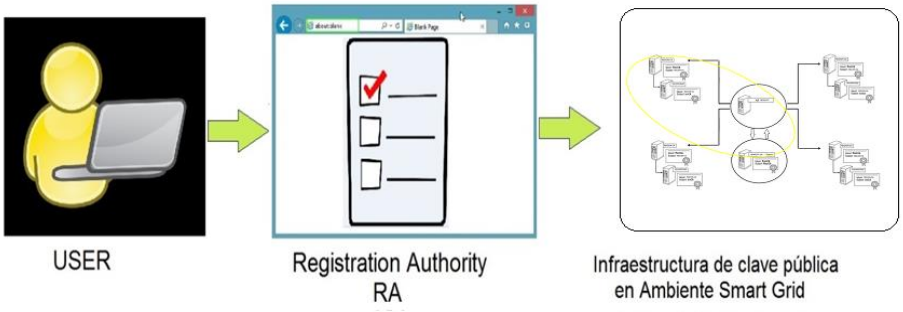


Figura 12. Proceso de Solicitud**.**

4.2.1 Nomenclatura del Modelo.

El modelo en puente permite conectar varias PKI entre sí, siendo esta apartada de su propia estructura por lo que la hace independiente, este proceso será permitido mientras es introducida una Autoridad Certificadora puente, la que permite que varias PKI establezcan relaciones de confianza.

El modelo establece que una Autoridad Certificadora puente no permite la emisión de certificados a los usuarios finales, solamente puede tener una relación con una AC por cada PKI, esta estructura tiene un crecimiento de notación lineal.

De manera genérica el modelo establece la nomenclatura, para cada AC, a este modelo se cambiará su nombre genérico quedando de la siguiente forma:

- AC Puente.- AC-SENECYT
- AC Raíz.- AC-Región-Sierra
- AC Subordinada.- AC-Universidad.

Para simular una infraestructura de llave pública PKI en ambiente Grid, y una vez que la AC Puente ha sido autofirmada, es necesaria la verificación y conexión con la AC que cumplirá con las veces de entidad certificadora de la región a la cual pertenece una Universidad basado en el seccionamiento por región geográfica establecido en las políticas a las cuales se está rigiendo este trabajo.

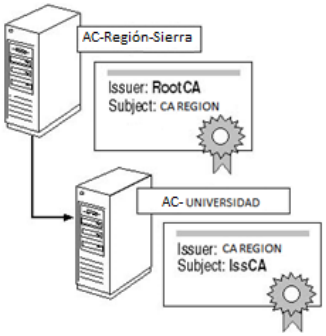


Figura 13. Ramificación de la estructura PKI**.**

El modelo establecido presenta varias ramificaciones para abarcar la totalidad de Universidades pertenecientes al SENECYT, la solución que se presenta en este trabajo obedece a demostrar la conexión de una rama como muestra la Figura 13**,** al obtener un certificado verificado por la AC-Universidad, que a su vez estable confianza con la AC-Región-Sierra, y esta fue verificada y firmada por AC -SENECYT. Se demostrará que el modelo esta funcional y es valedero; en el caso que se quiera abarcar con la totalidad de la estructura, simplemente se replicaría la configuración que se detalla en este capítulo.

4.2.2 Creación de la AC Puente.

Antes de que la AC central del modelo pueda firmar cualquier certificado, debe hacer lo propio con ella misma, de modo de que su identidad quede representada por su propio certificado.

Para hacer esto la AC realiza los siguientes pasos:

1. La AC genera aleatoriamente su propio par de claves.

2. La AC protege su clave privada.

3. La AC crea su propio certificado.

4. La AC firma el certificado con su clave privada.

Uno de los requisitos de Globus Toolkit es, que este software debe ser ejecutado bajo sistemas operativos de distribución Linux para un mejor funcionamiento de la herramienta; basándose en esto, en la Máquina Virtual denominada SENECYT que cumplirá con el rol de autoridad certificante Puente y para dar cumplimiento a los 4 pasos expuestos es necesario ejecutar instrucciones como adminuser ejecutando la instrucción sudo su.

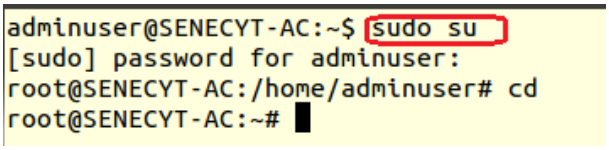


Figura 14. Cambiar el terminal de Ubuntu a root.

Luego se ingresa la clave establecida para el root user, una vez ejecutada esta sentencia se procede con la ejecución del script provisto por Globus Toolkit /usr/bin/grid-ca-create, se procede con la instalación y creación de la autoridad certificante en la máquina Virtual, obteniendo como resultado.

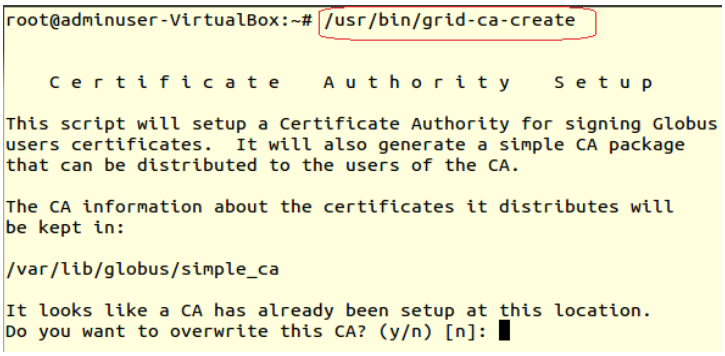


Figura 15. Instrucción para la creación de una AC en Grid.

Como parte de la creación de la AC se solicitará los componentes de la AC como son:

- cn.- Representa "nombre común". Identifica este certificado especial por lo que el certificado de AC dentro del dominio en este caso es AC-SENECYT.
- ou.- Representa "unidad organizativa". Identifica la AC de otras entidades emisoras creadas por SENECYT. El segundo "ou" específica para su nombre de host en estos casos se determinó como Universidades.
- o.- "organización", Identifica el Grid para este caso se establece como Senecyt.

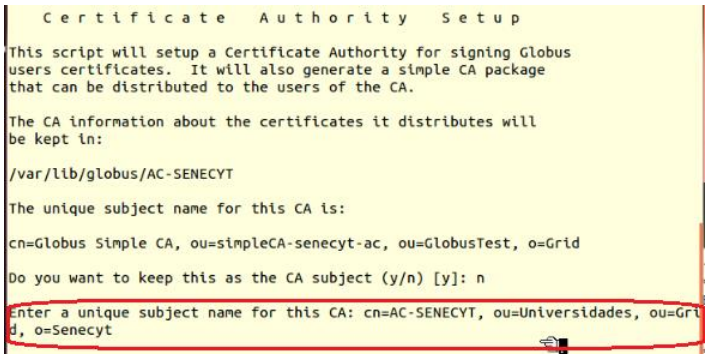


Figura 16. Especificación de los componentes de la AC.

Como siguiente paso dentro de la creación del AC se despliega la opción para ingresa la caducidad del Certificado estableciéndolo como 5 años, se debe ingresar en días.

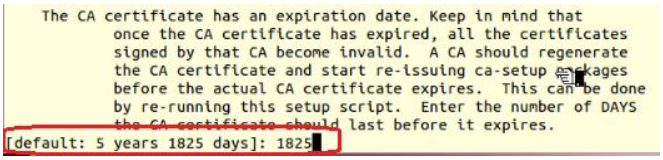


Figura 17. Caducidad del certificado para AC Puente.

Para proteger la AC-SENECYT es necesario ingresar una la clave privada Globus la denomina pass phrase, se la establece como PEM pass phrase =espe123

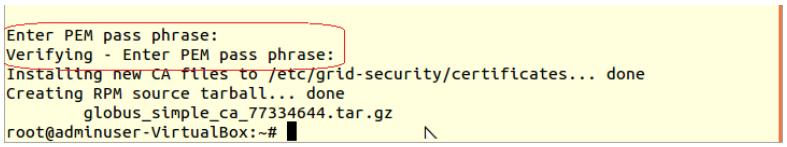


Figura 18. Clave para el certificado de la AC Puente.

Obteniendo como resultado el Certificado de la AC, además lo etiqueta haciendo uso de una función hash, generando una cadena de longitud fija, que será como distinguirá la AC para el resto de componentes del Grid. Además genera el certificado propio de la AC-SENECYT en formato .pem, formato de archivo empleado para almacenar certificados digitales en el directorio: /var/lib/globus/ AC-SENECYT/.

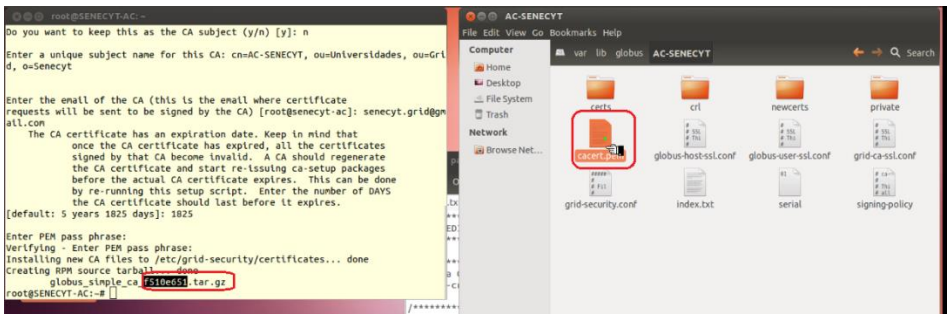


Figura 19. Certificado AC.

En la carpeta específica se observa, como se creó los archivos y carpetas necesarios para que pueda funcionar una Autoridad Certificadora.

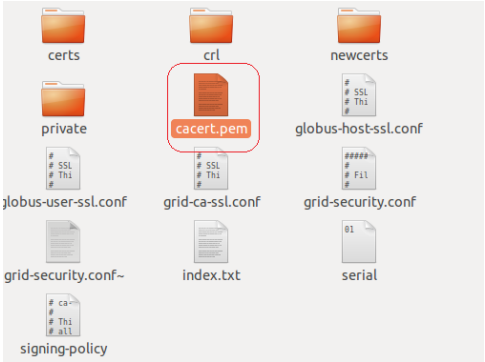


Figura 20. Archivos generados para la AC Puente.

Dentro de la carpeta que contiene los archivos principales que son el certificado de la AC, y su respectiva clave privada, esta se encuentra dentro de la subcarpeta private.

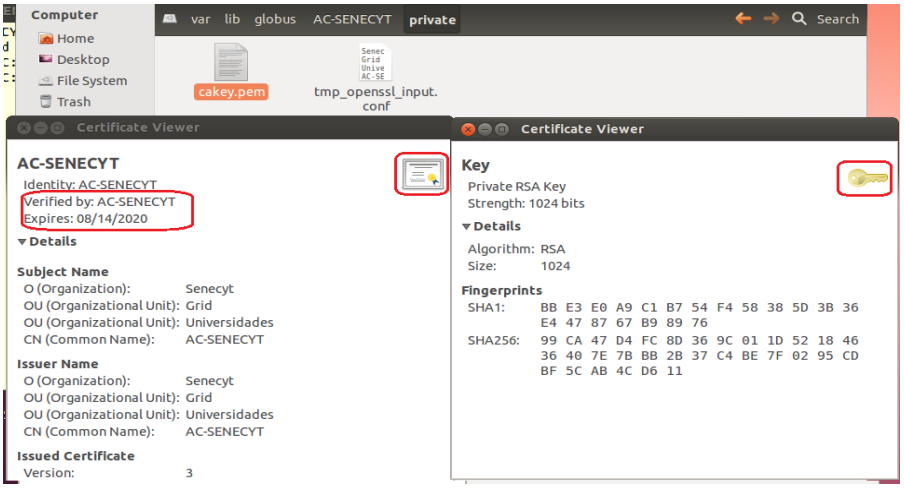


Figura 21. Certificado de la AC y su Clave privada.

Obsérvese en la Figura 21 que el certificado propio de AC Puente ha sido auto firmado por la propia AC, en la sección Verified by AC-SENECYT. Cumpliendo así con la premisa anteriormente descrita, antes que la AC Puente pueda firmar cualquier certificado, debe hacer lo propio con ella misma, de modo de que su identidad quede representada por su propio certificado.

Para verificar que el certificado fue creado con todos sus parámetros correctos se procede a visualizar el certificado en el navegador Mozilla Firefox, para agregarlo

como un certificado de Autoridad, donde después de agregarlo se puede hacer doble clic sobre el certificado, luego dirigirse a la parte superior en pestaña Herencia, validando así que se cuenta con nuestra AC en la raíz de la cadena de confianza que se establecerá.

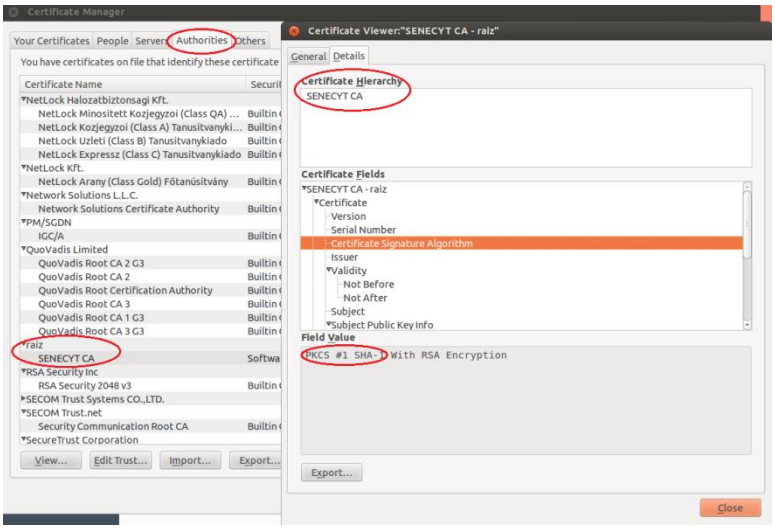


Figura 22. Certificado verificado en el navegador Mozilla Firefox.

