UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

PUESTA EN PRODUCCION DEL SISTEMA DE INFRAESTRUCTURA DE CLAVE PUBLICA (PKI)

Tesis previa a la obtención del Título de Ingeniero en Sistemas Informáticos y Computación.

AUTOR:

Bolívar Eduardo León Ortega

DIRECTORA

Ing. María Paula Espinoza V.

CODIRECTORA

Ing. Carlina Rueda

Loja - Ecuador

2010

CESIÒN DE DERECHOS

Yo, Bolívar Eduardo León Ortega, declaro ser autor del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la universidad”.

Bolívar Eduardo León Ortega

Msc.
María Paula Espinoza Vélez
DOCENTE INVESTIGADOR DE LA ESCUELA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

CERTIFICA:

Que una vez concluido el trabajo de investigación con el tema **"PUESTA EN PRODUCCION DEL SISTEMA DE INFRAESTRUCTURA DE CLAVE PUBLICA (PKI)"** previa la obtención del título de Ingeniero en Sistemas Informáticos y Computación, realizado por el señor Bolívar Eduardo León Ortega egresado de la Escuela de Ciencias de la Computación; haber dirigido, supervisado y asesorado en forma detenida cada uno de los aspectos de la tesis de pregrado.

Además, en mi calidad de DIRECTOR DE TESIS y al encontrar que se han cumplido con todos los requisitos investigativos, autorizo su presentación y sustentación ante el tribunal que se designe para el efecto.

Atentamente,

- -
Ing. María Paula Espinoza
DIRECTOR DE TESIS

AUTORÍA

Las ideas, opiniones, conclusiones, recomendaciones y más contenidos expuestos en el presente informe de tesis son de absoluta responsabilidad del autor.

_____

Bolívar Eduardo León Ortega

DEDICATORIA:

A Dios, que me ha permitido llegar hasta este momento de mi vida y disfrutarlo con las personas que más quiero.

A mis padres, mi razón de ser y la motivación para superarme y ser una persona mejor.

A mis hermanos, quienes siempre han estado presentes cuando los he necesitado.

A mi tío Cesar (+), su vida de lucha y perseverancia marcará siempre la mía.

A mi sobrino Ariel Camilo, mi alegría y mi orgullo.

A mis amigos, con los cuales he compartido experiencias que me han ayudado a forjar mi personalidad.

Bolívar Eduardo

AGRADECIMIENTOS

Mis más sinceros agradecimientos a todas las personas que han contribuido a la culminación de este proyecto, muy en especial a la Msc. María Paula Espinoza, Directora de Tesis, quien supo brindarme su apoyo tanto en lo académico como en lo motivacional, y sobre todo por su infinita paciencia para llevar a buen termino la presente investigación.

Bolívar Eduardo

INDICE GENERAL

CAPITULO 5

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

ANEXOS

I. PROPÓSITO DEL PROYECTO

De los estudios hechos anteriormente, se ha determinado y comprobado la importancia y ventajas que ofrece la Infraestructura de Clave Pública (PKI), y como ésta puede ser empleada como un potente mecanismo de seguridad en el intercambio de datos, transacciones y comunicaciones.

Una vez que se ha analizado y elaborado el modelo para la Universidad Técnica Particular de Loja y se ha implementado en un ambiente de pruebas, el siguiente paso es implantar el modelo PKI en un entorno de producción, definiendo los usuarios potenciales y enfocando dicha implantación hacia líneas de investigación, colaboración y de intercambio que maneje la Universidad.

La implantación de la PKI otorgará a los usuarios finales ciertos privilegios, como seguridad en las transacciones de comercio electrónico con su sitio web, o la facilidad de envío de información personal vía e-mail.

Proyectando esta visión a un futuro no distante, representaría para la Universidad ganar un total voto de confianza de parte de su recurso humano, es decir estudiantes, docentes y administrativos, en lo referente a la información que éstos manejen, así como de los organismos que mantengan convenios o vínculos con nuestra institución educativa.

II. COMPONENTES DEL PROYECTO

El presente proyecto abarca los siguientes componentes:

Una primera fase denominada Levantamiento de la información y análisis de la situación actual, en la cual se evalúa e identifica el entorno en el cual se planea poner en marcha la Infraestructura de Clave Pública (PKI).

Luego, en la Definición de los requerimientos de los usuarios finales, se trata de determinar lo que los usuarios a los cuales van dirigidos los servicios de PKI esperan de la implantación de dicha infraestructura.

Posteriormente se encuentra la fase de Instalación, Configuración y Explotación de Uso, en la cual se efectúa el proceso de implementación de la PKI en un entorno real.

La fase de Plan de Pruebas engloba aplicaciones prácticas del uso de los certificados digitales generados a usuarios de la infraestructura.

La quinta fase del proyecto es la Proyección a futuro de PKI, en ésta se analizan todas las propuestas disponibles para implementar PKI, se escoge la adecuada para llevar a cabo aplicaciones como firmas digitales y autenticación de sitios seguros en el entorno de la UTPL y así proyectar el campo de acción de la PKI en lo posterior.

Finalmente el capitulo seis denominado Discusión del Proyecto recoge las experiencias vividas a lo largo de la implementación de la PKI, y las expone a manera de recomendaciones para quien tome la posta de este proyecto.

III. ESTRATEGIA O METODOLOGIA DE DESARROLLO

- Instalación y configuración de PKI en el entorno de red real de la Universidad Técnica Particular de Loja.
- Generación de certificados y elección de los medios de usuario final adecuados.
- Difusión de la PKI de la UTPL a entidades afines, con el fin de establecer futuros proyectos conjuntos.

IV. OBJETIVOS

- Lograr que los usuarios a los cuales va orientada la PKI dentro de la Universidad puedan establecer comunicación con sus similares vía internet, cumpliendo con las características de autenticación, integración y confidencialidad.
- Garantizar la seguridad de la información que se encuentre bajo PKI, según la importancia de la misma.

CAPITULO 1

LEVANTAMIENTO DE LA INFORMACION Y ANALISIS DE LA SITUACION ACTUAL

1. LEVANTAMIENTO DE INFORMACIÓN Y ANÁLISIS DE LA SITUACIÓN ACTUAL

OBJETIVO:

Identificar y evaluar el entorno en el cual se planea poner en marcha la Infraestructura de Clave Pública (PKI).

1.1. Introducción

En proyectos desarrollados con anterioridad, como el de "Infraestructura de Clave Pública PKI y el diseño de un modelo para su implementación en la Universidad Técnica Particular de Loja" **[1]** e "Implementación de una Infraestructura de Clave Pública (PKI) para la Universidad Técnica Particular de Loja" **[2]**, se ha evaluado e identificado ya la necesidad que tiene la Universidad Técnica Particular de Loja de implementar en sus sistemas ciertos mecanismos que tengan como objeto el aseguramiento de las transacciones y procedimientos que manejan dichos sistemas.

Además, en los proyectos antes mencionados se han realizado estudios sobre la Infraestructura de Clave Pública, sus características, ventajas, desventajas y aplicabilidad en nuestra universidad. Sin embargo, no está de más hacer una breve revisión acerca de los aspectos más destacados de PKI.

1.1.1. Que es una PKI?

Una Infraestructura de Clave Pública (o ***P**ublic **K**ey **I**nfrastructure* por sus siglas en ingles) es un conjunto de aplicaciones y de servicios que nos permite utilizar la criptografía de clave pública (certificados) de una forma fácil y efectiva. **[3]**

PKI se basa en la criptografía asimétrica o de clave pública[1], ya que las propiedades de las cuales goza, la convierten en candidata ideal para prestar servicios como la *autenticación* de usuarios (para asegurarse de la identidad de un usuario, bien como signatario de documentos o para garantizar el acceso a servicios distribuidos en red, ya que sólo él puede conocer su clave privada, evitando así la suplantación), el *no repudio* (para impedir que una vez firmado un documento el signatario se retracte o niegue haberlo redactado), la *integridad* de la información (para prevenir la modificación deliberada o accidental de los datos firmados, durante su transporte, almacenamiento o manipulación), y el acuerdo de claves secretas para garantizar la *confidencialidad* de la información intercambiada. Su uso más común se plasma en la firma digital.

[1] **Criptografía asimétrica**: Es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella.

Para asegurarnos de que la clave pública de un usuario que hemos encontrado por ejemplo en un directorio o una página web, corresponde realmente a ese individuo y no ha sido falsificada por otro, y por lo tanto fiarnos de esa clave pública para confiarle algún secreto nuestro a dicho individuo, recurrimos a una tercera parte confiable, erigida en la figura de una autoridad de certificación (CA)[2].

La función básica de una CA reside en verificar la identidad de los solicitantes de certificados, crear los certificados y publicar listas de revocación cuando éstos son inutilizados. El certificado contiene de forma estructurada información acerca de la identidad de su titular, su clave pública y la CA que lo emitió.

Por lo tanto una PKI se puede utilizar para:

- **Gestión de claves**: nos permite crear, revisar o revocar claves, así como gestionar niveles de confianza.

- **Publicación de claves**: una vez creadas las claves, el PKI permite difundir nuestra clave pública, así como localizar las claves públicas de otros usuarios, junto con su estado (clave revocada, etc.)

- **Utilización de claves**: una vez recuperada una clave, PKI facilita el uso de la misma.

1.1.1.1. Necesidad de una PKI

La criptografía mediante clave pública, por sí sola, no basta si deseamos reproducir en un mundo electrónico las condiciones del comercio tradicional basado en el papel, también se requiere de:

· Políticas de seguridad para definir las reglas según las cuales deben funcionar
· Productos para generar, almacenar y gestionar las claves
· Procedimientos para establecer cómo generar, distribuir y emplear las claves y certificados

Todo esto es lo que maneja una **Infraestructura de Clave Pública (PKI)**.

La PKI proporciona el marco de acción para un amplio conjunto de componentes, aplicaciones, políticas y prácticas para combinar y obtener las cuatro funciones principales de seguridad para transacciones comerciales, las técnicas criptográficas, en diferentes combinaciones van a permitir proteger la información mediante:

· **Confidencialidad:** mantener privada la información
· **Integridad:** demostrar que la información no ha sido manipulada
· **Autentificación:** demostrar la identidad de una persona o aplicación
· **No repudio:** garantizar que no se puede rebatir la propiedad de la información **[4]**.

La falta de seguridad, a menudo, se cita como una de las mayores trabas para el crecimiento del comercio electrónico, el cual sólo puede basarse en la confianza que proced

[2] **CA:** Autoridad Certificadora, entidad encargada de receptar las solicitudes aprobadas por la Autoridad de Registro y firmarlas y generar los certificados de usuario.

de saber que todas las transacciones están protegidas por estas funciones centrales.

El rol principal de PKI es el de establecer identidades digitales en las que se pueda confiar, las cuales se pueden usar junto con mecanismos criptográficos para prestar un servicio de seguridad como autenticación, autorización o validación de una firma digital, garantizando así la confianza de los usuarios del servicio.

Una organización que emita identidades digitales de confianza (como pretende hacerlo en este proyecto la U.T.P.L.) debe tener el respaldo y la credibilidad de las personas que van a beneficiarse de sus servicios, de tal forma que éstas puedan confiar plenamente en las prestaciones que van a recibir.