4.2.3 Distribución de los archivos para establecer confianza hacia una AC.

Como se puede apreciar en la figura 19, se dispone de los archivos necesarios para ser distribuidos al resto de miembros del Grid que se desea establecer confianza con la Autoridad raíz, AC-SENECYT, y deberán ser guardados en el directorio específico de confianza.

La herramienta Globus confiará en los certificados emitidos por una AC siempre y cuando se puede encontrar información acerca de la AC en el directorio de certificados de confianza. El directorio de certificados de confianza está situado en /etc/grid-security/certificates Los siguientes dos archivos deben existir en el directorio para cada AC de confianza.

- cert_hash.0 .- código hash con el cual se etiqueta a una AC al momento de ser creada.
- cert_hash.signing_policy.- archivo de configuración que define los nombres completos de los certificados firmados por la CA.

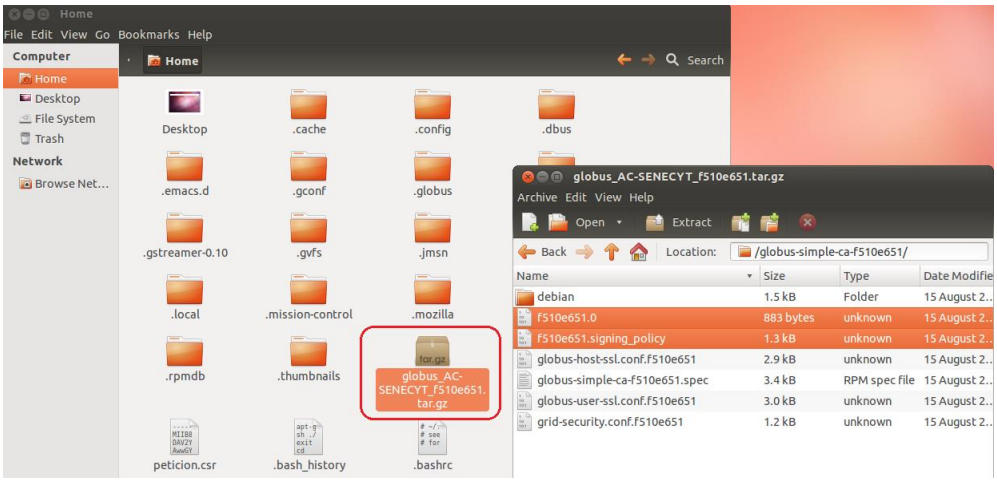


Figura 23. Archivos generados por la AC a ser distribuidos.

Luego de la creación de una AC, se genera automáticamente el paquete .tar que contiene los archivos estrictamente necesarios para establecer que un tercero perteneciente al grid, confié en nuestra AC. Como se puede observar en la figura 23 al abrir el paquete consta con los archivos anteriormente descritos.

4.2.4 Pasos para crear una AC No Auto firmada en Globus Toolkit.

Una de las partes fundamentales del proyecto de investigación es poner en marcha el modelo anteriormente descrito, para ello se debe establecer confianza entre la AC Puente con la AC Raíz que será la conexión de un brazo del modelo, para que se pueda firmar se establece los siguientes pasos:

1. Ubicarse en la carpeta de la nueva AC.
2. Ejecutar openssl req -new -key ./private/cakey.pem -out subcareq.pem -config grid-ca-ssl.conf
3. Firmar openssl ca -in ../AC-Universidad/subcareq.pem -extensions v3_ca -config grid-ca-ssl.conf

4.2.5 Creación de la AC Regional.

Al igual que con la creación de la AC-SENECYT, el proceso de creación se repite con la diferencia que se debe separar el certificado de solicitud (request), antes que se auto firme; y lograr firmarlo con la AC-SENECYT, siendo esto un reto, debido a que Globus Toolkit, al momento de ejecutar la sentencia grid-ca-create firma el request en cuanto se termina de ingresar los parámetros solicitados.

En este punto, es necesario destacar que se debe contar yá, con el archivo que distribuye la AC-SENECYT, donde sus respectivos archivos se encuentran en el directorio de AC de confianza, para verificar que no existe inconveniente con estos archivos, se ejecuta la sentencia grid-default-ca, despliega el listado de las autoridades certificadoras disponibles.

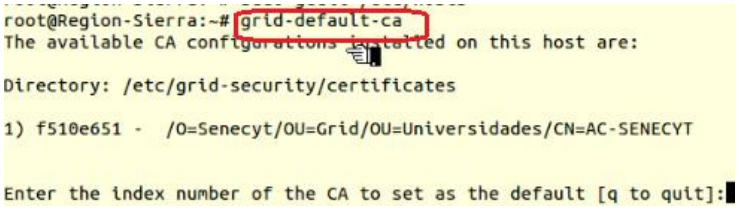


Figura 24. Autoridades Certificadoras Disponibles.

Para definir totalmente la confianza en esta Autoridad se escoge el digito indicativo que despliega en la lista en este caso se selecciona el número 1,

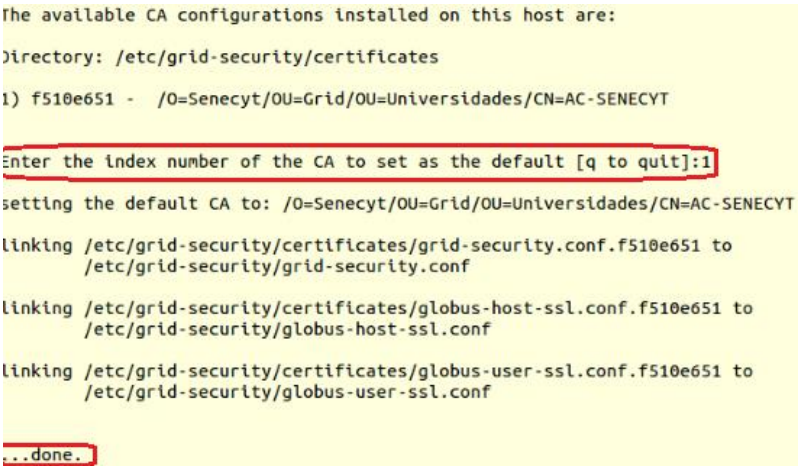


Figura 25. Establecer autoridad Certificadora por defecto.

Como resultado se cuenta con la Autoridad que firmará el certificado de la AC a ser creada.

Se ejecuta la sentencia propia de globus grid-ca-create, como parámetro adicional se ingresa la ruta donde se encuentran las AC para globus, en esta sentencia se especifica el nombre de la carpeta que contendrá los archivos de la nueva AC.

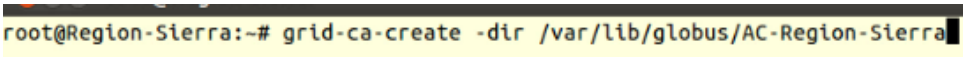


Figura 26. Comando Globus para la creación de una AC

Como siguiente paso, solicita los parámetros de la nueva AC, definida con el nombre de AC-Región-Sierra, con validez de la autoridad para 1825 días, 5 años a partir de la creación.

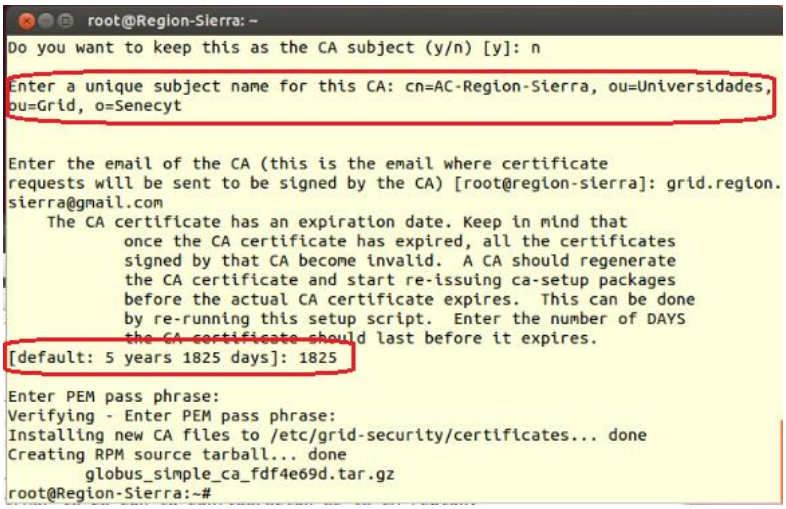


Figura 27. Parámetros AC-Región-Sierra.

Para este punto la nueva AC ya ha sido creada con su certificado firmado por sí misma, es entonces donde se procede con los siguientes comandos para que evite ser auto firmada.

4.2.6 Creación de la AC Entidad Final.

Al igual que con la creación de la AC-SENECYT, el proceso de creación se repite con la diferencia que se debe separar el certificado de solicitud (request), antes que se auto firme; y lograr firmarlo con la AC-SENECYT, siendo esto un reto, debido a que Globus Toolkit, al momento de ejecutar la sentencia grid-ca-create firma el request en cuanto se termina de ingresar los parámetros solicitados.

En este punto, es necesario destacar que se debe contar ya con el archivo que distribuye la AC-SENECYT, donde sus respectivos archivos se encuentran en el directorio de AC de confianza, para verificar que no existe inconveniente con estos archivos, se ejecuta la sentencia grid-default-ca, despliega el listado de las autoridades certificadoras disponibles.

4.3 Certificados Digitales en Globus Toolkit.

Partiendo de la primicia inicial en la cual se fundamenta la Computación Grid, de compartir procesamiento y almacenamiento sobre internet, de elementos computacionales dispersos geográficamente, surgen Las cinco ideas principales de Smart Grid.

- Compartir recursos.- Mecanismos para establecer confianza y responsabilidad.
- Seguridad.- políticas de acceso, autenticación, autorización.
- Balance de tareas.-Balance óptimo de tareas.
- Eliminación del factor distancia.- actualmente ya es realidad en telefonía.
- Estándares abiertos.- Arquitectura de Código Abierto para el Grid OGSA por siglas en ingles de Open Grid Services Architecutre, con el paquete Globus Toolkit.

La seguridad para estas ideas por lo tanto deberá ser elevada para proteger y permitir el acceso a los Componentes fundamentales del Grid.

Globus Toolkit proporciona una Infraestructura de Seguridad denominada GSI (Grid Security Infrastructure) basados en sistema de clave pública, GSI extiende y se construye sobre el protocolo TLS (Transport Layer Security). Adicionalmente se utiliza el estándar de protocolos de Internet para las comunicaciones. Para la autenticación, protección de las comunicaciones y autorización utiliza certificados digitales que son el vehículo que SSL utiliza para la criptografía de clave pública.

La autenticación en Globus Toolkit está fundamentada en certificados X.509, como se puede observar en la Figura 25 se cuenta con un ejemplo de Certificado Digital creado ya en ambiente Smart Grid. El ente principal para la autenticación GSI es el certificado. Cada usuario, servicio se identifican mediante un certificado, que contiene información vital para la identificación y autenticación del usuario o servicio.

Las partes principales de un certificado GSI incluye la siguiente información:

- Nombre de sujeto, o subject name, identifica a la persona u objeto que representa el certificado.
- La clave pública perteneciente al sujeto.
- La identidad de una entidad emisora de certificados AC, firma y certifica que la clave pública y la identidad pertenecen al sujeto.
- La firma digital de la AC.

El vínculo entre la clave pública y el sujeto en el certificado viene establecido por la AC, para confiar en el certificado y su contenido, el certificado de la AC debe ser de confianza para el ambiente Grid, además deberá quedar establecido el vínculo entre la AC y el certificado o de lo contrario el sistema no es digno de confianza.

Los Certificados GSI como ya se mencionó, están codificados en el formato de certificados X.509, formato standard para certificados, establecidos por la Internet Engineering Task Force (IETF). Estos certificados se pueden compartir con otros programas basados en clave pública, incluyendo navegadores web, como se puede visualizar en la Figura 26.

4.4 Gestión de Certificados en la AC de Entidad Final del Modelo.

Las entidades finales que se podrá certificar bajo un ambiente Smart Grid son:

Figura 28. Entidades Finales Certificables.

Para gestionar los certificados creados por la Infraestructura, la encargada de emitirlos será la Autoridad Certificadora Subordinada, para la investigación se la denominó como AC-Universidad, la misma que recibirá solicitudes, las procesa y emite un resultado.

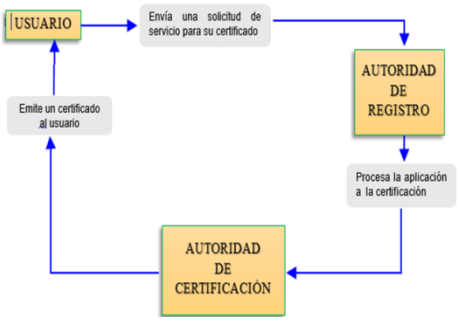


Figura 29. Proceso de Gestión de un Certificado.

La Autoridad Certificadora deberá ser gestionada por una o varias personas con conocimientos sólidos en Linux y deberá atender y dar solución a las peticiones que conforme sean solicitadas se las pueda solventar, además deberá estar vinculada a la entidad emisora de certificados bajo un contrato de confidencialidad debido al manejo de información de alta vulnerabilidad.

Para gestionar el ciclo de vida de los certificados es importante destacar que todos los comandos Grid, se los debe ejecutar como usuario root la Figura 14 ilustra como ejecutar el comando sudo su.

4.4.1 Emisión

Primer paso Crear el request o solicitud para la creación de un nuevo certificado ejecutando la sentencia grid-cert-request –force, el directorio para nuevas solicitudes está ubicando en /root/.globus.

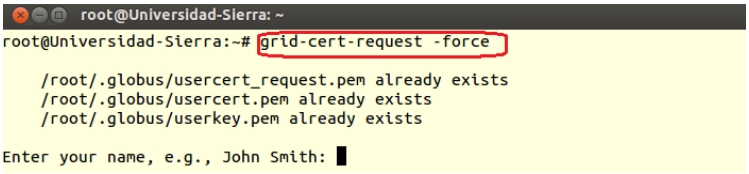


Figura 30. Solicitud de Certificado.

Como segundo paso solicita el nombre de la entidad final a la cual pertenecerá el certificado, luego ingresar la clave para el archivo de solicitud en formato .PEM.

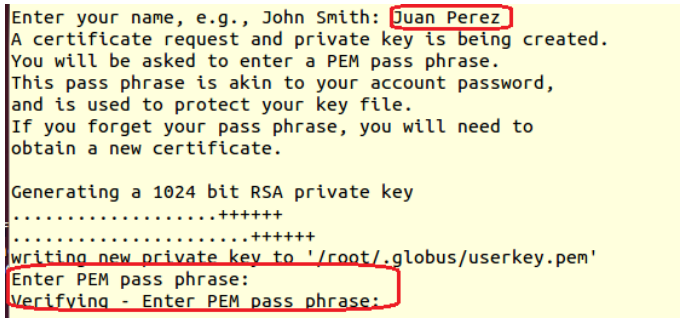


Figura 31. Datos de la solicitud de nuevo Certificado.

Esta sentencia además Genera la clave privada para el certificado en el directorio /root/.globus/userkey.pem.

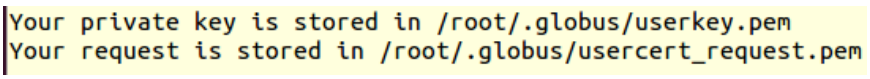


Figura 32. Ubicación de la solicitud y de la llave privada.

El siguiente paso es firmar la solicitud para generar el nuevo certificado, para conseguir esto es necesario digitar la ubicación de la solicitud para hacer uso de la sentencia Grid, grid-ca-sign -in /root/.globus/usercert_request.pem -out usercert.pem.

Figura 33. Sentencia Grid para firmar solicitudes de Certificados.

Para realizar la firma solicitará la clave de la llave privada de la Autoridad Certificadora, luego de ingresar la clave correctamente, genera el nuevo certificado firmado el nombre del archivo está establecido por el archivo de configuración Serial establecido como números secuenciales, en este caso lo denomina 04.pem

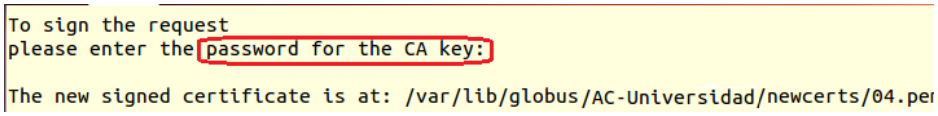


Figura 34. Ubicación del certificado generado.

Además actualiza el archivo de configuración index.txt, que hace las veces de base de datos de todos los certificados donde se puede verificar el status de un certificado, para el caso de nuevos certificados establece la letra [V=Validate].

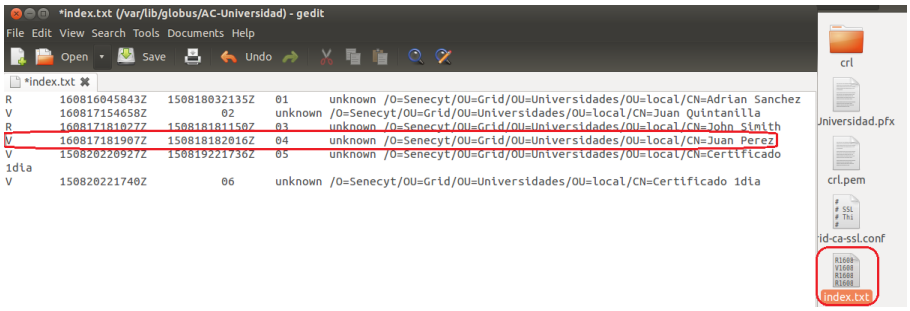


Figura 35. Índex de los certificados generados.

Los siguientes pasos a seguir son:

- Convertir el certificado al formato pfx.
- Generar la clave de exportación.

- Publicar de forma segura el certificado.

4.4.2 Revocación

La AC Recibe la Solicitud de Revocación del certificado, ubica el hash del certificado de AC, esto se puede realizar con el comando grid-default-ca.

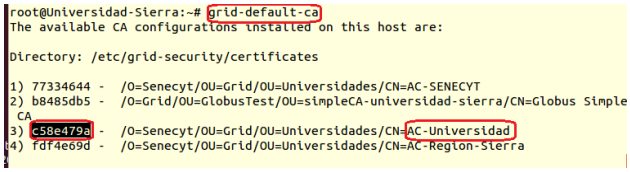


Figura 36. Identificación hash de la AC.

Luego ubicare en el directorio de la Ac, cd /var/lib/globus/AC-Universidad, para luego ejecutar el comando openssl ca -config grid-ca-ssl.conf -gencrl > c58e479a.crl, teniendo así, la lista de revocación.

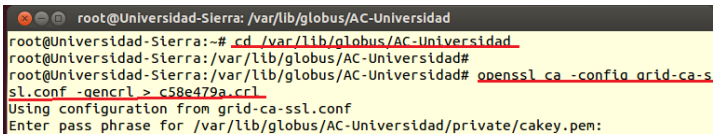


Figura 37. Creación de la Crl.

La nueva lista de revocación será creada con el nombre hash de la AC, y con extensión .crl, ubicada en el directorio /var/lib/globus/AC-Universidad

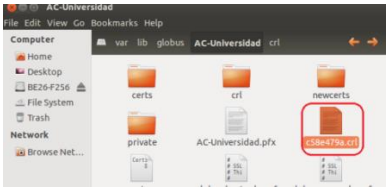


Figura 38. Ubicación de la Crl.

Para revocar un certificado, es necesario la clave privada del mismo, primer paso ubicarse en el directorio de la AC, cd /var/lib/globus/AC-Universidad y ejecutar el comando, openssl ca -config grid-ca-ssl.conf -revoke newcerts/01.pem, este comando revocara el certificado 01.pem, ubicado en el directorio newcerts, y lo copia al directorio crl.

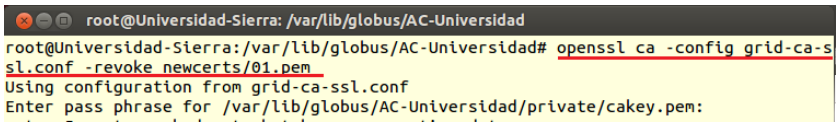


Figura 39. Revocación de un certificado

Además, Actualiza la base de Datos con la etiqueta [R= Revocate], para actualizar el archivo de crl, se debe ejecutar el comando, openssl ca -config grid-ca-ssl.conf -gencrl -out crl.pem.

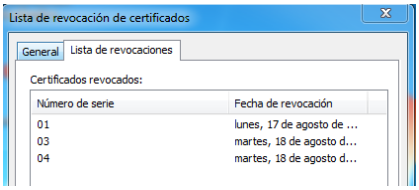


Figura 40. Lista de Certificados Revocados.

Como siguiente paso, se publica de forma segura la lista de certificados revocados para que las entidades puedan verificar la validez de un certificado.

4.4.3 Suspensión

- La AC, recibe la solicitud de Suspensión.
- Revoca el certificado, por determinado tiempo, ya que en los certificados grid, solo cuenta con estas tres opciones para un certificado "V" (Valid), "R" (Revoked) o "E" (Expired).
- Actualiza la base de Datos [R= Revocate].
- Crea y dispone una nueva CRL para ser publicada de forma segura.

4.4.4 Renovación

- La AC, recibe la solicitud de Renovación.
- Busca el certificado por su número de serie.
- Establece nueva caducidad.
- Firma el certificado.
- Actualiza la Base de Datos con la etiqueta [V=Validate].

CAPÍTULO 5

APLICACIONES PKI SMART GRID

La computación Grid tiene varios puntos comunes tanto con sistemas distribuidos como paralelos, pero también difieren de estas arquitecturas en varios aspectos. Como en los sistemas distribuidos, debe integrar dispositivos de muchos y diferentes tipos conectados por redes y a menudo localizados en diferentes dominios administrativos. Sin embargo, las necesidades de las aplicaciones pueden requerir de modelos e interfaces radicalmente diferentes de los usados en sistemas distribuidos. Por otro lado, al igual que en un sistema paralelo, las aplicaciones de computación Grid limita la aplicación de las actuales herramientas y técnicas de paralelización. Estas consideraciones muestran que mientras la computación Grid puede construirse sobre tecnologías tanto distribuidas como paralelas, necesita además de importantes avances en mecanismos de comunicación, técnicas y herramientas.

(Se considera cuatro tipos de aplicaciones:

- **De escritorio** (Desktop supercomputing)
  Estas aplicaciones conectan la capacidad de visualización de datos con supercomputadoras o base de datos remotas, lo que permite una mejor explotación por parte de los usuarios de los recursos computacionales, al mismo tiempo que consigue una independencia de la distancia entre recursos, desarrolladores y usuarios.
- **De instrumentación** (Smart intrument)
  Aplicaciones que permiten la conexión entre instrumentos que pueden ir desde microscopios hasta satélites, y supercomputadoras remotas. Esta relación puede permitir procesos e interacción de datos en prácticamente tiempo real.
- **Entornos colaborativos**
  Este tercer tipo de aplicaciones acoplan múltiples entornos virtuales para que usuarios en diferentes localizaciones geográficas puedan interactuar con recursos de otras organizaciones.

- **Supercomputación distribuida**

  Las aplicaciones encargadas de acoplar múltiples computadoras para que resuelvan un mismo problema que escapa de la capacidad de una sola máquina, resuelvan un mismo problema que escapa de la capacidad de una sola máquina, así como diferentes componentes de un mismo problema en diferentes arquitecturas.)

5.1 Cifrado Web

Para establecer conexión segura en la página web que será la interfaz gráfica que gestionara el ciclo de vida de los certificados y cumplirá con el rol de Autoridad Registrante, es necesario que esta brinde las prestaciones de seguridad acordes a las de un repositorio web de certificados digitales, para dar cumplimiento con este requerimiento y para demostrar la funcionalidad de los certificados emitidos por la infraestructura creada. Se hará uso de un certificado digital para implementar el protocolo de seguridad web HTTPS, protocolo que combina el protocolo HTTP usado en cada transacción web con el protocolo SSL/TLS usado para establecer comunicaciones cifradas en sitios web.

SSL son las siglas del idioma ingles de Secure Sockets Layer, Capa de conexiones seguras, protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet. En la actualidad este protocolo ha generado un nuevo protocolo basado en SSL y totalmente compatible denominado SSL/TLS, donde TLS se deriva de Transport Layer Security, este nuevo protocolo permite confiar la información personal a sitios web utilizando métodos criptográficos mientras se navega o se realiza transacciones de envío de datos.

5.1.1 Creación de Certificado SSL/TLS

La estructura de Llave Pública creada bajo el ambiente Smart Grid, permite crear certificados Digitales que soportan este protocolo, garantizando la vinculación entre un servidor o entidad con su llave pública; Dentro de la infraestructura la Autoridad Certificadora encargada de emitir este certificado es la AC-SENECYT, siguiendo los mismos pasos para la emisión de Certificados.

Como primer paso es ingresar a la máquina virtual que cumple con las funciones de Autoridad Certificadora Puente, SENECYT, abrir una nueva terminal , cambiar la consola a modo root, con el comando sudo-su e ingresar la clave de root, luego de esto digitar el comando para solicitar un nuevo certificado: grid-cert-request –force.

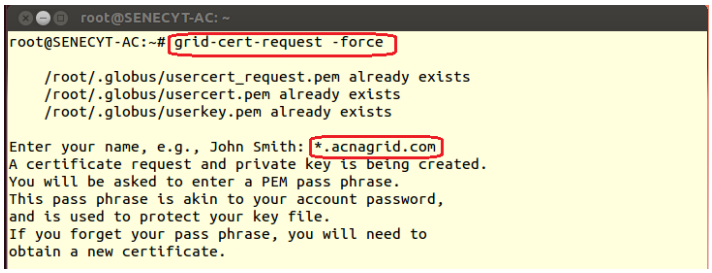


Figura 41. Solicitud de Certificado.

Ingresar el nombre de *.acnagrid.com, es el nombre del dominio de la página, obteniendo así la solicitud de certificado digital.

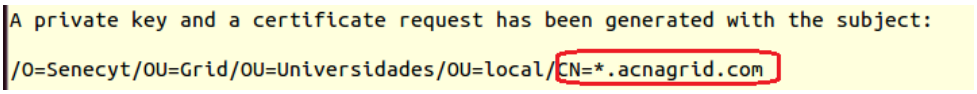


Figura 42. Datos del nuevo certificado.

Siguiente paso es firmar la solicitud para generar el Certificado Digital, para este proceso se apunta al directorio donde se almacena las peticiones de nuevos certificados, el comando para firmar bajo ambiente grid es: grid-ca-sign –in /root/.globus/usercert_request.pem –out usercert.pem.