En conclusión PKI brinda los componentes y servicios necesarios para desarrollar y operar un sistema que use certificados; para lo cual maneja aspectos como:

- Creación segura de buenas claves.
- Validación de identidades iniciales.
- Expedición, renovación y terminación de certificados.
- Validación y distribución de certificados.
- Almacenamiento seguro y recuperación de claves.
- Generación de firmas.
- Establecimiento y administración de relaciones de confianza.

Por último es muy importante destacar que para lograr una mayor eficiencia, PKI debe estar integrada con el sistema de seguridad interno y externo de la universidad, para realmente brindar servicios de seguridad confiables.

Dentro de PKI, un concepto importante es el relacionado a Certificados Digitales, por tanto se hace una breve descripción de los mismos a continuación.

1.1.2. Certificados Digitales

Un *certificado digital* forma una asociación entre una identidad y la pareja de claves pública/privada que posee el tenedor de la identidad. Además suministra información suficiente para que una tercera persona crea plenamente que Ud. es el poseedor correcto de la identidad.

Como muestra la fig. 1-1, la forma de un certificado digital viene dada por el estándar X.509 [3] y comprende los siguientes campos **[4]**:

- *Sujeto:* nombres y apellidos del individuo
- *Clave Pública:* corresponde a la clave privada del sujeto
- *Expedidor :* la fuente de confianza que generó y firmó el certificado
- *Número de serie :* identificación única del certificado
- *Periodo de validez :* tiempo de duración del certificado
- *Uso de certificado :* usos válidos para la pareja de claves del sujeto
- *Firma digital:* la firma digital del expedidor.

---

[3] **X.509**: El estándar que define el certificado digital.

1.1.2.1. Tipos y atributos de los certificados

Existen atributos que además de identificar al propietario del certificado como los enumerados anteriormente, están en relación con el uso que se le dé al certificado, por ejemplo, los certificados destinados al aseguramiento de correo electrónico incluirán la dirección electrónica del emisor, para comparar la identidad en el certificado con la dirección de origen de correo electrónico en el mensaje.

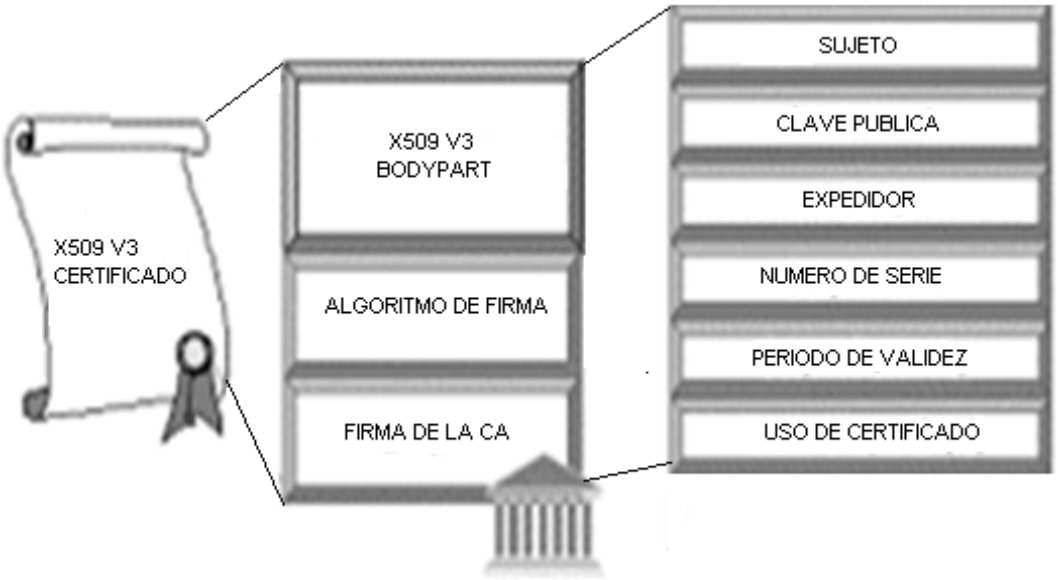


Fig. 1-1 Estructura de un certificado X.509

Para identificar a las computadoras o componentes de red como routers en un enlace de red como una VPN[4], se deberán emplear requerimientos de nombre distintos a los de una entidad humana. En estos casos la identidad suele ser las direcciones de red TCP/IP[5] que las máquinas utilizan en los paquetes de red.

Dado que los certificados son estructuras públicas que contienen información de ese carácter, incluida la clave pública que se utiliza en el proceso de validar la identidad, se pueden publicar y acceder a ellos libremente, por tal razón resulta de especial cuidado determinar el tipo de información que deben contener, de manera que no esté comprometido ningún dato confidencial del usuario del certificado.

Cabe señalar que los certificados son estructuras *autoprotegidas*, al modificarse el contenido de un certificado o detectarse que proceden de fuentes no confiables, el usuario recibirá una advertencia por parte del software de su aplicación.

1.1.2.2. Cómo trabajan los certificados

[4] Red Privada Virtual (**V**irtual **P**rivate **N**etwork)
[5] Protocolo de Capa de Transporte/Protocolo de Internet

Supongamos que un usuario U1 ha obtenido un certificado de una autoridad de certificación cualquiera y envía un documento firmado a otro usuario U2. Este usuario U2 validará la firma **[4]** como se muestra en la figura 1-2.

- U2 obtiene el certificado del U1.

- Del certificado obtenido coge la clave pública de U1 y con ella valida la firma. Como ahora el U2 tiene la clave pública de U1, U2 podrá enviar mensajes cifrados a U1.

- Para verificar que la clave pública de U1 es realmente de quien dice ser, se comprobará en la CA que dicho certificado es correcto.

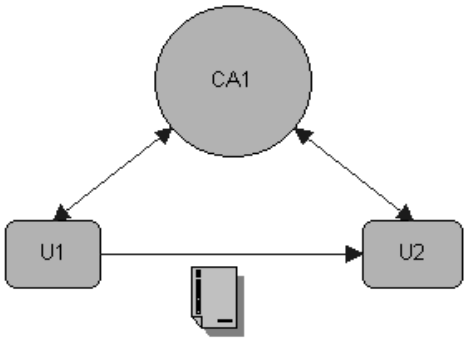


Fig. 1-2 Ciclo de trabajo de un certificado

Pero es posible que exista una jerarquía de CA, de tal forma que el proceso de validación de un certificado irá pasando desde un usuario hasta una CA tenga su certificado autofirmado. El proceso de validación en esta jerarquía de CA sería el que muestra la figura 1-3:

Fig. 1-3 Proceso de validación de un certificado en una jerarquía de CA

1.2. Aplicaciones y Requerimientos de la PKI

El presente proyecto desea poner en funcionamiento una PKI, que como vimos con anterioridad, basa su fiabilidad en la Autoridad Certificadora, la cual debe ser puesta en operación dentro del ambiente de la Universidad Técnica Particular de Loja. Esta Autoridad Certificadora se encargará de la administración de certificados digitales en dos categorías, tanto para usuarios finales como para servidores.

1.2.1. Usuarios Finales

En lo relacionado a usuarios finales, la generación de certificados estará orientada a lo que son las firmas digitales y el cifrado de datos, cuya eficacia mejora a través del uso de e-tokens. Estos dispositivos, también llamados token USB basados en tarjeta inteligente, proveen simplicidad, seguridad y facilidad de uso para soluciones PKI, generando claves de usuario y almacenándolas en el token. Sin embargo su empleo puede ser por lo pronto opcional.

Cabe por tanto, hacer una breve descripción de lo que son las firmas digitales, su uso y sus aplicaciones:

1.2.1.1. Firma Digital.

La firma digital se basa en técnicas criptográficas que permiten emular digitalmente la firma manuscrita, con la misma validez legal **[4]**.

1.2.1.1.1. Características:

- Se emplean algoritmos criptográficos asimétricos.
- Se genera a través de una clave que posee únicamente el firmante.
- Depende del documento que se firma.
- Permite asegurar la integridad y el no repudio de los documentos firmados.

Una de las aplicaciones más extendidas de la firma digital es el correo electrónico, para asegurarnos que el remitente de un correo es realmente quien aparece en el campo *from* del mensaje, es decir, para evitar que se envíen correos en nombre de otras personas.

La firma debe cumplir los siguientes requisitos:

-La firma de un usuario sólo puede ser generada por ese usuario.
-Se genera a través de la clave privada.
-Puede ser verificada por cualquiera que conozca la clave pública.
-Debe ser distinta para documento firmado
-Se debe basar en el contenido del documento.
-No se puede falsificar una firma a partir de la firma de otro documento

El fundamento de las firmas digitales es la criptografía, disciplina matemática que no sólo se encarga del cifrado de textos para lograr su confidencialidad, protegiéndolos de ojos indiscretos, sino que también proporciona mecanismos para asegurar la integridad de los datos y la identidad de los participantes en una transacción.

Todos los algoritmos se basan en un mismo método: en vez de usar una misma clave (simétrica) para encriptar y desencriptar datos (como la contraseña en un documento Word), usan dos: una privada y una pública. La primera es la que el usuario guarda; la segunda se publica en el sitio de una autoridad certificante o CA (una entidad confiable que da fe de que la clave pública pertenece a una persona o entidad).

La información encriptada con una clave, puede ser desencriptada con la otra, siendo posible:

- Desencriptar una información conociendo sólo la clave con la que se encriptó.
- Averiguar el valor de una clave conociendo la otra.

El cifrado consiste en transformar un texto plano mediante un algoritmo en un texto cifrado, gracias a una clave de cifrado, que resulta ininteligible para todos excepto para el legítimo destinatario del mismo.

Cada clave es el resultado de hacer ciertas operaciones matemáticas sobre dos números primos (divisibles sólo por sí mismos y por uno) muy grandes, de entre 512 y 2048 bits: los resultados son las dos claves. La importancia de usar números primos es que es extremadamente difícil factorizar las claves para recuperar los primos originales.

Cualquier persona que conozca la clave pública puede desencriptar, pero se asegura que solo el poseedor de la clave privada ha podido generar el documento encriptado **[4]**. Así se muestra en la figura 1-4.

Fig. 1-4 Encriptación con clave privada

Asimismo cualquier persona que conozca la clave pública puede encriptar, pero se asegura que solo el poseedor de la clave privada puede desencriptar el documento, como se muestra en la figura 1-5.

A continuación se presenta un ejemplo de comunicación entre dos usuarios, A y B**:**

- Si A desea enviar información segura a B, se envía empleando la clave pública de B, sólo B podrá descifrarla con su clave privada.