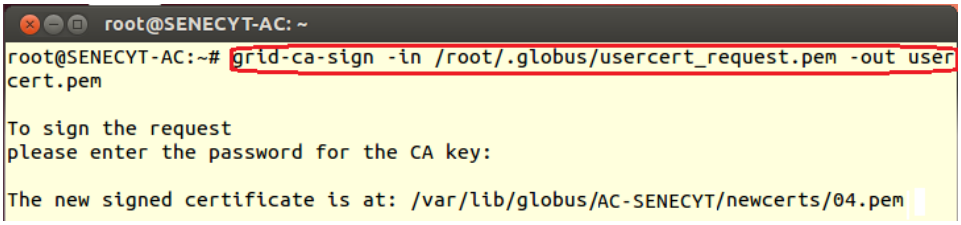


Figura 43. Firma de solicitud.

Para validar la firma ingresar la contraseña de la llave privada de la AC-SENECYT, obteniendo como resultado un nuevo certificado firmado ubicado y nombrado por el secuencial establecido en la configuración de la Autoridad.

Como siguiente paso es necesario cambiar el formato del nuevo certificado, para que sea usando en Sistemas operativos de distribución Windows, para conseguir esto, es necesario ubicarse en el directorio donde se alojan los certificados creados con el siguiente comando cd /var/lib/globus/AC-SENECYT/newcerts.

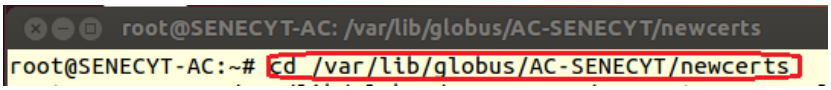


Figura 44. Directorio de nuevos certificados.

Ubicados en este directorio ejecutar: openssl pkcs12 -export -out acnagrid.pfx -inkey /root/.globus/userkey.pem -in 04.pem

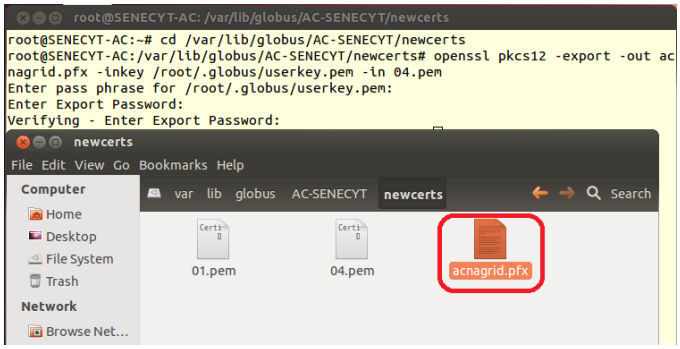


Figura 45. Nuevo formato de certificado.

La sentencia cambia el tipo de archivo de un certificado, para lo cual hace uso de la clave privada del mismo y establece una nueva clave denominada Clave de Exportación, obteniendo como resultado el certificado Digital en formato pfx.

Para hacer uso del nuevo certificado denominado acnagrid.pfx, es necesario quitar los permisos de root para evitar problemas al momento de instalarlo, para ello ingresamos a las propiedades del archivo y se procede a modificar los permisos de Owner y Access.

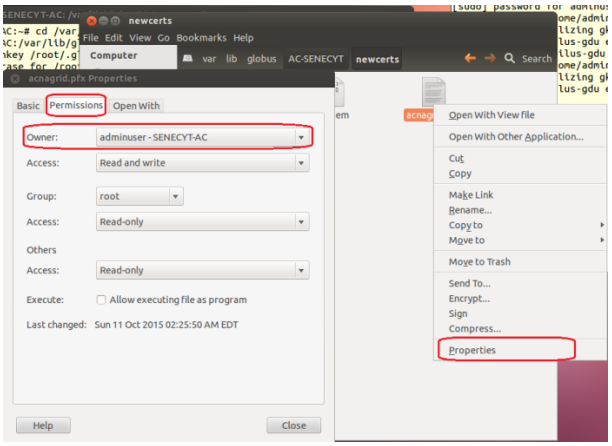


Figura 46. Permisos de usuario de certificado.

Una vez ejecutado este procedimiento se puede visualizar el certificado que estará listo para ser instalado en el servidor web para que levante la aplicación con https.

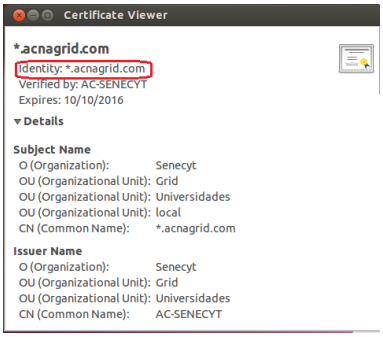


Figura 47. Certificado para SSL/TLS.

5.1.2 Configuración en Servidor

Como antecedentes, es necesario destacar que la infraestructura bajo la cual está desarrollada la aplicación es IIS 7.0 Internet Information Server, en un servidor web con Sistema Operativo Windows Server 2003, donde se procederá con la instalación del certificado acnagrid.pfx.

Para instalar el certificado sobre la aplicación web, primero dirigirse a Inicio – Administrative Tools - Internet Information Services (IIS) Manager, como ilustra la figura.

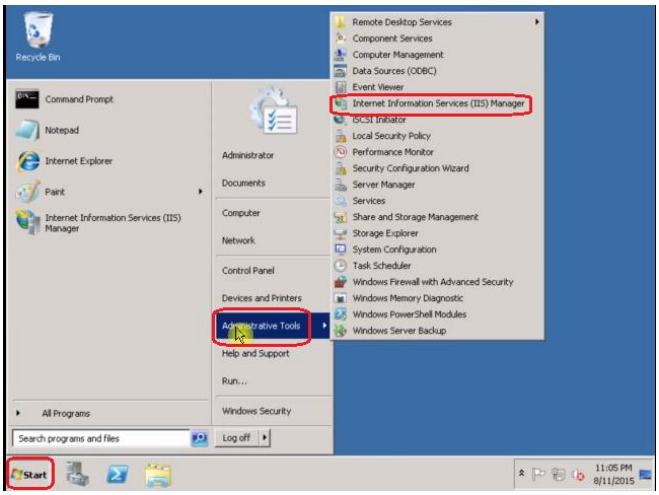


Figura 48. IIS Manager.

Se despliega la nueva ventana del administrador de aplicaciones, en la parte derecha se aprecia la carpeta donde se aloja todos los archivos para que pueda ejecutarse la aplicación, se selecciona la carpeta en este caso está dentro de Default Web Site, la carpeta llamada Certificación luego en el menú de la derecha seleccionar Edite Site en la ventana emergente, seleccionar Add.

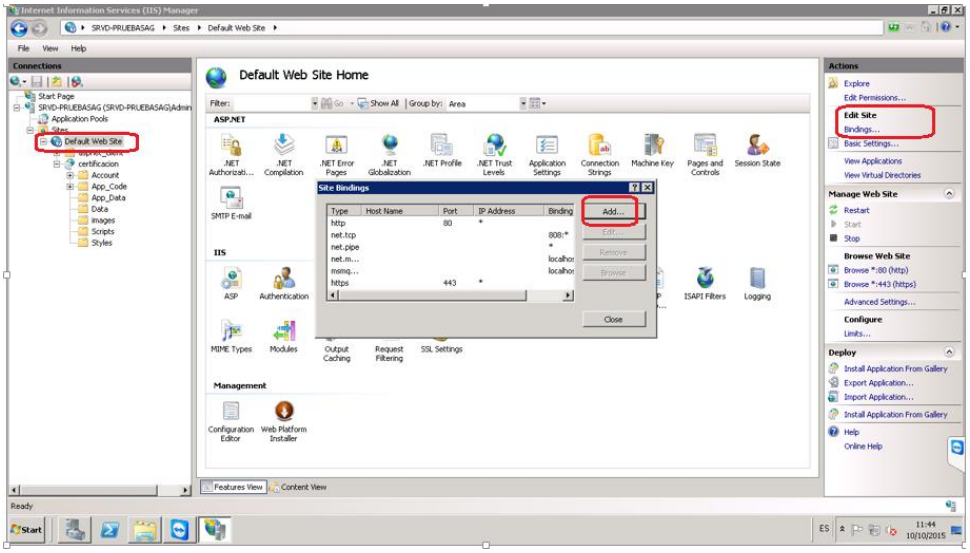


Figura 49. Configuración de IIS.

Se abrirá una nueva ventana para editar y agregar el certificado previamente creado para este fin como ilustra la figura.

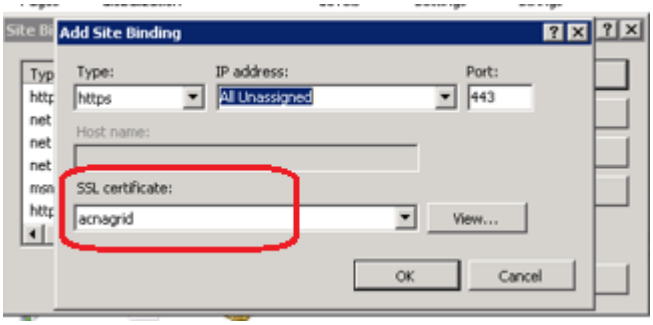


Figura 50. Configuración de https.

5.1.3 Verificación de funcionamiento en cliente

Para revisar que el cifrado web está funcionando sin ninguna novedad, ingresar a la página web del proyecto https://www.acnagrid.com/certificacion/, dependiendo del navegador se puede verificar el certificado instalado para el https de la página.

En Mozilla Firefox, clic en el candado ubicado al lado derecho de la barra de direcciones, se puede visualizar el dominio de la página y la leyenda de Conexión Segura.

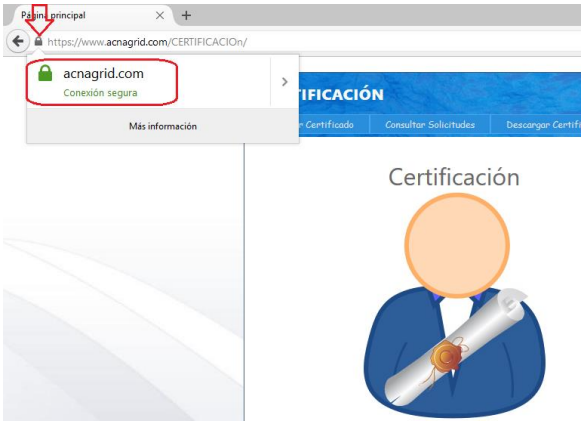


Figura 51. Configuración https en Mozilla Firefox.

Para visualizar el certificado anclado a esta página, clic en Más Información, en la ventana emergente oprimir sobre ver certificado, como ilustra la figura.

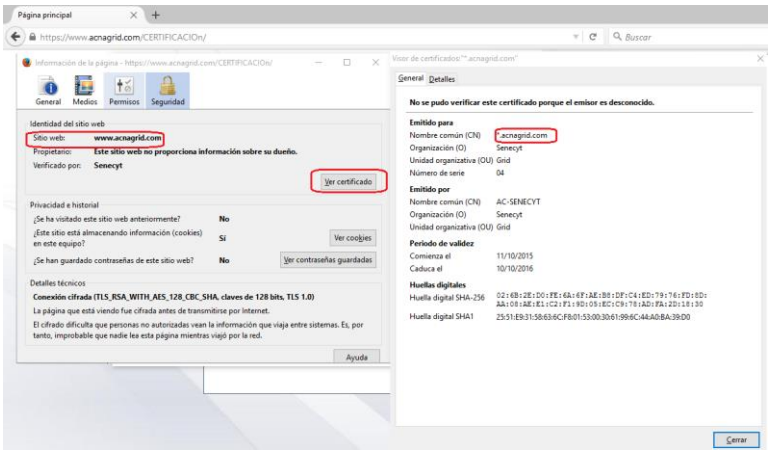


Figura 52. Visualizar certificado en Mozilla Firefox.

El proceso es bastante similar para los dos navegadores más usados en la actualidad, ejemplo Google Chrome, de igual manera se digita la página, en la parte derecha de la barra de direcciones se presiona sobre el icono del candado, despliega las opciones de la conexión.

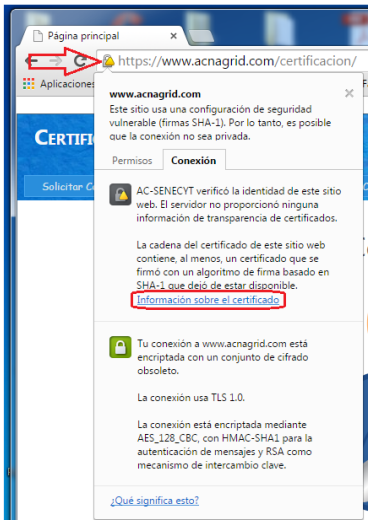


Figura 53. Información https en Google Chrome.

Para ver el certificado, se presiona sobre Información de este certificado, y abre la ventana con los datos del certificado, para revisar el nombre común establecido en la creación del certificado, dirigirse en las pestañas superiores a la opción Detalles.

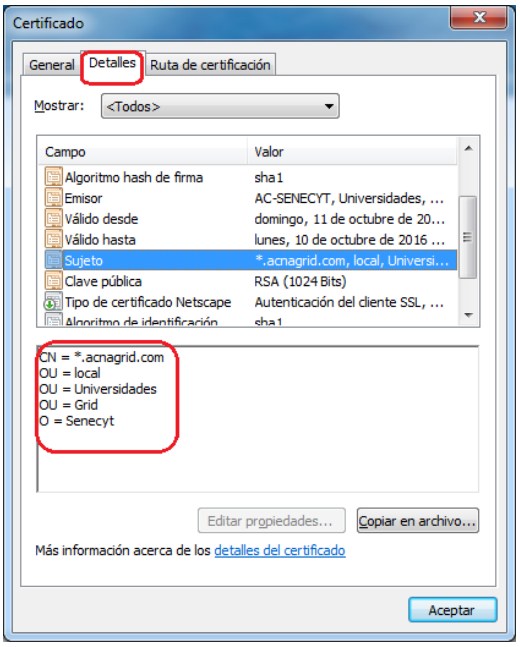


Figura 54. Visualización de certificado en navegador.