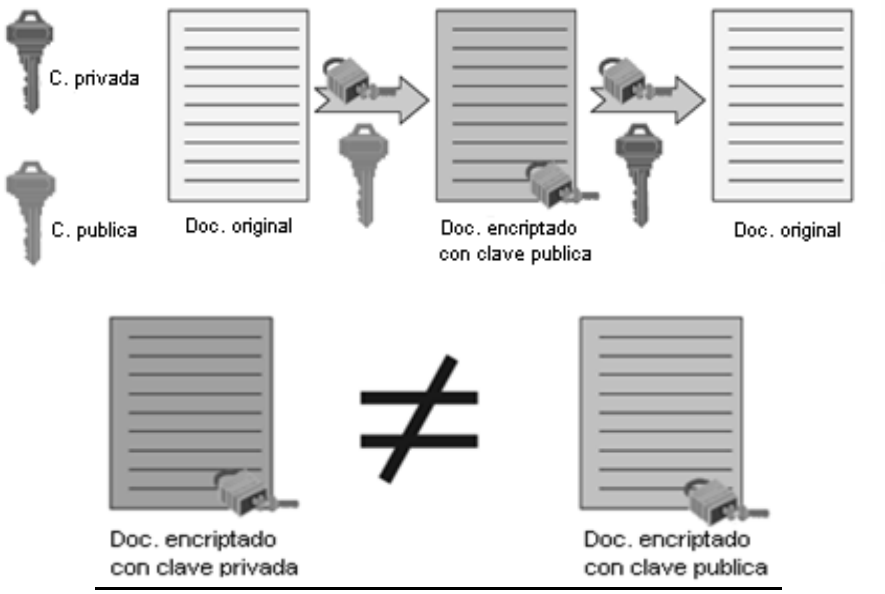


Fig. 1-5 Encriptación con clave pública

- Si A envía información encriptada con su clave privada, B podrá desencriptarla con la clave pública de A y tendrá la certeza de que sólo ha podido enviarla A.

- Las claves públicas se almacenan el lugares públicos (bases de datos, directorios LDAP...) accesibles por todas las personas que intercambien información segura.

A envía información segura a B (Figura 1-6).

Fig. 1-6 Información segura enviada de A hacia B.

Debido a que el proceso de cifrado utilizando algoritmos asimétricos es lento, lo que se agravaría en el caso de cifrar documentos extensos, es conveniente emplear las denominadas funciones hash que se describen a continuación.

1.2.1.1.2. Funciones HASH

Las funciones *hash* sirven para comprimir un texto en un bloque de longitud fija. Se utilizan en autenticación y firma digital para elaborar un resumen de un documento, con dicho resumen luego se comprueba si la clave privada del emisor es auténtica, no es necesario cifrar todo el texto si no se quiere confidencialidad. **[3]**

Además son empleados para poder comprobar automáticamente la *autenticidad*. Si se cifra todo el texto, al descifrar solo se puede comprobar la autenticidad mirando si el resultado es inteligible. Evidentemente este proceso debe realizarse de forma manual. Utilizando un resumen del texto, se puede comprobar si es auténtico comparando el resumen realizado en el receptor con el descifrado.

Por último sirven también para comprobar la *integridad* del texto, ya que si ha sido dañado durante la transmisión o en recepción no coincidirá el resumen del texto recibido con el descifrado.

Las funciones *hash* deben ser públicas e irreversibles. No cifran, solo comprimen los textos en un bloque de longitud fija. Son diferentes de las funciones clásicas de compresión de textos, como por ejemplo ZIP, Huffman o V-42, ya que estas funciones son reversibles e intentan eliminar la redundancia de los textos manteniendo el significado. Las funciones *hash* deben cumplir las siguientes condiciones:

- Transformar un texto de longitud variable en un bloque de longitud fija.
- Ser irreversibles, es decir, no se puede recuperar el texto desde el resumen.
- Conocido un mensaje y su función *hash* debe ser imposible encontrar otro mensaje con la misma función hash. Esto se debe cumplir para evitar que los criptoanalistas firmen un mensaje propio como si fueran otra persona. Es imposible inventar dos mensajes cuya función *hash* sea la misma.

1.2.1.1.3. Generación de una Firma Digital

A continuación se detallan los pasos en la generación de una firma digital:

- Paso 1: Generar el “resumen”, es decir aplicar una función hash, para lo cual se emplean algoritmos conocidos, como MD5[6] ó SHA– 1[7] **[4]**. (Figura 1-7)

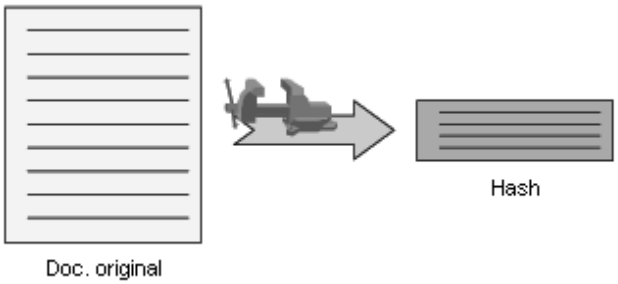


Fig. 1-7 Paso 1: Generación de un resumen.

[6] **MD5**: Es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

[7] **SHA-1**: Es un sistema de funciones hash criptográficas que produce una salida resumen de 160 bits de un mensaje que puede tener un tamaño máximo de 2^{64} bits.

- Paso 2: Cifrar el “resumen” con la clave privada. La encriptación se realiza con algoritmos asimétricos como DSA [8] o RSA [9].

Se transmite el documento original y la firma. (Figura 1-8).

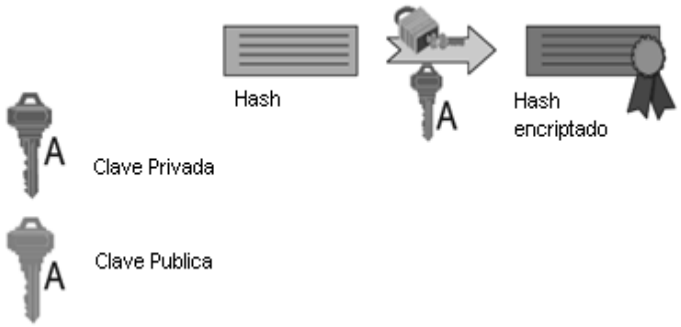


Fig. 1-8 Paso 2: Cifrado del resumen con la clave privada.

1.2.1.1.4. Comprobación de una Firma Digital

Si la comparación tiene éxito, sabemos que el documento ha sido firmado por el usuario A y que no ha sido modificado **[4]**. (Figura 1-9)

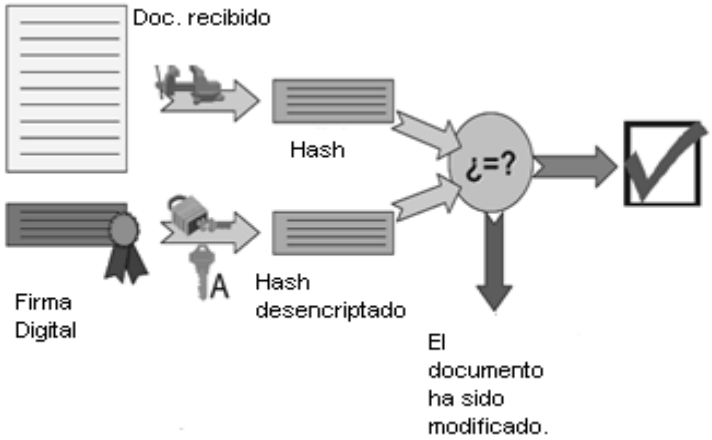


Fig. 1-9 Comprobación de una firma digital.

---

[8] **DSA**: **D**igital **S**ignature **A**lgorithm **o** Algoritmo de Firma Digital es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. este algoritmo como su nombre lo indica, sirve para firmar y no para cifrar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que RSA.

[9] **RSA**: Es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

1.2.1.1.5. Seguridades que brinda la firma digital

La firma digital proporciona un amplio abanico de servicios de seguridad:

• Autenticación: permite identificar unívocamente al signatario, al verificar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas, bien para garantizar el acceso a servicios distribuidos en red.

• Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

• Integridad: permite que sea detectada cualquier modificación por pequeña que sea de los datos firmados, proporcionando así una garantía ante alteraciones fortuitas o deliberadas durante el transporte, almacenamiento o manipulación telemática del documento o datos firmados.

• No repudio: ofrece seguridad inquebrantable de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma digital adjunta a los datos un timestamp, debido a la imposibilidad de ser falsificada, testimonia que él, y solamente él, pudo haberlo firmado.

• Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados,

• El acuerdo de claves secretas garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL.

1.2.2. Servidores

En lo referente a servidores, más adelante se hará un análisis de la situación actual de los mismos y quienes requerirían de servicios de PKI. Por lo pronto es necesario señalar que el beneficio que proporciona la aplicación de certificados digitales a los servidores tiene que ver con la autenticación de los mismos ante un usuario, de tal manera que no exista suplantación de servidores ni de la información que éstos proveen. Esto se logra por medio del protocolo SSL que a continuación revisaremos.

1.2.2.1. Nivel de Socket Seguro.

Secure Socket Layer o Nivel de Conectores Seguro, es el encargado de establecer un canal seguro del nivel de transporte entre dos partes, de tal forma que se garantiza el acceso a, por ejemplo, información segura en la web. Toda la información que fluya en la sesión utilizará codificación para garantizar su privacidad. **[4]**

SSL es un protocolo con dos capas: la de más bajo nivel se denomina *SSL Record*, la cual

encapsula los datos de protocolos de niveles más altos. La capa más alta de SSL consta de los mensajes que transporta el nivel de registro, los cuales incluyen el protocolo *Especificación de Cambio de Cifrado de Trama (Change Chiper Spec)*, el protocolo *Alarma (Alert)* y el protocolo *Toma de Contacto SSL (Handshake).*

SSL emplea PKI para autenticar a las partes durante el establecimiento de la conexión, los certificados comprueban la identidad de los involucrados, especialmente del lado del servidor, de la siguiente manera:

Al establecer una conexión con un sitio *https*[10], el servidor web envía su certificado firmado por una entidad de confianza al navegador web, para que el usuario pueda verificar que el sitio con el que quiere establecer una conexión es en efecto el propio, y que no existe alguien intentando suplantar la identidad de dicho sitio. Una vez comprobada la identidad, se procede al intercambio de información.

1.2.2.2. Redes Privadas Virtuales.

Las Redes Privadas Virtuales o VPN (*Virtual Private Networks*) permiten el uso público de internet como si fuera una red privada **[4]**. Esto se logra codificando la información que fluye entre los usuarios de la red. Pero como no están restringidos el acceso a la red ni los nodos participantes, es necesario establecer la identidad de los mismos, en este caso de las máquinas que se están comunicando.

En el caso de una VPN, la identidad que se establece es la del nodo de red y la dirección de red que está usando. De tal forma que los certificados emitidos a los nodos deben incluir la dirección de red de la entidad que se está identificando.

En conclusión, cada entidad destino debe identificarse ante las demás por medio de su certificado y verificando que el resto de entidades posean las claves correspondientes.

Las VPN's tiene distintos modos de operación, por medio de SSL e IPSec[11]. Como previamente se revisó SSL, analizaremos brevemente IPSec.

IPSec establece un conjunto de servicios de seguridad para las comunicaciones a nivel de red.

Puede operar en dos modos: modo túnel y modo de transporte.

En el primero de ellos, todo paquete de IP está cifrado y se convierte en la parte de los datos de un nuevo paquete IP más grande, al que se agregan un nuevo encabezado IP y un encabezado IPSec. El modo Túnel se usa con puertas o nodos de enlace y proxys, y los sistemas intermedios implementan los servicios IPSec.