En Internet Explorer el icono del candado se encuentra ubicado en la parte izquierda de la barra de direcciones, se procede de igual manera, para visualizar el certificado clic en Ver Certificados, como ilustra la figura.

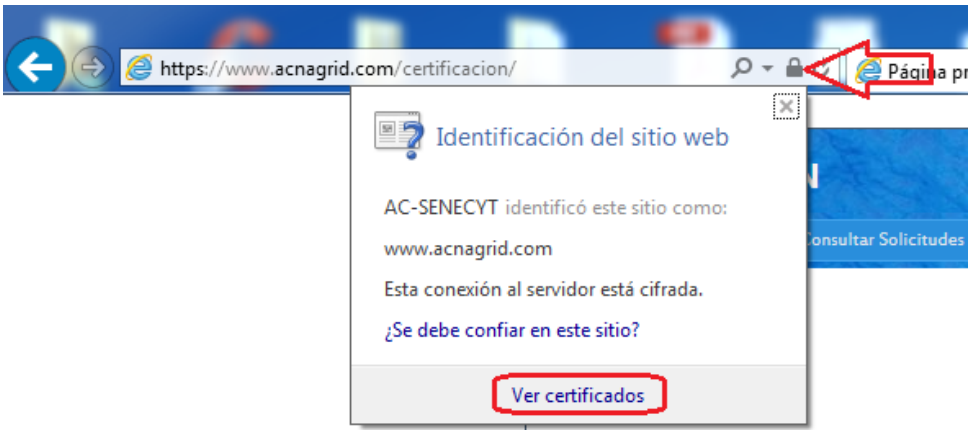


Figura 55. Visualización de certificado en Internet Explorer.

5.2 Firma Digital

Es un método criptográfico que permite tener más seguridad a la hora de emitir un documento de manera íntegra a través de sistemas telemáticos, generalmente la red, o enviados por correo electrónico.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma en el que se emplea una clave privada, al resultado de la operación anterior; generando la firma digital. El software de firma digital debe además efectuar varias validaciones, entre las cuales destacan:

- Vigencia del certificado digital del firmante.
- Revocación del certificado digital del firmante (puede ser por OCSP o CRL).
- Inclusión de sello de tiempo.

5.2.1 Instalación de herramienta para firmar archivos PDF

La herramienta para firmar electrónicamente documentos que se procederá a instalar es JSignPdf es una aplicación Java que añade las firmas digitales a documentos PDF, y es una aplicación recomendada por el Banco Central del Ecuador, misma que dispone de este software para realizar la descarga en la página https://www.eci.bce.ec/web/guest/paso_3.

Se puede utilizar como una aplicación independiente o como un add-on en OpenOffice.org en el caso de ambientes de distribución Unix, JSignPdf es un software de código abierto y puede ser libremente utilizado en los sectores privado y empresarial en este caso en el sector de la Educación Superior.

Una vez descargado el archivo instalador se procede con la instalación que no es tan complicada y se deberá seguir los pasos del asistente de instalación.

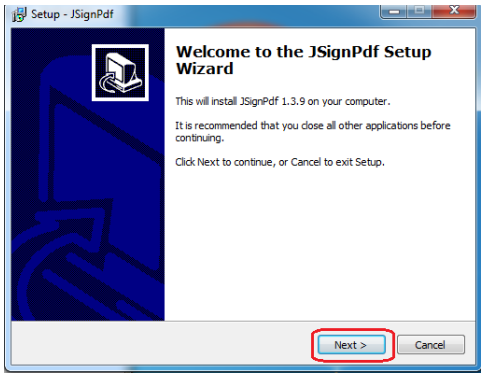


Figura 56. Instalación de JSingPdf.

Al pulsar doble clic sobre el instalador aparece la ventana de bienvenida, dar clic en Next, luego aceptar los términos de licencia y pulsar Next.

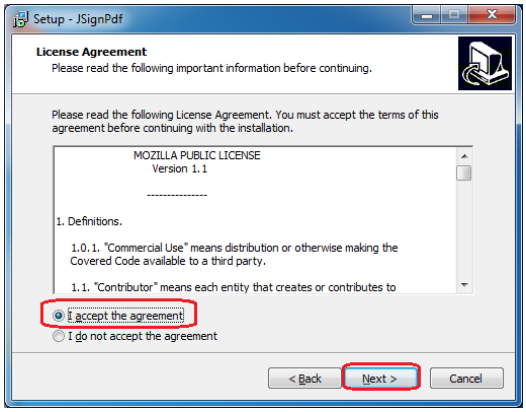


Figura 57. Condiciones del software JSingPdf.

Seleccionar la carpeta de destino en este caso dejar la que viene por defecto, clic en Next.

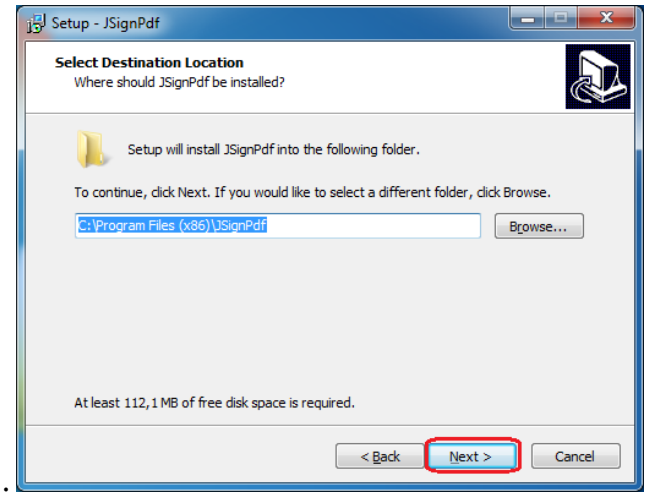


Figura 58. Instalación de JSingPdf.

Como paso final en la siguiente ventana pulsar Install.

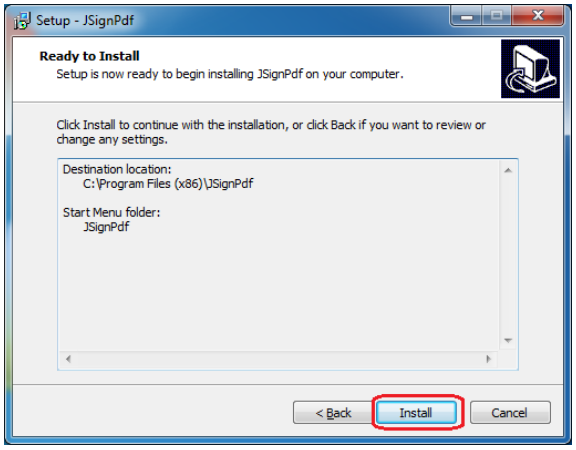


Figura 59. Instalación de JSingPdf.

5.2.2 Firmar archivos

Para firmar un archivo considerar que ya se cuenta con el certificado digital instalado al igual que el software para firmar archivos PDF, abrir la aplicación JSignPdf Inicio - Todos los Programas – JsignPdf.

Una vez abierto el programa por defecto aparecerá la siguiente ventana, percatarse que los checkbox de Advanced view y de Visible signature este marcados, de igual manera el primer campo Keystore type este seleccionado PKCS12, formato del certificado digital a ser usado para la firma.

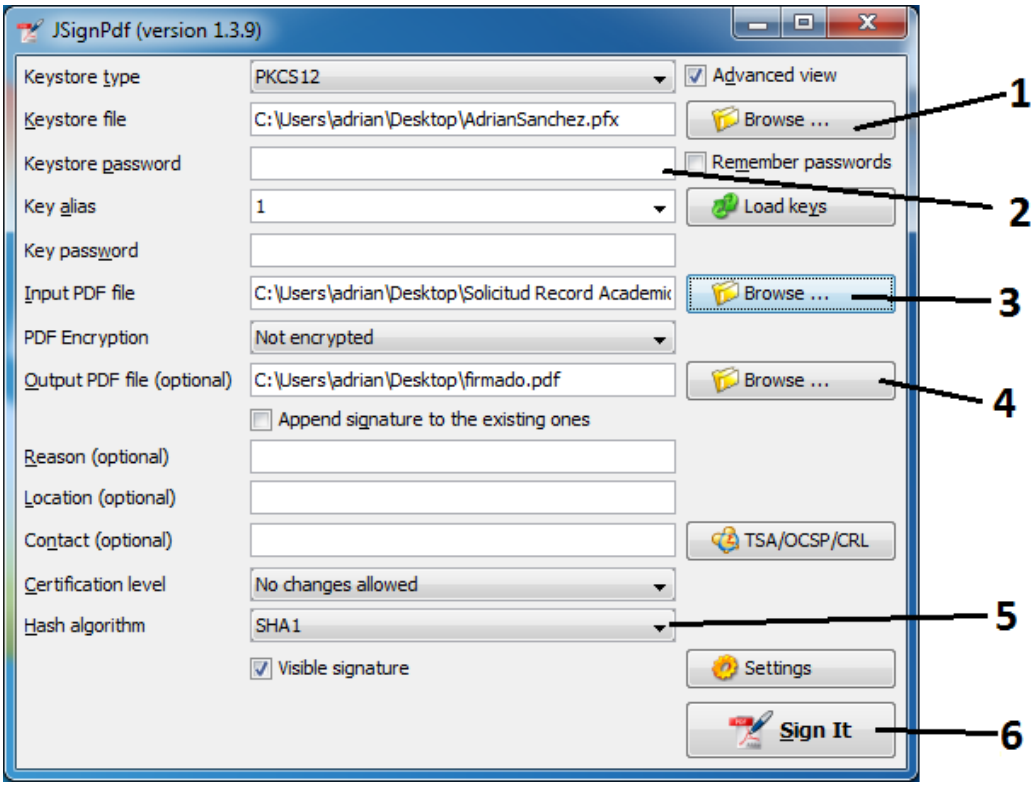


Figura 60. Firma de Archivos.

A continuación un resumen con los pasos que deben estar configurados previos a la firma.

1. Cargar el certificado digital con el que se va a firmar.
2. Ingresar la clave de exportación para el certificado.
3. Se ubica el archivo PDF que va a ser firmado ejemplo “Solicitud Record Académico .pdf”.
4. Establecer nombre al nuevo archivo que será el que contenga la firma.
5. Seleccionar como algoritmo hash SHA1.
6. Se procede a firmar el documento.

Teniendo como resultado Firma Creada Correctamente, para verificar la firma deberá ubicarse en el archivo en la carpeta que se indicó en el software previo a la firma.

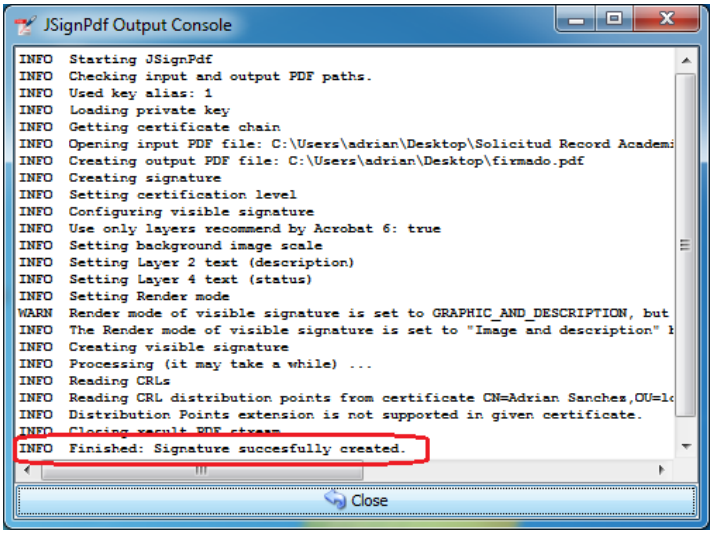


Figura 61. Consola de Firma de documentos.

Abrir el nuevo documento firmado, en este caso con Adobe Acrobat Reader versión 2015, identifica el archivo como firmado digitalmente además de agregar una firma visible al pie del documento, dar clic en Panel de Firma para visualizar el certificado y percatarse que efectivamente fue firmado por el certificado digital emitido por la Autoridad Certificadora No Acreditada bajo un Ambiente Smart Grid.