El modo de Transporte inserta un encabezado IPSec en el paquete IP y ambos extremos de la conexión deben implantar IPSec, los sistemas intermedios no realizan ningún procesamiento de IPSec en el paquete.

[10] **Https**: Es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

[11] **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.

1.3. Análisis de la Situación actual

1.3.1. Situación actual de los servidores

Según informe presentado con fecha 21 de mayo de 2009 sobre los servidores existentes en el predio universitario[12], se pudo conocer que actualmente existen 56 servidores. De todos estos existen los servidores externos o que tienen contacto con el exterior; y los servidores internos que son empleados dentro de la red interna.

Dado el grado de criticidad de la información que manejan, es conveniente darle mayor prioridad de seguridad a los servidores externos, además de que están expuestos a mayor cantidad de ataques del exterior.

De dicho informe se extrae y presenta un listado de los servidores que reúnen estas características, debido a que algunos de estos servidores no cuentan con un sistema de autenticación de la información que les permita asegurar la misma.

Los servidores que integran dicho listado, y que están representados en el cuadro 1-10 deberían ser asegurados con certificados emitidos por una organización confiable y reconocida a nivel mundial, Mientras que el resto de servidores pueden emplear los certificados que la Autoridad Certificadora CA-UTPL genere.

1.3.2. Requerimientos hardware y software disponibles actualmente.

Para determinar si los requerimientos que conlleva la implementación de una PKI en cuanto a hardware y software están solventados en los predios universitarios, se realizó el levantamiento de la información a través del Grupo de SST (Soporte Tecnológico) de la universidad, con el ánimo de saber a ciencia cierta qué condiciones se cumplían para la puesta en marcha de una Infraestructura de Clave Pública y qué faltaba por hacer dentro del entorno universitario.

Los requerimientos planteados se relacionaron con los sistemas operativos, navegadores y clientes de correo instalados, principalmente en los laboratorios de cómputo y en las oficinas departamentales, necesarias para la emisión y soporte de certificados digitales:

1.3.2.1. Sistemas Operativos instalados:

Los Sistemas Operativos instalados principalmente en las salas de cómputo de la universidad son mostrados en el cuadro 1-11:

---

[12] Tomado de: ***Informe sobre la Capacidad Instalada a Nivel de Servidores en la UTPL al 21 de Mayo de 2009***. *RESPONSABLE: Unidad de Proyectos y Sistemas Informáticos, Soporte Técnico (Galo Picoita).*

Servidor	Servicio
GDR1.UTPL.EDU.EC	Servicio Web
ASUTPL	DEIAP; Reporting Service; Syllabus
Cajanuma	Base de Datos
DEVSERVER.OLD	Refactory
PODCASTSERVER.UTPL.EDU.EC	PodCast
Gdr2	Resolución de nombres
Repo	FTP, Repositorio
Webmail	Servicio de correo
Gdr3	Servicio de Correo
ULoja	Baan
Eva	Eva
CA	Autoridad Certificadora
NODO1SGA	Servicios Profesor; Syllabus
WSUTPL	Servicios Web en internet(Sitio profesor, estudiantes, centros
PRESENTATION SERVER	Administrador Aulas Virtuales
BDVirtual	Dspace, entorno virtual de aprendizaje

Cuadro 1-10 Servidores de servicios externos más críticos de la universidad

Sistemas Operativos instalados en las salas de cómputo de la universidad
Windows XP v2002 SP3 Windows Vista V2005 SP1 GNU/Linux (CentOS versión 5.0) MacOS versión 10.6 Windows Server 2003

Cuadro 1-11 Sistemas Operativos instalados en los predios universitarios

El mayoritario es Windows XP, pero también existen distribuciones Linux como Ubuntu, CentOS, y otros como MacOs y Windows Server 2003.

Windows XP soporta, tanto navegadores Microsoft (IE), como de código libre en el caso de Mozilla Firefox, por lo que no se reporta ningún inconveniente con los sistemas operativos instalados.

1.3.2.2. Navegadores instalados:

Navegadores instalados en las salas de cómputo
Mozilla Firefox versión 3.06 Internet Explorer versión 7.0 y 8.0 Safari versión 4.0

Cuadro 1-12 Navegadores instalados

Son los listados en el cuadro 1-12. El predeterminado es Mozilla Firefox, aunque también está el originario de Microsoft, Internet Explorer y Safari.

Los certificados emitidos por una PKI implementada con una herramienta opensource como lo es OpenCA, la cual se planea utilizar, vienen por defecto para ser instalados en navegadores desarrollados bajo código libre como Mozilla Firefox, y también para navegadores como IE, Zafari, Opera, Konkeror, por lo cual esta característica también está cubierta.

1.3.2.3. Clientes de correo instalados:

Sistema Operativo	Cliente de Correo
Microsoft	Outlook Express 6.0 Outlook 2007
GNU/Linux	Evolution v2.0
MacOS	Email

Cuadro 1-13 Clientes de correo instalados

Los principales clientes de correo instalados en la universidad son mostrados en el cuadro 1-13. Existen tanto Outlook Express, producido por Microsoft, Email para el sistema operativo MacOS y Evolution, que es propio de los sistemas operativos GNU-Linux.

Aparte de los mencionados, existe un cliente de correo multiplataforma llamado Thunderbird, el cual es fácil de instalar y manejar; y al ser opensource, se complementa muy bien con la herramienta OpenCA. Por lo tanto no se debe descartar esta alternativa, la cual como dijimos puede ser instalada sin dificultad en todos los navegadores de las computadoras de la universidad.

Las demandas en cuanto a software están satisfechas, lo que queda por hacer es delimitar el área específica de implementación de la PKI.

CAPITULO 2

DEFINICION DE LOS REQUERIMIENTOS DE LOS USUARIOS FINALES

2. DEFINICION DE LOS REQUERIMIENTOS DE LOS USUARIOS FINALES.

OBJETIVO:

Determinar lo que los usuarios que se beneficiaran de la PKI esperan de la implantación de dicha infraestructura.

2.1. Introducción

Una PKI, como lo cita el proyecto de tesis señalado en **[2]**, constituye el marco de referencia que permite desarrollar servicios de seguridad que se basan en cifrado, utilizando una clave pública y una privada; creando las entidades y la confianza necesarias para los procesos de identificación, autenticación, integridad y no repudio mediante la emisión y administración de certificados digitales.

En tal virtud, el referido proyecto de tesis realizó un estudio de las aplicaciones que se encontraban en etapa de producción y proveían los diferentes servicios de internet dentro de la universidad, determinando mediante encuestas y entrevistas a los administradores de dichas aplicaciones, aquellas que requerían servicios de seguridad basados en PKI, tomando en cuenta la importancia de los datos que manejaba cada aplicación y el nivel de seguridad con la que contaban en ese entonces.

No obstante, la generación de certificados digitales puede ser aplicada, a más del cifrado de datos y la autenticación de servidores, a la generación de firmas digitales.

Partiendo de estas premisas, debemos en primer lugar determinar los tipos de usuario que serán cubiertos por la Autoridad Certificadora de la UTPL, así como los niveles de seguridad y los algoritmos de cifrado empleados en la generación de los certificados digitales para dichos usuarios.

Por último, analizar brevemente cómo los tipos de usuario pueden solicitar un certificado digital de identificación personal a la Autoridad Certificadora de la UTPL (denominada en adelante CA-UTPL).

2.2. Tipos de usuario

Se han determinado dos tipos de usuario que podrán acceder a los servicios de certificación por parte de CA-UTPL.

El primero de ellos está en función del rol que una persona ocupe dentro del ámbito universitario, es decir, si son estudiantes, docentes, personal administrativo, autoridades o administrador de algún servidor.

Para este tipo de usuarios, los certificados digitales tendrán como aplicabilidad la utilización de firmas digitales para el envío seguro de correo electrónico por la red.

Los requerimientos son los mismos para cada uno de los roles citados anteriormente, los cuales están contemplados en el apartado 2.3.1

Sin embargo, la información que cada rol maneje tiene un grado de importancia distinto.

Por ejemplo, mientras un estudiante firme digitalmente un correo electrónico que contenga un saludo a un amigo, un docente podría emplear el proceso de firma digital para enviar un correo a Secretaría conteniendo las notas de un bimestre. O el jefe del departamento X con el presupuesto anual de su área para que sea aprobado.

Es de acuerdo a este parámetro que se emplean distintos niveles de seguridad en la generación de los certificados para cada rol, haciendo más seguros aquellos certificados destinados a roles que manejen información crítica.

Estos niveles de seguridad están determinados por tres factores:

- Nivel de fiabilidad
- El algoritmo de encriptación de clave
- El tamaño de la clave

2.2.1. Nivel de Fiabilidad:

Determina el nivel de seguridad que tendrá el proceso de generación del certificado, es decir es el tipo de autenticación física que le es otorgada al usuario para la generación de su certificado por parte de la aplicación.

Los niveles de fiabilidad disponibles son:

2.2.1.1. Low

Este nivel de seguridad es usado para certificados de tiempos de vida cortos, empleados para accesar a recursos no críticos. No es utilizada para ningún tipo de usuario.

2.2.1.2. Medium

Este nivel de seguridad será usado para certificados de estudiantes, por tener la suficiente seguridad para este tipo de usuario, sin implicar un excesivo consumo de recursos del procesador por parte de estos.

2.2.1.3. High

Este nivel es empleado para certificados de un nivel de seguridad más alto. Por lo tanto es ideal para certificados de docentes, personal administrativo y autoridades.

2.2.1.4. Very High

Este nivel de seguridad es empleado en certificados de seguridad crítica. Por ejemplo puede ser requerido para una subCA, roles administrativos de PKI (Operadores de CA y RA) y certificados para administradores de servidor.

2.2.1.5. Test

Este nivel de seguridad es empleado únicamente para pruebas y propósitos de desarrollo, por lo que tampoco tiene mayor aplicabilidad para usuarios.

Se ha establecido un cuadro en el cual se asocian los diversos roles de este grupo de usuarios con los niveles de seguridad óptimos para lograr un proceso de generación de certificado ideal.

Tipo de Usuario	Nivel de Fiabilidad
Estudiantes	Medium
Docentes	High
Autoridades	High
Administrativos	High
Administradores de servidor	Very High

Cuadro 2-1 Niveles de fiabilidad según el rol de usuario

2.2.2. Algoritmo de Encriptación de clave

Se pueden implementar tres tipos de algoritmos: RSA, DSA y ECDSA[13]**.** Una descripción detallada de dichos algoritmos se encuentra en el **anexo [2-1]**

El usuario puede seleccionar cualquiera de estos algoritmos, los cuales se combinan con los denominados *grados de seguridad* para brindar un aseguramiento ideal en la generación de petición de un certificado. Los grados de seguridad disponibles son:

Base: Soporta 3 algoritmos de encriptación de clave: RSA, DSA y ECDSA

Advanced: Soporta 2 algoritmos de encriptación de clave: RSA y ECDSA

Strong: Soporta 2 algoritmos de encriptación de clave: RSA y ECDSA

Strongest: Soporta 2 algoritmos de encriptación de clave: RSA y ECDSA

El algoritmo recomendado por ser el más reconocido y empleado es el RSA, utilizando un grado de seguridad *base,* que provee un tamaño de clave de 1024 bits.

2.2.3. Tamaño de la Clave

El tamaño de la clave es una medida de seguridad del sistema*,* se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos[14].

Como conclusión, los diferentes roles de usuario tienen niveles de fiabilidad, grados de seguridad, algoritmos de encriptación y tamaños de la clave, dependiendo de si son estudiantes, docentes, autoridades, administrativos o administradores de servidor. Las configuraciones recomendadas se encuentran en el cuadro 2-2:

---

[13] **ECDSA: E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm, modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA. Requiere números de tamaños menores para brindar la misma seguridad que DSA o RSA.

[14] Tomado de **http://es.wikipedia.org/wiki/Criptografía_asimétrica**

Usuario	Nivel de Fiabilidad	Grado de Seguridad	Algoritmo de Encriptación	Tamaño de la clave
Estudiantes	Medium	Base	RSA	1024 bits
Docentes Administrativos Autoridades	High	Base	RSA	2048 bits
Administradores de Servidor	Very High	Base	RSA	2048 bits

Cuadro 2-2 Tipos de usuario según sus grados de fiabilidad

El segundo tipo de usuario involucra a los servidores de la universidad que requieran servicios de seguridad basados en PKI, tal como lo determinó el estudio realizado en el proyecto **[2]**.

Un certificado digital emitido a un servidor de la universidad ayudará a autenticar a éste frente a los usuarios que traten de acceder a sus servicios, de manera que tengan la certeza de que se trata del mismo servidor y no de una suplantación.

Los requerimientos que deben cumplir los servidores para obtener un certificado digital se muestran en el apartado 2.3.2.

2.3. Tipos de Certificados

Existen dos tipos de certificados que corresponden a cada tipo de usuario visto anteriormente, estos son: certificados de cliente y certificados de servidor.

Los *certificados de cliente* abarcan el primer tipo de usuarios, es decir estudiantes, docentes, autoridades, administrativos de la Universidad y administradores de servidores.

Los *certificados de servidor* serán otorgados a los servidores de la universidad que lo requieran.

La diferenciación que se establece entre estos tipos de usuario tiene que ver principalmente con la funcionalidad que cada tipo de usuario dé a su certificado digital. Mientras el primer tipo de usuario lo utilice para firmar digitalmente sus e-mails, los servidores lo requerirán para autenticarse frente a un usuario que trate de acceder a sus servicios.

Luego de esta aclaración, se detalla seguidamente cada uno de los tipos de certificados.

2.3.1. Certificados de Cliente y sus requerimientos

Este tipo de certificado está destinado a estudiantes, docentes, autoridades, personal administrativo de la universidad y administradores de servidores.

Dentro del grupo de estudiantes, existen los de modalidad clásica y los de modalidad a distancia. Por ahora es recomendable tomar en consideración únicamente a los estudiantes de modalidad presencial, a fin de que sea más fácil comprobar físicamente su identidad.

Los requerimientos que los usuarios de este tipo de certificados deben cumplir para que su petición de certificado digital sea atendida, son mostrados a continuación:

Nombres del usuario

Apellidos del usuario

Fecha de Nacimiento (en el formato día/mes/año)

Identificador de Usuario, puede indicar el nombre favorito del usuario, este campo es opcional.

Además el usuario debe proporcionar otro tipo de información como:

E-mail (necesariamente el correo de la universidad del usuario)

Departamento (en caso de ser estudiante, el departamento donde presta servicios de GP)

Teléfono (convencional o celular)

Dirección (barrio o ciudadela)

Ciudad

Provincia

País

Código ZIP, el cual es un número escogido aleatoriamente por el usuario, que debe tener como mínimo 5 dígitos y que sirve como identificador del usuario.

Un tercer grupo de requerimientos a cumplir por parte del usuario consta de:

Nombre de Usuario (los nombres y apellidos llenados anteriormente ahora concatenados.)

Grupo de Petición de Certificado. Aquí es donde el usuario (excepto los administradores de servidor) debe establecer a que categoría de las consideradas anteriormente pertenece (es decir estudiante, docente, autoridad o administrativo).

Para diferenciar entre los usuarios ubicados dentro del grupo de petición de certificado (citado anteriormente) y los administradores de servidor, se requiere de otro nivel de seguridad denominado tipo de certificado:

Tipo de Certificado. Los estudiantes, docentes, autoridades y administrativos obligatoriamente deben seleccionar ***User***, los otros campos son utilizados para certificados de administradores de servidor.

Seleccionar Autoridad de Registro *(RA)*, por defecto se presenta RA-UTPL (así se conocerá en adelante a la Autoridad de Registro de la UTPL.)

Nivel de Fiabilidad: Son los niveles Low, Medium, High, Very High y Test que se analizaron anteriormente.

Modo de Generación de Clave, es decir el método por el cual se ponen a consideración los algoritmos de clave asimétrica a ser empleados, este modo de generación muestra dos posibilidades:

- Browser
- Server

En el modo *browser* es el navegador empleado para realizar la petición el encargado de la generación de la clave. Al emplear este método, el algoritmo de generación de clave por defecto es RSA, con un tamaño estándar de clave de 1024 bytes.

En cambio en el modo *server*, el servidor de la aplicación se encarga de dicha generación. Brinda al usuario la posibilidad de seleccionar entre tres tipos de algoritmos con distintos tamaños de clave para cada uno. Por tal motivo, este modo de generación es el más recomendable.

Algoritmos de Encriptación y Tamaños de Clave soportados

El modo server soporta los algoritmos RSA, DSA y ECDSA con sus correspondientes tamaños de clave los cuales se mostraron en el cuadro 2.2.

2.3.2. Certificados de Servidor y sus requerimientos

Estos certificados estarán destinados para la autenticación de los servidores críticos de la universidad.

Para obtener un certificado de servidor, el administrador de dicho servidor debe completar algunos datos requeridos por la aplicación para determinar la autenticidad del servidor que administra. Estos datos serán posteriormente revisados por el administrador de la Autoridad de Registro para constatar su validez. Aquí se muestran dichos requerimientos:

Request (en formato PEM): El administrador, para obtener un certificado para su servidor, debe primeramente generar una petición en formato PEM PKCS#10[15] con toda la información concerniente a dicho servidor. Una forma de hacerlo es mostrada en el **anexo [2-2]**.

Una vez generado el requerimiento de petición en formato PEM PKCS#10, es anexado al resto de requerimientos de petición.

Registration Authority: Es el nombre de la Autoridad de Registro, por defecto es RA-UTPL.

[15] **PKCS#10:** Estándar de solicitud de certificación. Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública.

Role: Presenta los diferentes tipos de rol que puede tener el servidor, por ejemplo Web Server, CA Administrator, RA Operator, web mail.

Level of Assurance: Al igual que para los certificados de usuario, los niveles pueden ser *Low, Medium, High y Very High*. Para los servidores, los niveles recomendados son *high* o *very high*, la decisión queda a voluntad del administrador del servidor. (Cuadro 2-3)

Tipo de usuario	Nivel de Fiabilidad	Grado de Seguridad	Algoritmo de Encriptación	Tamaño de Clave
Servidor	High	Base	DSA ECDSA RSA	2048 bits 256 bits 2048 bits
		Advanced	ECDSA RSA	384 bits 4096 bits
		Strong	ECDSA RSA	521 bits 8192 bits
	Very High	Base	ECDSA RSA	256 bits 2048 bits
		Advanced	ECDSA RSA	384 bits 4096 bits
		Strongest	ECDSA RSA	521 bits 8192 bits

Cuadro 2-3 Niveles de Fiabilidad según el tipo de servidor

PIN: O clave de seguridad que es suministrada por el administrador del servidor. Debe ser una clave segura, difícil de descifrar pero fácil de recordar para el administrador.

Repetir el PIN: La misma clave anterior para confirmación.

Cédula: El numero de cedula del administrador del servidor.

Nombre: El dominio del servidor o algún nombre que identifique al servidor.

E-mail: La dirección de correo del administrador del servidor (el correo de la UTPL).

Departamento: El área en la cual está ubicado el servidor o en la cual presta servicios.

Teléfono: Convencional o móvil del departamento en donde está ubicado el servidor, o del administrador.

Posterior a esto, la petición de certificación esta completada, a la espera de su revisión, aprobación y posterior generación del certificado, procesos que son manejados por administradores de los servidores CA y RA de la misma forma que para los usuarios de los certificados de cliente.

CAPITULO 3

INSTALACION, CONFIGURACION Y EXPLOTACION DE USO

3. INSTALACION, CONFIGURACION Y EXPLOTACION DE USO EN BASE A DICHOS REQUERIMIENTOS.

OBJETIVO:

Realizar el proceso de implementación de la PKI en un entorno real.

3.1. Introducción

Previo a poner en marcha todo lo referente a la configuración de la Infraestructura de Clave Publica, es necesario recordar cuál es el software que nos ayudara en la implementación propiamente dicha.

La herramienta se denomina ***OpenCA,*** misma que fue evaluada y sugerida por el proyecto **[2]** luego de que en el mismo se efectuase una comparación entre alternativas open source (OpenCA, pki-Iris, EJBCA) y software propietario (Verisign, Identity Guard Entrust, Windows Server 2008 PKI), inclinándose hacia la propuesta open source según las conclusiones de sus autoras, citadas textualmente a continuación:

"Sin embargo, se puede observar que las soluciones Open Source ofrecen muchas ventajas con relación al Software Propietario principalmente por el costo y el control total sobre el código abierto, a demás, la Universidad promueve Open Source a toda su comunidad universitaria, aplicando en su mayoría, herramientas libres en servidores y ahora en demás estaciones de trabajo, razón por la cual se decide utilizarla como herramienta de solución para la implementación de la Infraestructura de Clave Pública." [16]

Dentro de las nombradas herramientas open source, también se efectuó un proceso comparativo entre ellas, en base a aspectos también considerados por las autoras y detallados a continuación:

- Soporte Técnico y humano.
- Confiabilidad del software en la administración.
- Plataforma que soporta.
- Requerimientos adicionales.
- Documentación disponible.

Finalmente concluyeron que OpenCA constituía la mejor alternativa, de acuerdo a sus propias palabras, nuevamente citadas:

"OpenCA, es la herramienta que más se adapta a las necesidades de las aplicaciones instaladas en la Universidad, el soporte se basa en la ayuda de los desarrolladores y demás personas con experiencia con ésta herramienta mediante Foros y Chat de ayuda. También, la amigabilidad con las herramientas adicionales para la instalación de la herramienta como es OpenSSL, OpenLDAP, MySQL, etc." [17]

---

[16] Fase 3, Apartado 3.2.3: *Evaluación y selección de la Herramienta software*, página 24

[17] Fase 3, Apartado 3.2.5: Análisis estadístico y elección de la herramienta PKI Open Source, página 27

El presente proyecto, como continuación lógica del referido en **[2]**, tomó en cuenta esta conclusión debidamente evaluada y comprobada, y por ende se decidió utilizar la herramienta OpenCA para la implementación de la PKI en la UTPL.