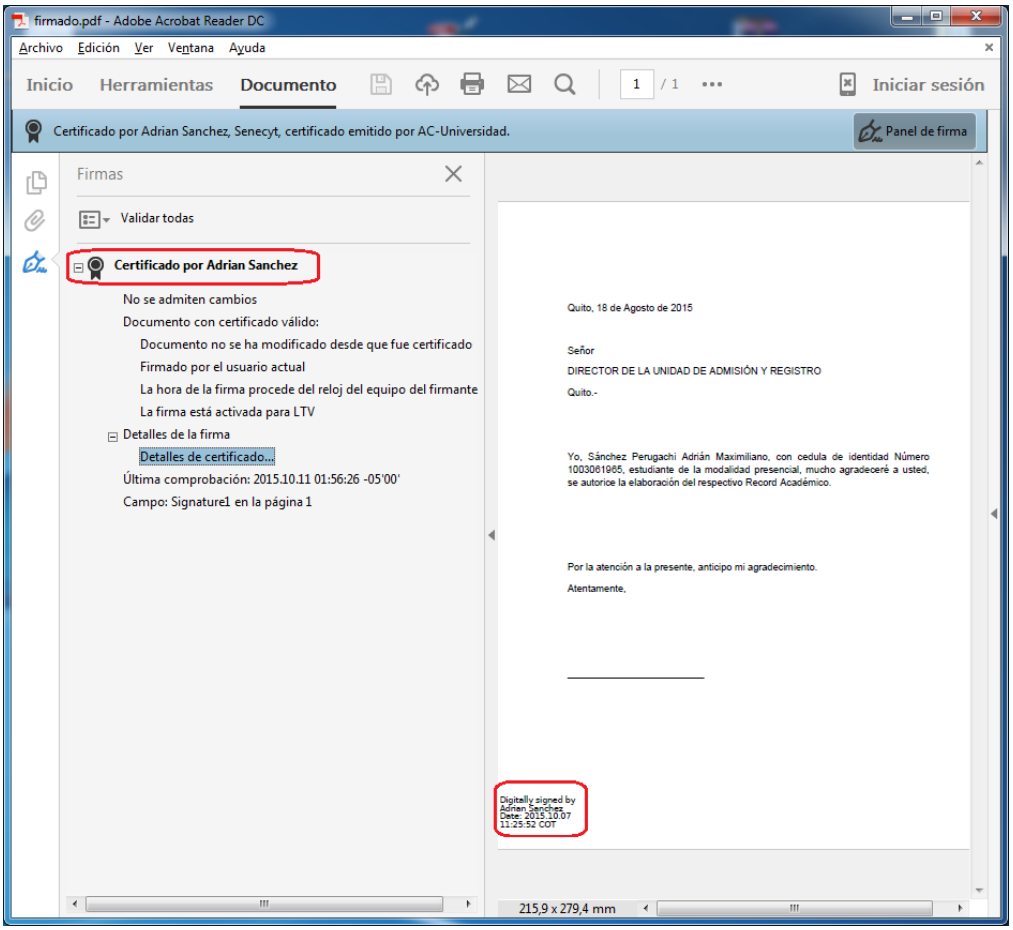


Figura 62. Documento firmado digitalmente.

5.3 Correo Seguro

Mediante el Grid se puede incorporar múltiples componentes de seguridad que establecen la identidad de los usuarios o servicios (autenticación), proteger las comunicaciones, y determinar quién está autorizado para llevar a cabo las acciones (autorización), así como gestionar las credenciales de usuario.

Muchos sistemas de correo electrónico, utilizan estándares como:

- Privacy Enhanced Mail (PEM).
- Secure/Multipurpose Internet Mail Extensions (S/MIME).

Para un correo seguro se utilizan certificados digitales, firmas digitales, para el intercambio de claves cifrar y descifrar mensajes.

Para realizar la verificación de un certificado digital emitido por la infraestructura Certificadora, una de las aplicaciones que servirá de apoyo es Correo Seguro.

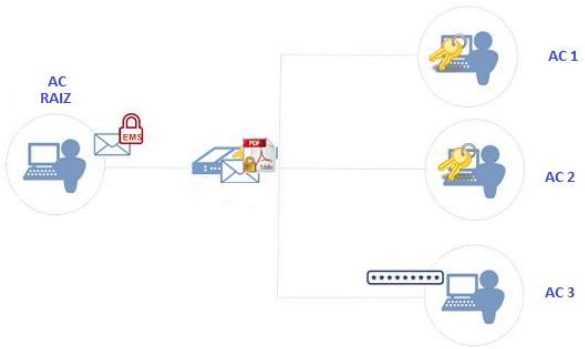


Figura 63. Lista de Certificados Revocados.

Se debe incluir un medio eficaz para la prevención de la entrega de correo electrónico que viole las políticas entre cada AC de confianza, ya que sin ello pueden poner en aislamiento o bloquear correos electrónicos que contiene malware detectado, ataques de phishing, spam y otros contenidos maliciosos. Esto evita muchos ataques que impidan que lleguen a los destinatarios de otras AC, las credenciales de usuario y los datos sensibles.

5.3.1 Configuración en Cliente de Correo Electrónico.

El software de cliente electrónico que será utilizado es Microsoft Outlook, como antecedentes tener una cuenta de correo electrónico valida y funcional.

Abrir Outlook, Inicio – Todos los Programas – Microsoft Office – Outlook,

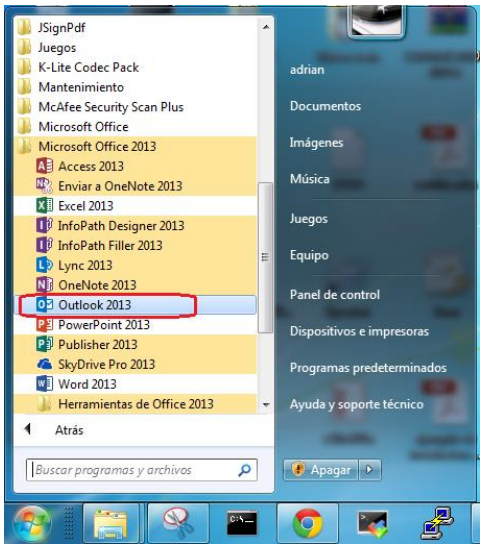


Figura 64. Cliente de correo Electrónico.

En la siguiente pantalla llenar los datos respectivos correctamente, luego pulsar Siguiente., pulsar siguiente.

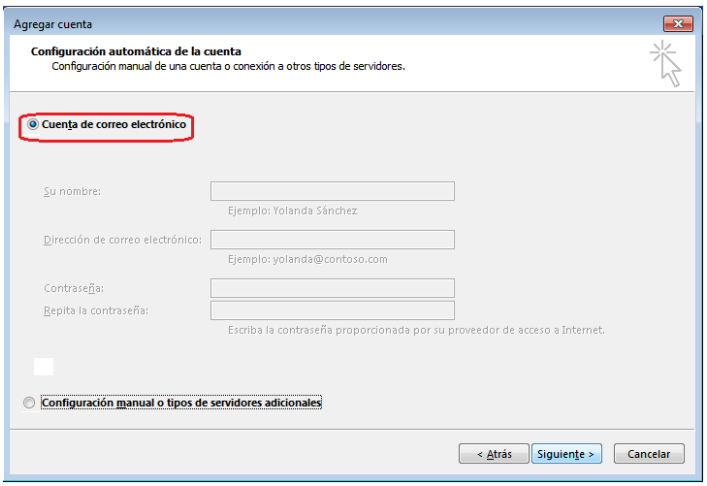


Figura 65. Agregar cuenta de correo electrónico a Outlook.

Realiza la comprobación de conexión con el servidor al cual se tiene la cuenta de correo electrónico.

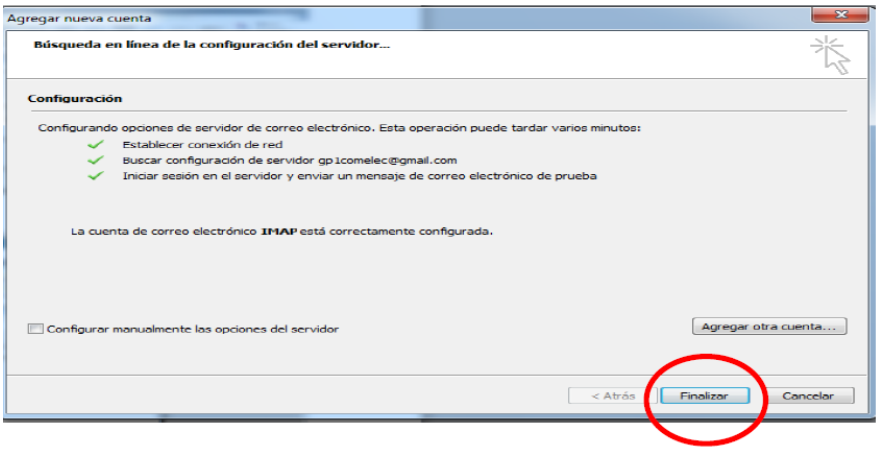


Figura 66. Agregar cuenta de correo electrónico a Outlook.

Clic en Finalizar, para así tener agregada una cuenta a nuestro cliente de correos electrónicos, como ilustra la siguiente figura.

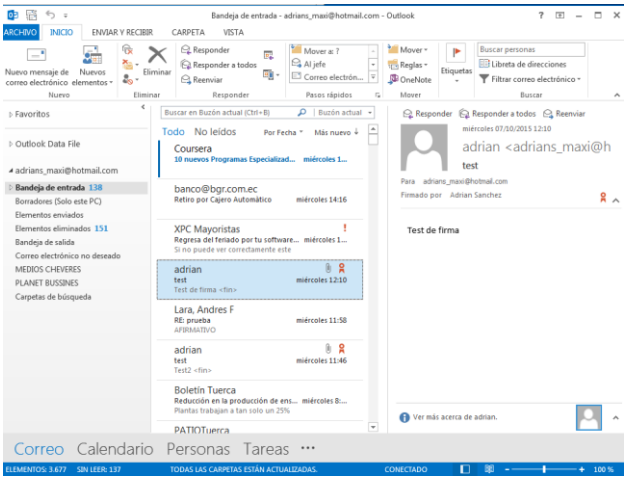


Figura 67. Cliente de correo Microsoft Outlook.

Hasta el momento se cuenta con una cuenta configurada dentro del gestor de correos, como siguiente paso para poder firmar correos electrónicos, el estándar S/MIME requiere que el certificado contenga una dirección de email. Como este no es el caso de los Certificados Digitales bajo el ambiente Smart Grid, Es estrictamente necesario indicar al Outlook que desactive esta comprobación.

Ejecutar en Windows el editor del registro, en Inicio – Ejecutar - Regedit.exe.

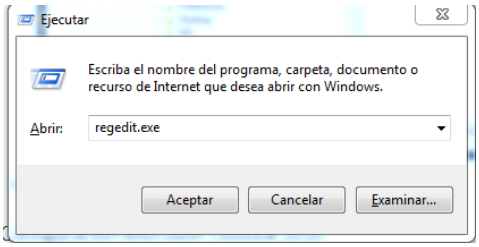


Figura 68 Editor de registros.

Para la versión de Outlook 2010 debe dirigirse al siguiente directorio: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security.

Para la versión de Outlook 2013 dirigirse a: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Security.

Si no existe, crear la clave SupressNameChecks tipo DWORD y asignar el valor 1, como indica la figura.

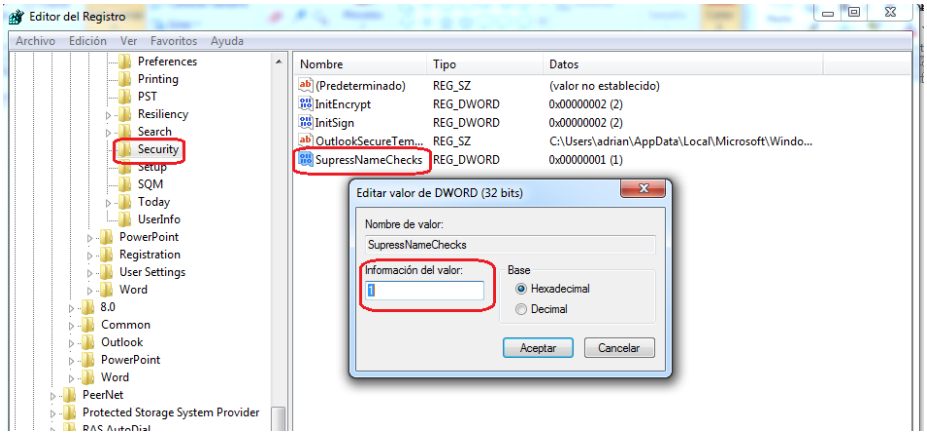


Figura 69. Archivo SupresNameChecks.

Una vez suprimido la verificación propia de Outlook, es momento de configurar la firma digital para correos salientes, para esto Dirigirse dentro de la ventana principal de Outlook en la parte superior Derecha a Archivo – Opciones.

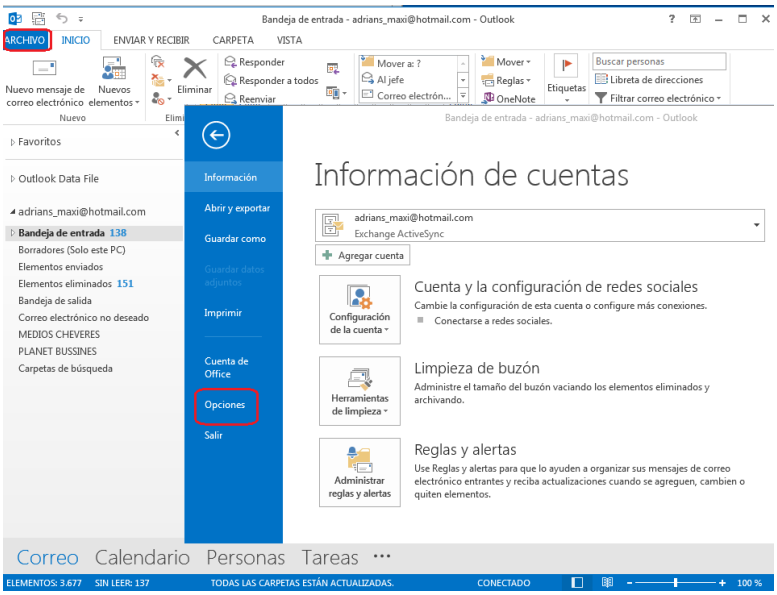


Figura 70. Opciones de Outlook.

Se despliega una nueva ventana titulada Opciones de Outlook, dirigirse a centro De Confianza, en la parte derecha seleccionar Configuración del Centro de confianza.