3.1.1. Características de OpenCA

OpenCA es una aplicación open-source que proporciona un interface Web basada en Perl para poder administrar una Infraestructura de Clave Pública (PKI), operaciones criptográficas basadas en ***openssl***[18] y una base de datos. **[5]**

Además soporta los siguientes elementos:

- Módulo para la parte pública de la CA con su respectiva Interfaz Pública
- Módulo para administrar la Autoridad de Registro con su Interfaz RA
- Módulo para administrar la Autoridad de Certificación con su Interfaz CA
- Módulo adicional para administrar el repositorio de certificados con su Interfaz LDAP
- Contraseña basada en login y password
- Certificados basados en login (incluyendo smartcards)
- Roles basados en control de accesos.
- PIN basado en revocación
- Firmas Digitales basadas en revocación
- Emisión de CRL.
- Soporta (Internet Explorer, Mozilla, Konkeror, Opera,

La versión de OpenCA con la que se trabajó anteriormente fue la **0.9.3,** mientras que la versión más actual de la herramienta, y que se implementará, es la **1.0.2** que si bien es cierto cubre algunos bugs que tenia la versión anterior, trae nuevas opciones que no están cubiertas en el manual de configuración del software.

Una vez familiarizados con las opciones que dicha herramienta provee, se debe realizar la configuración de acuerdo a las necesidades de la universidad.

3.2. Ubicación de los servidores dentro de la Red de la universidad

Para llevar a efecto la implementación de la PKI, se nos proporcionó dos servidores. El primero de ellos destinado para almacenar la Autoridad Certificadora (CA) y el segundo albergará la Autoridad de Registro (RA) y la interfaz pública (PUB).[19]

El servidor de la CA tiene instalado el Sistema Operativo Debian [20] Etch 8.04, mientras que el servido de la RA y de la interfaz pública PUB, posee como Sistema Operativo Ubuntu [21] 8.04. Aunque los servidores no tienen un sistema operativo común, tanto Debian como

---

[18] **OpenSSL:** Security Socket Layer, estándar abierto utilizado en criptografía.

[19] **PUB**: Interfaz a la cual pueden accesar los usuarios que requieran un certificado digital.

[20] **Debian:** Sistema operativo GNU basado en software libre precompilado y empaquetado.

[21] **Ubuntu**: Es una distribución de GNU/Linux orientada a escritorio, basada en Debian.

Ubuntu mantienen una gran compatibilidad, tanto así que el segundo es un derivado del primero.

Un esquema de la interacción de los dos servidores es mostrado en la figura 3-1. En el mismo se puede observar que OpenCA posee tres funciones diferentes, las cuales pueden ser instaladas en un solo servidor, en servidores independientes o agrupadas.

Esta última opción ha sido adoptada en la implementación de la PKI de la universidad, de tal forma que el servidor de CA aloja la función de CA; y el servidor de RA tiene las funciones de RA y Pub. Cada una de estas funciones constituye los que se denominan *nodos.*

A continuación se describen estos nodos que conforman OpenCA:

- **Nodo CA:** Es el nivel más alto y el que requiere mayor seguridad en el sistema. Existe solo una CA por cada certificado CA raíz que pueda generarse (aunque varias CA's pueden ser encadenadas en una jerarquía). El acceso a esta máquina debe ser restringido únicamente para el operador de la CA. Almacena la clave privada de la CA, empleada para firmar los certificados que han sido aprobados.

- **Nodo RA:** Aquí es donde los requerimientos son aprobados por el/los operador(es). Luego estos requerimientos son transferidos al servidor de CA para su firma. A este nodo solo pueden conectarse los operadores de RA y de ser necesario, el operador de CA. Pueden existir muchas Autoridades de Registro por cada Autoridad Certificadora.

- **Nodo de Interfaz Pública (PUB)**: Es una interfaz web que permite a los usuarios hacer sus solicitudes de petición de certificados, y pone a disposición los certificados ya firmados, así como el certificado de la CA **[6]**.

La información entre los nodos CA y RA (certificados aprobados y firmados) se logra a través de los *nodos de intercambio*.

Una vez asignados los servidores, se realizó el direccionamiento de los mismos, a fin de ubicarlos dentro de la zona de mayor seguridad dentro de la red universitaria. Especial cuidado requiere el servidor CA o de la Autoridad Certificadora, mismo que contiene la clave privada de esta, y de cuya seguridad depende toda la infraestructura implementada. Por tal razón se lo ubicó dentro de la zona de los servidores críticos (la de mayor seguridad), mientras que el servidor de RA y de la Interfaz Pública se encuentra dentro de los servidores monocríticos. Estos dos grupos de servidores están protegidos por el switch de Core[22]

También se muestra el esquema de red de la universidad, y la ubicación de los servidores de PKI dentro de la misma (figura 3-2).

[22] **Switch de Core:** O interruptor de Red Troncal, es un switch posicionado en el núcleo físico o espina dorsal (*blackbone*) de una red de alta capacidad.

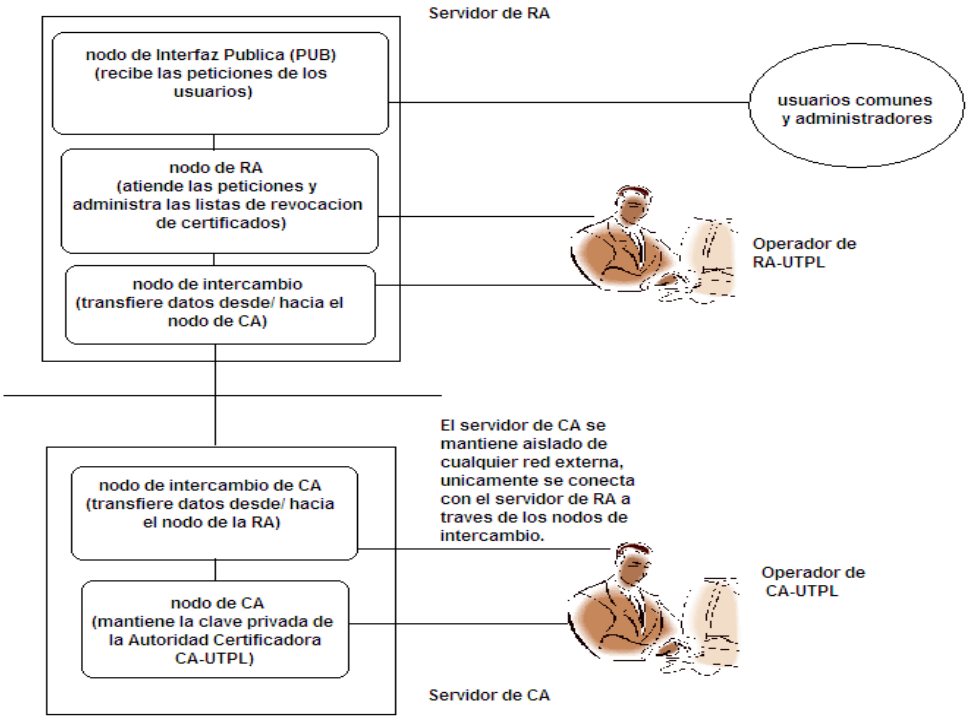


Fig 3-1. Interacción entre los servidores de OpenCA

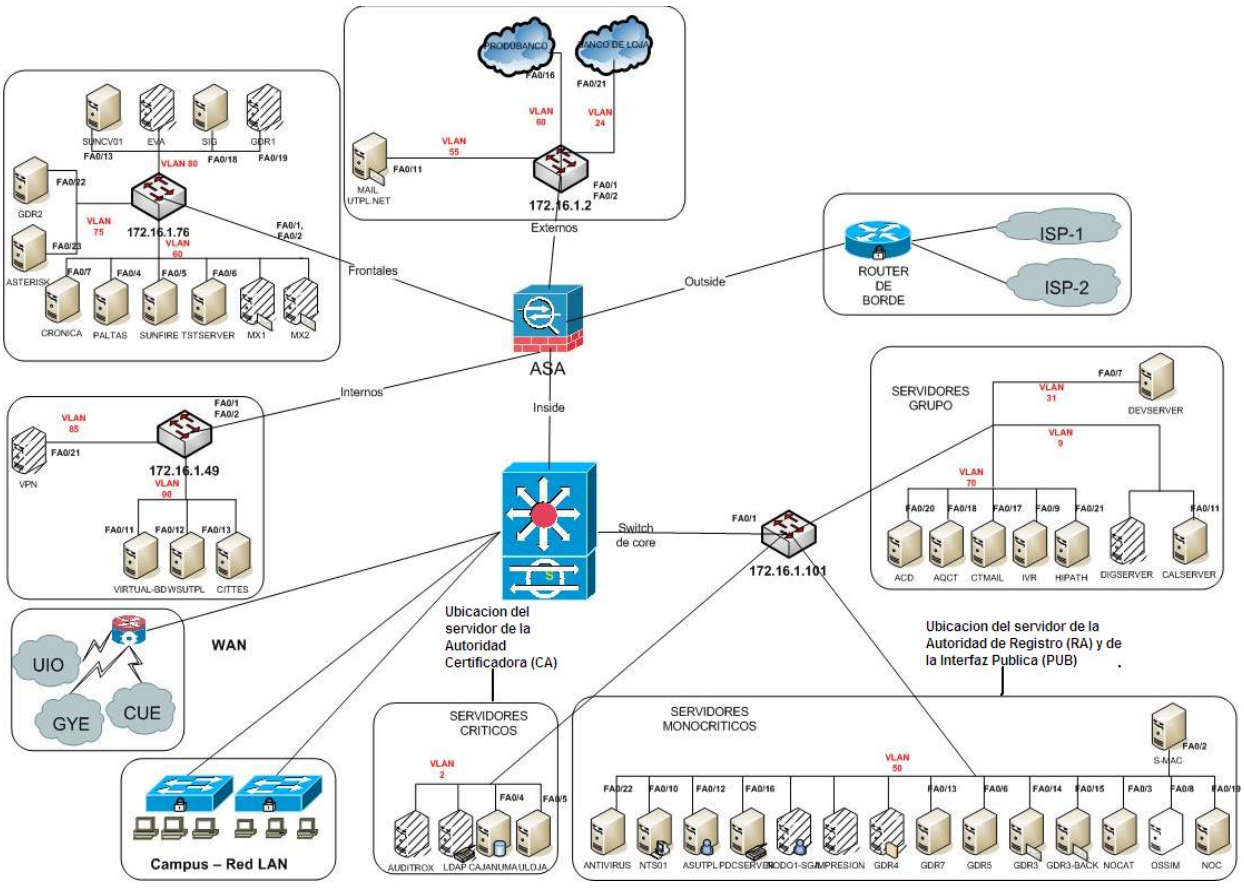


Fig. 3-2. Ubicación de los servidores dentro de la red universitaria

El direccionamiento para los servidores, así como otros detalles referentes a los mismos, se encuentran detallados en el **anexo [3-13]** (manual del administrador).

De ahora en adelante, cuando aparezca el nombre CA, se hará referencia al servidor de la Autoridad Certificadora, mientras que RA indicará el servidor de la Autoridad de Registro o la Interfaz Pública.