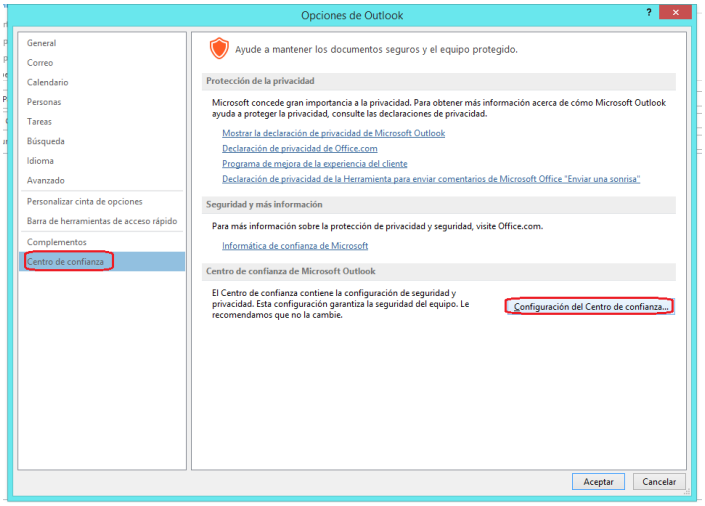


Figura 71. Opciones de Outlook.

Se desplegará la ventana de Centro de confianza en donde se seleccionará en el submenú de la izquierda: Seguridad del Correo electrónico, en la parte derecha marcar la opción agregar firma digital a los mensajes salientes. Luego dar clic en Importar o Exportar.

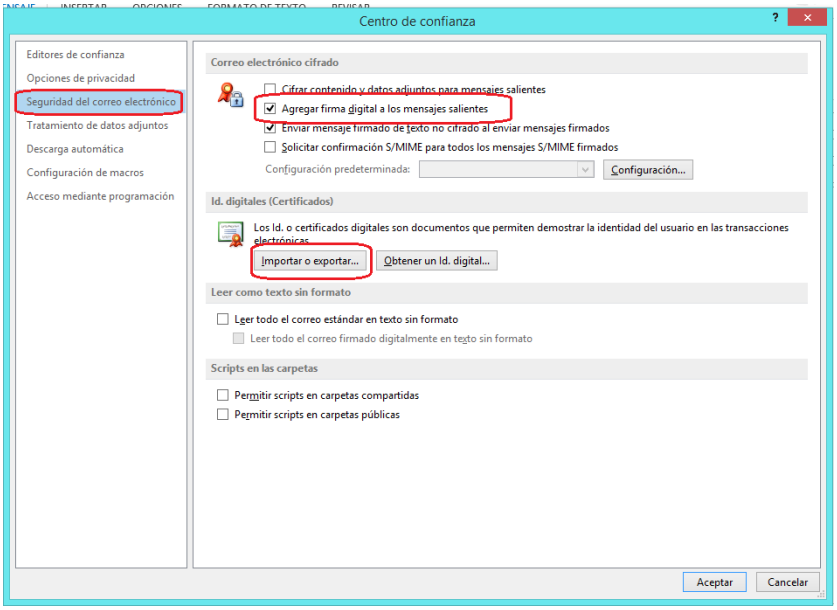


Figura 72. Centro de confianza de Outlook.

En la ventana de Importación Clic en Examinar, buscar la ubicación del Certificado Digital instalado y dar doble clic, luego en Contraseña digitar la clave de Exportación proporcionada por la página.

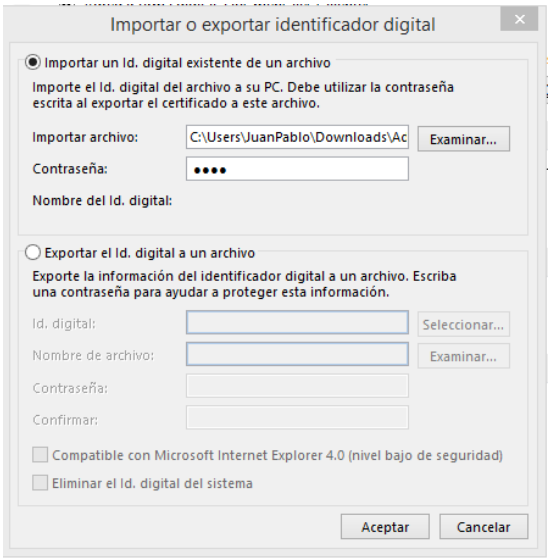


Figura 73. Importación de certificado en Outlook.

Como paso final en la ventana de centro de confianza clic en configuración

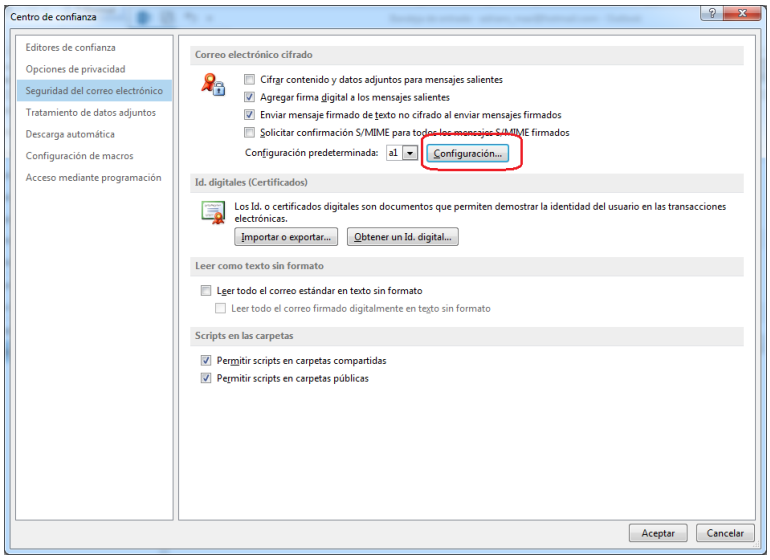


Figura 74. Configuración centro de Confianza.

En la ventana emergente, Establecer un nombre a la configuración de seguridad, percatarse que todos los checkbox estén marcados como en la imagen, luego en certificados y Algoritmos dar clic en Elegir, confirmar el certificado Digital y dar clic en Aceptar.

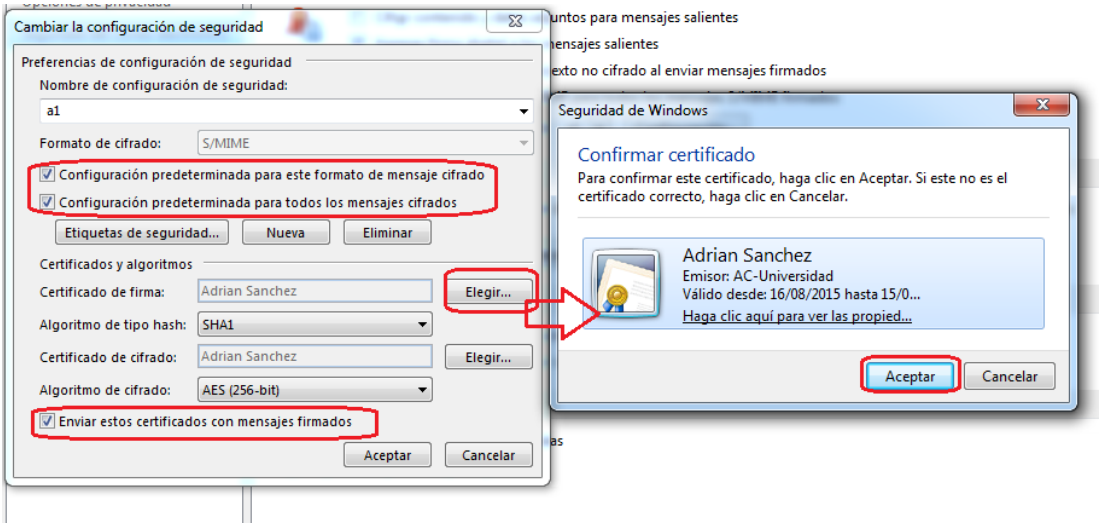


Figura 75. Configuración centro de Confianza.

Se procede aceptar todos los cambios realizados, para salvar la configuración para firmar digitalmente los correos a ser enviados.

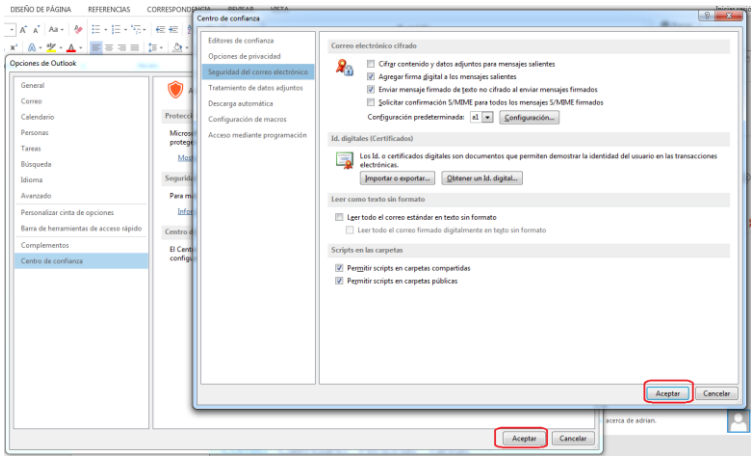


Figura 76. Guardar cambios en Configuración.

5.3.2 Verificación de funcionamiento

Al crear un nuevo mensaje de correo electrónico este, tendrá la capacidad de ser enviado con la firma digital del certificado creado bajo la infraestructura Grid. Para esto en la barra de herramientas de Microsoft Outlook dar clic en Nuevo mensaje de correo electrónico.

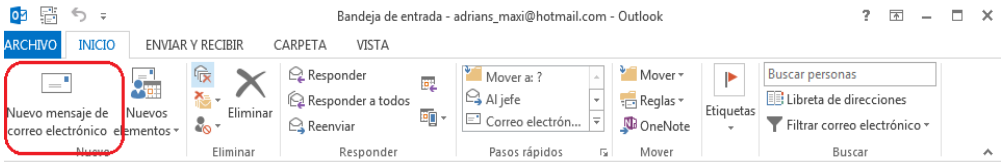


Figura 77. Nuevo Mensaje en Outlook.

Esta opción despliega una nueva ventana para digitar un nuevo mensaje, dentro de esta ventana dirigirse a Opciones, se puede observar como la opción firmar se encuentra activada.

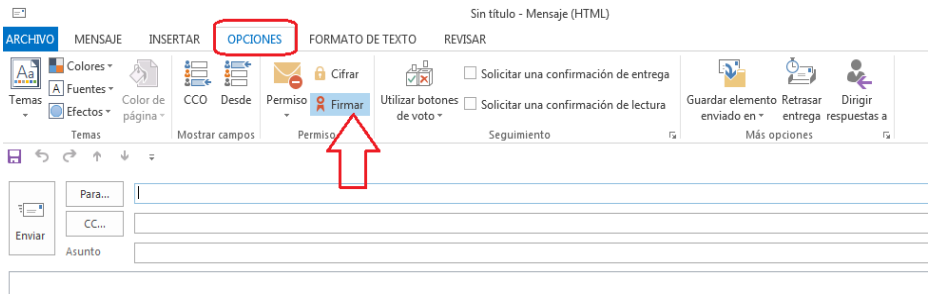


Figura 78. Opción de firma sobre nuevos mensajes.

Como paso de verificación que efectivamente se enviará un correo firmado, se procede a enviar un mail de prueba, puede ser auto enviado a la cuenta configurada anteriormente en Outlook. Para observar que el mail ha sido emitido con firma digital.

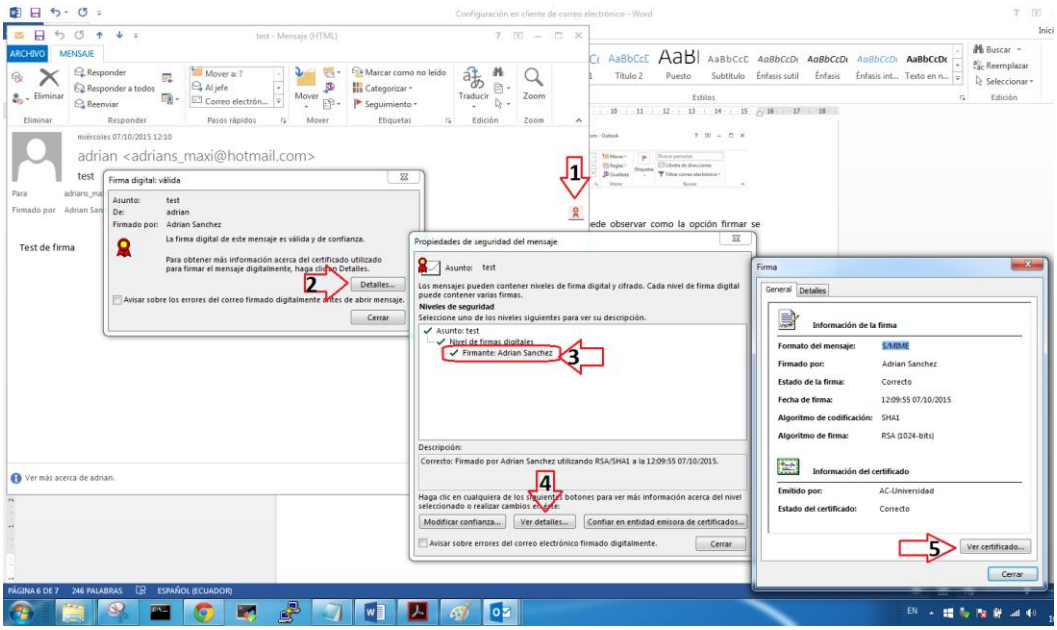


Figura 79. Certificado de firma sobre mensajes enviados.

A continuación un resumen con los pasos que se deben seguir para revisar un certificado digital en un correo electrónico enviado.

1. Pulsar clic sobre el icono de certificado digital.
2. Clic en detalles
3. Seleccionar el último Nivel, la opción Firmante.
4. Clic en Ver detalles.
5. En la nueva ventana emergente clic en Ver certificado.

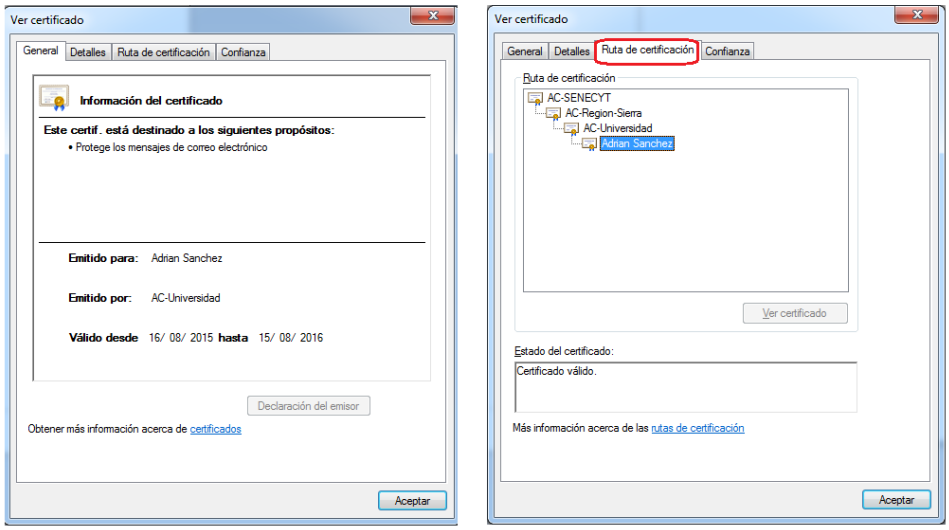


Figura 80. Visualización de certificado.

Es de esta forma como se puede dar positiva la verificación de la firma con el certificado digital antes mencionado, además se puede verificar la Ruta de Certificación.

A manera de prueba se ejecutará la verificación en un receptor de un mail firmado en Outlook, en este caso el receptor cuenta con un cliente de correos electrónicos propio de sistemas de Distribución Mac OS. Denominado Mail.

Posicionarse en el mensaje firmado recibido, clic en la opción Mostrar detalles ubicado en la parte superior derecha.

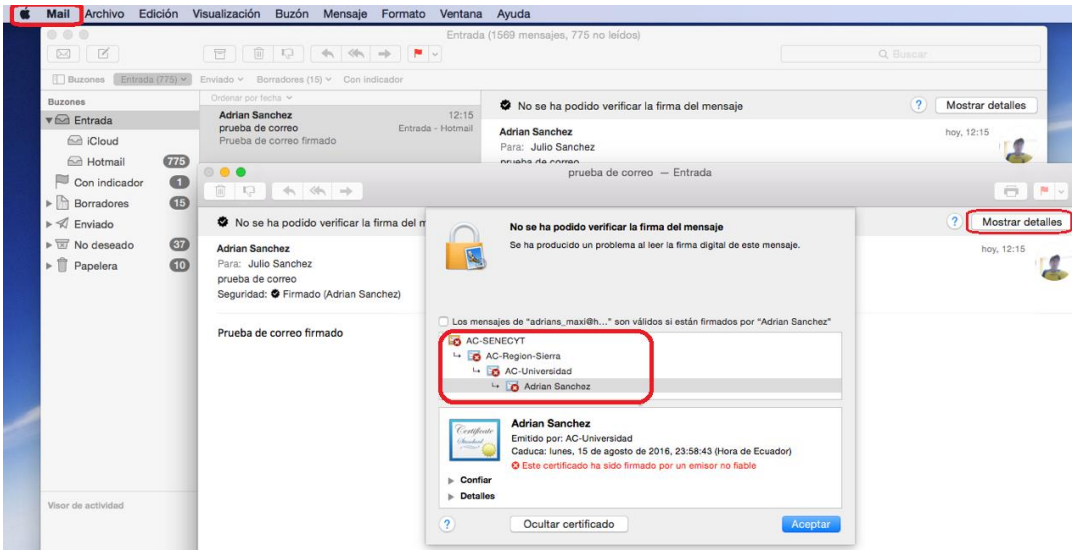


Figura 81. Visualización de certificado sobre Mac OS.

Verificando así la ruta de certificación, y la correcta funcionalidad del certificado utilizado para firmar correos, además que se está comprobando bajo otra plataforma de sistema operativo con el particular que emite un error que el certificado no es fiable, esto se debe a que no se ha instalado los certificados de la ruta de certificación y se ha establecido la respectiva confianza en la entidad certificadora que emitió este certificado.

5.4 S/MIME

S / MIME (Secure / Multipurpose Internet Mail Extensions) se utiliza para cifrar y firmar mensajes de correo electrónico por estándar X.509, para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME que permite a los usuarios firmar digitalmente y cifrar correo electrónico para firmar o cifrar mensajes de correo electrónico.

S / MIME ofrece que exista integridad de los mensajes entre AC confiables, la autenticación, la privacidad a través de la encriptación de datos, y no repudio a través de la firma digital.

S / MIME interactúa con los certificados digitales en las siguientes áreas:

- Acceso con el control S / MIME.
- S / MIME y recuperación de certificados digitales.
- S / MIME y validación de certificados.
- S / MIME y operaciones S / MIME.
- S / MIME y tarjetas inteligentes.
- S / MIME y capacidades de cifrado S / MIME.

Beneficios:

- Evitar la manipulación de correo electrónico.
- Evitar la exposición del contenido de correo electrónico.
- Comunicación flexible y segura.
- Fácil de implementar.

5.5 Cifrado XML

El cifrado XML es ya un concepto familiar para la mayoría de los profesionales de seguridad y adoptado por los protocolos comúnmente usados en Internet para garantizar la confidencialidad.

A nivel de red el cifrado de datos se usa en SSL/TLS o IPSec. A nivel de aplicación, se usan los estándares de PKCS7/CMS o XML para la protección de los documentos y S/MIME o WS-Security para la protección de mensajería.

El uso de la PKI permite el cifrado global para grupos de personas, no obstante introduce la necesidad de gestión de las claves asimétricas y los certificados digitales. Su funcionamiento se basa en usar certificados digitales para obtener la clave pública con la que se cifrará una clave simétrica de cifrado, de forma que cada receptor pueda acceder a ésta y descifrar los datos usando su clave privada. El procedimiento incluye la evaluación previa de la validez y la fiabilidad de los certificados digitales para determinar, de esta forma, qué receptores podrán acceder a los datos.

5.6 IKE

Los certificados de clave pública acaban con la necesidad de que los sistemas que se comunican compartan material de claves secreto fuera de banda. A diferencia de las claves previamente compartidas, un certificado de clave pública se puede utilizar en un equipo portátil o en un sistema cuya numeración podría cambiar.

Los certificados auto firmados requieren menos carga que los certificados públicos de una autoridad de certificación, pero no se escalan fácilmente.

En la consola del sistema, asuma el rol de administrador principal o conviértase en súper usuario.

El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando ssh para un inicio de sesión remota seguro.

5.7 IPsec

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

IPsec está implementado por un conjunto de protocolos criptográficos que sirve para:

1.- Asegurar el flujo de paquetes.

2.- Garantizar la autenticación mutua.

3.- Establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par

de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPIs, y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos.

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- La herramienta de software libre Globus Tool Kit permite la implementación de una SmartGrid y la creación de una entidad certificadora privada, integrando ambas tecnologías en un ambiente estable y seguro. El Globus Tool Kit tiene grandes beneficios para instituciones públicas o privadas que deseen crear una SmartGrid, ya que provee un gran número de servicios que se actualizan periódicamente y de gran calidad, así como aplicativos de seguridad y transferencia de archivos sin costo.

- En la implementación de un SmartGrid fue necesario la utilización de un middleware, mismo que permitió simplificar los procesos para la creación del modelo de autoridad de certificación; y servicios para ofrecer a las entidades finales mayor seguridad de acceso a los datos de las operaciones presentes y sus aplicaciones.

- La utilización de certificados digitales otorgados por entidades propias de en un ambiente SmartGrid, elevan los parámetros de seguridad para la autenticación de los usuarios.

6.2 Recomendaciones

- Implementar las herramientas provistas en el paquete Globus Tool Kit para el desarrollo de ambientes SmartGrid ya que esta permite integrar entidades certificadoras en Grids privadas. Además se puede acceder a los diversos servicios y soportes que GLOBUS ALLIANCE provee con regularidad.

- Hacer uso de las tecnologías actualmente disponibles como el middlewares, globus Toolkit para la implementación de un SmartGrid ya que estos permiten simplificar los procesos y servicios para así ofrecer a los usuarios finales un ambiente factible de uso.

- Los certificados digitales que son emitidos por entidades certificadoras, desarrolladas en el ambiente Smart Grid garantizan legal y tecnológicamente los procesos de autenticación de entidades finales para con la organización.

Bibliografía

(s.f.).

(23 de Octubre de 2003). Obtenido de Proasetel: http://www.proasetel.com/paginas/articulos/obligaciones_entidades.htm

(23 de Octubre de 2003). Obtenido de Proasetel: http://www.proasetel.com/paginas/articulos/obligaciones_entidades.htm

Arnao, D. N. (s.f.). Obtenido de www.uv.es/~montanan/redes/trabajos/PKI.doc

Arnao, D. N. (s.f.).

Arnao, D. N. (2002). *www.uv.es/~montanan/redes/trabajos/PKI.doc.*

C. Adams, S. L. (s.f.). *Understanding PKI: Concepts, Standars and Deployment Consierations.* 2 edition Addison-Wesley Professional.

CÁRDENAS, E. H. (2006). *MODELO DE GESTIÓN DE SERVICIOS PKI BASADO EN UNA ARQUITECTURA ORIENTADA A SERVICIOS.*

Certificación Electrónica Banco Central del Ecuador. (s.f.). Obtenido de https://www.eci.bce.ec/quienes-somos

Certificación, A. A. (s.f.). *www.anf.ec*. Obtenido de https://www.anf.ec/ec/certificacion/pki-anf-ac/autoridad-de-certificacion.html

CUESTA RUIZ, J., & PUÑALES CASTERO, M. (2002). *Scribd.* Obtenido de http://es.scribd.com/doc/116154580/Infraestructura-de-clave-publica-PKI

Data, S. (s.f.). *www.securitydata.net.ec*. Obtenido de www.securitydata.net.ec: https://www.securitydata.net.ec/

Ecuador, B. C. (2015). *www.eci.bce.ec*. Obtenido de https://www.eci.bce.ec/home;jsessionid=c81bec539e5dbec267dee300003f

Ecuador, B. C. (s.f.). *https://www.eci.bce.ec/*. Obtenido de https://www.eci.bce.ec/quienes-somos

EcuadorUniversitario. (2012). Obtenido de EcuadorUniversitario: http://ecuadoruniversitario.com/de-instituciones-del-estado/senescyt/la-senescyt-coordina-el-sistema-de-educacion-superior-con-la-funcion-ejecutiva/

FAO. (s.f.). *www.fao.org*. Obtenido de http://www.fao.org/docrep/004/ad094s/ad094s03.htm

Foster, I. (2002). What is the Grid? En *GRIDToday.*

Fuentes, A., Vazquez , J. L., Huedo, E., Montero, R. S., & Llorente, M. (2005). En *Benefits Achieved in Bioinformatics by Using Grid Computing Technology.*

Gallegos, R. R. (2013). *TERCERA OLA DE TRANSFORMACIÓN DE LA EDUCACIÓN SUPERIOR.* Obtenido de TERCERA OLA DE TRANSFORMACIÓN DE LA EDUCACIÓN SUPERIOR: http://www.educacionsuperior.gob.ec

GRID CAFÉ. (s.f.). Obtenido de Grids Internacionales: http://www.gridcafe.org/grids-internacionales_ES.html

IAEN. (s.f.). Obtenido de http://repositorio.iaen.edu.ec/bitstream/24000/400/4/REGLAMENTO%20PARA%20LA%20ACREDITACION.pdf

infoleg. (s.f.). *infoleg.mecon.gov.ar*. Obtenido de http://infoleg.mecon.gov.ar/infolegInternet/anexos/50000-54999/54714/norma.htm

Judicatura, C. d. (s.f.). *www.funcionjudicial.gob.ec*. Obtenido de http://www.funcionjudicial.gob.ec/index.php/es/inicio.html

Kapil, R. (s.f.). *PKI Security Solutions for the Enterprise.* Wiley.

La Camara de Quito. (12 de Septiembre de 2011). Obtenido de http://www.lacamaradequito.com/uploads/tx_documents/decreto867.pdf

Lapuente, C. G. (21 de Junio de 2011). *Implantación de un sistema de certificados.* Obtenido de http://upcommons.upc.edu/pfc/bitstream/2099.1/12398/1/61021.pdf

LaTecnología PKI. (19 de 11 de 2009). Obtenido de http://glenys-tics.blogspot.com/2009/11/algunas-ventajas-y-desventajas-de-la.html

Ley 2002-67 (Registro Oficial 557-S, 17-IV-2002). (13 de Octubre de 2011). *Desarrollo Amazónico.* Obtenido de http://www.desarrolloamazonico.gob.ec/wp-content/uploads/downloads/2014/05/LEY-DE-COMERCIO-ELECTRONICO-DE-FIRMAS.pdf

Momoth, J. (2012). *Smart Grid Fundamentals of Design and Analysis.* Wiley.