Se cuenta además con reglas de control de acceso, de tal forma que el servidor CA no tenga contacto con ninguna red externa, únicamente con el servidor de la RA, para el intercambio de información.

Para el correcto funcionamiento de la herramienta OpenCA, se deben cumplir con ciertos requerimientos previos a su instalación, mismos que están descritos en el cuadro 3-3.

Aplicaciones	Software	Versión
Sistema Operativo	Debian Ubuntu	8 8.04
Base de Datos	MySQL	5.0.45-7.el5
Servidor Web	Apache OpenSSL OpenLDAP	2.2.6 0.9.8b 2.3.27
Módulos Perl	Perl	5.8.8-15.el5

Cuadro 3-3. Requerimientos previos a la instalación de OpenCA.

Adicionalmente se requieren varios módulos Perl [23] que son mostrados en el **anexo [3-1]**

Con todos estos antecedentes a continuación se detalla los pasos a seguir para la configuración de OpenCA, que pondrá en marcha la Infraestructura de Clave Publica:

3.3. Instalación y configuración de OpenCA

Los pasos para la instalación de OpenCA se encuentran detallados en el manual del administrador, en el **anexo [3-13]**.

La configuración de los archivos principales de la herramienta OpenCA está detallada en el manual de administrador (**anexo [3-13]**). Ahora se muestran los directorios principales que componen la herramienta, tanto en el servidor RA como en el de CA.

[23] **Perl**: Lenguaje de Programación, toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

3.3.1. Componentes del servidor RA.

Dentro del directorio instalado (`/usr/local/`), existen dos directorios muy importantes para el funcionamiento de OpenCA. Estos son: `/var y /etc`.

Dentro del primer directorio, se encuentran subdirectorios y archivos variables de OpenCA, además de archivos temporales, archivos de logs, claves públicas de la Autoridad Certificadora y correos generados para los usuarios.

En cambio en el directorio `/etc`, se ubican subdirectorios y archivos de configuración de la herramienta, (base de datos, control de acceso, etc.).

Los subdirectorios más importantes dentro del directorio `/etc` son:

- **`Access_Control.`**– Este subdirectorio se encarga de regular el acceso a las dos interfaces que forman el servidor de la RA, (ra y node) es decir, generar los mecanismos necesarios para autenticar a los administradores/operadores de estas interfaces. Este acceso lo consigue por medio de ciertos archivos de configuración, node.xml.template y `ra.xml.template`. La interfaz `pub`, al ser de acceso público, no tiene necesidad de autenticar a sus visitantes.

Los aspectos más importantes de la configuración de dichos archivos se encuentran en el **anexo [3-4]**.

- **`Agreements.`**– Contiene los archivos que contienen los acuerdos de certificación entre el usuario y la organización certificadora (CA-UTPL). **anexo [3-5]**

- **`Menús.`**– Aquí se modifica la presentación de las diferentes interfaces.

- **`Servers.`**– Esta formado por archivos que contienen información del intercambio de datos entre los nodos *online* y *offline*. Su configuración se aprecia en el **anexo [3-6]**.

En cuanto a los archivos de configuración, los más importantes son:

- **`Config.xml.`**- Es el archivo principal, de cuya configuración depende el funcionamiento correcto de la herramienta OpenCA.

Los aspectos más destacados de su configuración se destacan en el **anexo [3-7]**.

- **`Browser_req.xml.`**- Contiene la configuración de la solicitud de petición de usuario, por lo que hay que modificarla de acuerdo a nuestras expectativas. **anexo [3-8]**

- **`Loa.xml.`**- Mantiene información sobre los niveles de seguridad empleados en el requerimiento de firmas de certificados (CSR), detallados en la fase dos de este proyecto. (**anexo [3-9]**)

- **`Server_req.xml.-`** Contiene la configuración de la solicitud de petición de servidor. (**anexo [3-10]**)

3.3.2. Componentes del servidor CA

La interfaz CA contiene prácticamente los mismos archivos y subdirectorios existentes en el servidor de RA, excepto en lo referente a la interfaz ***pub***. Sin embargo la configuración de los archivos varia un poco, en especial las secciones de control de acceso ubicada en el directorio `/usr/local/etc/openca/access_control` y de intercambio de datos (nodo), misma que esta contenida en el directorio `/usr/local/etc/openca/servers`

Toda la configuración de `/usr/local/etc/openca/access_control` se muestra en el **anexo [3-11].**

Toda la configuración de `/usr/local/etc/openca/servers` se muestra en el **anexo [3-12].**

3.4. Procesos de Certificación

En el cuadro 3-4 se explica el proceso de interacción entre un usuario y los administradores de CA y RA que tiene por finalidad la generación de un certificado de firma digital.

Este proceso además esta descrito de forma detallada en el manual de procedimientos **[anexo 3-15]**

El intercambio de los datos (tanto las solicitudes de certificación aprobadas que se envían de la RA hacia la CA, como los certificados generados de la CA hacia la RA para su publicación en el sitio web de la Autoridad Certificadora) son administrados por los *nodos de intercambio*.

Tanto el servidor de la CA como el de la RA cuentan con un nodo de intercambio, dichos nodos deben ser configurados de forma tal que permitan la correcta sincronización del flujo de información entre los dos servidores.

3.4.1. Solicitud de Certificado para usuarios de certificados de cliente

Los entes que conforman la comunidad universitaria, ya sean estudiantes, docentes, personal administrativo, autoridades o administradores de servidores, tienen derecho a hacer la petición para obtener su certificado digital de identificación personal; obviamente deberán para ello demostrar sus roles como tal y pertenecer actualmente a la actividad universitaria.

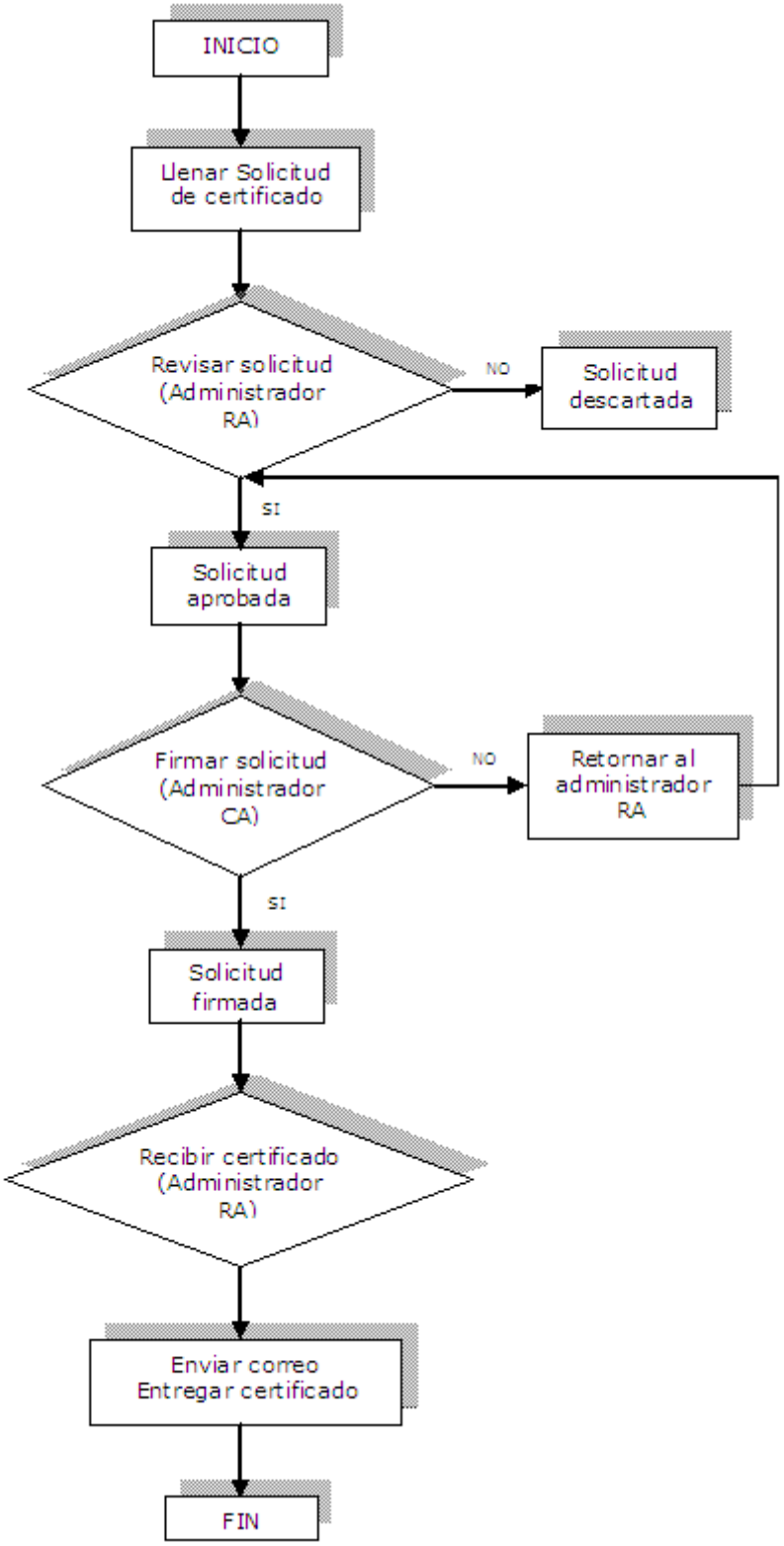


Fig. 3-4 Proceso de certificación de CA-UTPL

3.4.2. Aprobación de la Solicitud de Certificado

Luego de que el usuario ha generado su petición de firma de certificado (CSR), y se ha identificado ante el administrador de la RA, deberá esperar a que se apruebe su petición y se genere el correspondiente certificado digital de identificación.

Una vez notificado de la asignación de su certificado, al solicitante se lo considera acreedor de un certificado digital de Identidad como miembro de la UTPL, cuyo periodo de validez es de dos años. El usuario deberá descargarlo y de ahora en adelante se responsabiliza de mantener su clave privada protegida, ya sea en algún lugar seguro de su computador o de preferencia en un token criptográfico **[anexo 3-15].**

3.4.3. Solicitud de Certificados Digitales para servidores

La petición de un certificado digital de identificación para un servidor de la universidad la formulará el administrador de dicho servidor, luego de comprobar tal condición ante el administrador de la RA.

El procedimiento a llevarse a cabo entre estas dos partes esta contemplado en el **[anexo 3-15]**

3.5. Revocaciones

3.5.1. Causas de revocación

Un certificado podrá ser revocado si:

Ha existido pérdida, robo, modificación, divulgación no autorizada, u otro compromiso de la clave privada del sujeto del certificado.

Por caso fortuito, cuando la información de otra persona se ve materialmente amenazada o comprometida.

Si la UTPL conoce o tiene motivos para creer razonablemente que uno de los hechos representados en el certificado es falso o cambiado.

Si la UTPL conoce que alguno de los requisitos de emisión del certificado no fue cumplido.

Si el sistema de certificación se ve comprometido de modo tal que afectara la fiabilidad del certificado.

3.5.2. Revocación a petición del solicitante de certificado

La manera en que un usuario solicita la revocación de su certificado esta sintetizada en la figura 3-5.

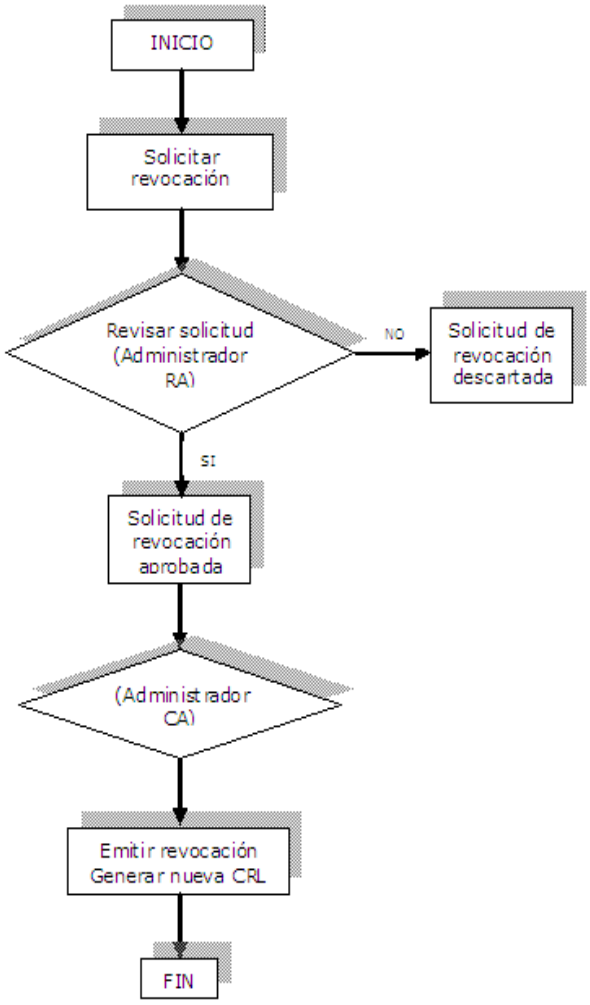


Fig. 3-5. Petición de revocación por parte de un usuario

La UTPL, en la persona del administrador de la Autoridad de Registro deberá revocar un certificado a petición del suscriptor de un certificado, ya sea un usuario o un administrador de servidor, una vez que haya comprobado que la persona que realiza la solicitud de revocación es en efecto el suscriptor, y que este haya justificado debidamente el motivo de la revocación, quedando registrada la causa. La identificación de las personas se hará a través de la credencial o con su cédula de identidad.

El procedimiento empleado por usuario y administrador de la RA se muestra en el **[anexo 3-15]**

3.5.3. Revocación por error en la emisión

CA-UTPL revocará un certificado si descubre y confirma que no fue emitido de acuerdo con los procedimientos establecidos en este documento. El administrador de la RA-UTPL que intervino en el procedimiento de emisión podrá igualmente solicitar la revocación en este caso.

3.5.4. Revocación del Certificado de CA-UTPL

El único caso de revocación del certificado de la CA-UTPL, será cuando la clave privada se vea comprometida, se procederá de la siguiente manera:

A partir de ese momento, se considerarán inválidos todos los certificados firmados por la CA-UTPL, procediendo a la generación de un nuevo certificado para CA-UTPL.

Seguidamente, la UTPL generará todos los certificados para los miembros de su comunidad universitaria, firmados con la nueva clave privada de CA-UTPL: certificados de identidad personal para usuarios comunes y certificados digitales para administradores de servidores.

3.5.5. Revocación de Certificado de la Autoridad de Registro

La revocación del certificado de la Autoridad de Registro RA-UTPL firmado por la CA-UTPL de la Universidad, se hará bajo el protocolo descrito a continuación:

El administrador de la RA-UTPL notificará, con la mayor brevedad posible, al administrador de la CA-UTPL la necesidad de revocación de su certificado, presentándose físicamente ante él e identificándose de la manera anteriormente descrita.

Comprobada la identidad del solicitante, el administrador de la CA-UTPL procederá a revocar el certificado del administrador de la RA inmediatamente.

A partir de este momento, se consideran inválidas todas las solicitudes de certificados llegadas a la Autoridad de Certificación de la UTPL, previa identificación por la Autoridad de Registro revocada, desde el momento en que se comprometió o alteró la clave privada, procediendo a la revocación de los certificados de Identidad Personal firmados desde ese instante y procedentes de dicha Autoridad de Registro.

3.6. Expiración de los Certificados

El grupo de seguridad de la UTPL notificará a sus usuarios, por correo electrónico, la próxima expiración de sus certificados. Tal aviso tiene como finalidad única, comunicar al suscriptor la necesidad de renovar su certificado.

CAPÍTULO 4

PLAN DE PRUEBAS

4. PLAN DE PRUEBAS

OBJETIVO

Realizar aplicaciones prácticas del uso de los certificados digitales.

4.1. Introducción

Una vez que se han analizado los procesos de petición, aprobación y generación de certificados, y se han obtenido los mismos por parte de un usuario, es preciso aplicar estos certificados en procesos como el firmado y cifrado de correos electrónicos.

Para que un certificado emitido por la Autoridad Certificadora de la UTPL (CA-UTPL) sea efectivo, es necesario que en el navegador en el cual se efectuó la solicitud de petición de certificado se encuentre instalado el certificado raíz de CA-UTPL, mismo que valida todos los certificados generados por la Autoridad Certificadora de la Universidad.

4.2. Pruebas

4.2.1. Instalación del certificado raíz de CA-UTPL

Este paso es de gran importancia en todo el proceso subsiguiente, puesto que sin la presencia del certificado de la Autoridad Certificadora CA-UTPL (también llamado certificado raíz) en el navegador que se emplee, cualquier certificado de usuario emitido por dicha Autoridad Certificadora será inútil y no podrá ser reconocido por dicho navegador.

La herramienta proporciona algunas maneras de obtener el certificado digital de la Autoridad Certificadora de la UTPL, de acuerdo al navegador que se esté utilizando. Para ello presenta algunos formatos que contienen el certificado:

- CRT (Certificado de seguridad)
- PEM (Certificado cifrado)
- DER (Certificado de seguridad)
- CER (Certificado de seguridad)
- TXT (Certificado de seguridad)

Los navegadores pueden importar el certificado de CA-UTPL en los formatos CRT, DER y CER, lo que varía es la forma de instalarlos. Mientras que PEM muestra la clave pública del certificado de CA-UTPL y TXT es un archivo en modo texto que contiene información acerca de la Autoridad Certificadora de la Universidad. Una descripción de acuerdo al tipo de navegador es mostrada en el cuadro 4-1.

La manera de importar el certificado raíz de CA-UTPL en cada navegador es descrito en el **anexo [4-1].**

	Internet Explorer (versión 6 y 7)	Mozilla Firefox (versión 1.5 y +)	Opera (versión 9.6)
CRT	Se descarga como un archivo para ser importado posteriormente	Se instala en el mismo instante	Se instala en el mismo instante
PEM	Solamente para Información	Solamente para información	Solamente para información
DER	Se descarga como un archivo para ser importado posteriormente	Se descarga como un archivo para ser importado posteriormente	Se descarga como un archivo para ser importado posteriormente
CER	Se descarga como un archivo para ser importado posteriormente	Se descarga como un archivo para ser importado posteriormente	Se descarga como un archivo para ser importado posteriormente
TXT	Solamente para información	Solamente para Información	Solamente para información

Cuadro 4-1. Tipos de formato de certificado raíz soportados por distintos navegadores

4.2.2. Solicitud de certificado de usuario

Luego de haber instalado el certificado de la autoridad raíz CA-UTPL, se procede a realizar la solicitud del certificado.

Se realizaron pruebas a cinco usuarios potenciales que solicitaron su certificado digital. Tres de ellos son estudiantes y dos son empleados. Uno de los empleados es el administrador de los servidores de CA y RA.

Se solicito además a los usuarios que hicieran algunas observaciones acerca de la experiencia que tuvieron al momento de realizar la petición de certificado

4.2.2.1. Resultados

Los resultados de las pruebas de petición de certificado de los usuarios antes indicados se muestran en el cuadro 4-2.

Las observaciones que dichos usuarios formularon están citadas a continuación:

- El hecho de que se pueda acceder a la interfaz únicamente por medio del proxy de la universidad fue un inconveniente para tres de los cinco usuarios.

- Falta en el diseño de la página algún enlace adicional que muestre con mayor detalle lo que el usuario debe realizar como primer paso al momento de formular la petición.

- El tamaño de la clave de seguridad o clave privada, que es como mínimo de nueve caracteres es excesivo, debería ser mínimo de seis caracteres.

Usuario	Navegador	Sistema Operativo empleado	Petición exitosa	Grado de dificultad	B= Bajo M= Medio A= Alto
Usuario 1 (estudiante)	Mozilla Firefox (versión 3.0)	Windows XP	SI	A	
Usuario 2 (estudiante)	Internet Explorer (versión 7)	Windows XP	SI	B	
Usuario 3 (estudiante)	Opera 9.64	Windows XP	SI	M	
Usuario 4 (empleado)	Internet Explorer (versión 6)	Windows XP	SI	M	
Usuario 5 (empleado administrador)	Mozilla Firefox (versión 1.5)	CentOS 5.0	SI	M	

Cuadro 4-2. Pruebas de solicitud de certificado aplicadas sobre distintos usuarios

- Los tiempos de respuesta por parte de la aplicación fueron algo lentos, en especial al emplear el navegador Opera.
- No saber elegir el algoritmo de cifrado adecuado (entre RSA, DSA o ECDSA), ni el tamaño de clave idóneo para la elaboración de las claves.

Estas observaciones obviamente deben ser tomadas en cuenta para el mejoramiento de la interfaz web de CA-UTPL.

4.2.3. Solicitud de certificado de servidor

Se efectuaron pruebas sobre un servidor de la UTPL, precisamente el servidor que alberga la Autoridad de Registro y la Interfaz Publica dentro de la PKI, cuyo nombre de host es ***repo.utpl.edu.ec***.

Para solicitar el certificado para este servidor (y para cualquier otro), es necesario primeramente que el administrador de dicho servidor adjunte una petición de certificación en formato PKCS#10 previamente elaborada, y cuyo nombre de servidor sea el dominio que tiene dentro de la red universitaria. La manera de formularla se encuentra descrita en el **[anexo 2]**.

4.2.3.1. Resultados

Los datos de la prueba de petición de certificado para el servidor web de CA-UTPL se muestran en el cuadro 4-3.

Usuario	**Dominio servidor**	**Navegador empleado**	**Sistema Operativo**	**Método de generación de petición de certificado**	**Éxito en la petición**	S= Si N= No
Usuario 6 (servidor RA)	repo.utpl.edu.ec	Mozilla Firefox 1.5	Debian Etch	openssl	S	

Cuadro 4-3 Prueba de petición de certificado realizada para el servidor web de CA-UTPL

Existen también algunas sugerencias que cabe destacarlas a continuación:

- No se efectuaron pruebas con el método de generación de petición de Windows (Microsoft **I**nternet **I**nformation **S**ervice o IIS), únicamente desde GNU/Linux mediante el empleo de **openssl**.

- La generación de la petición en formato PKCS#10 puede presentar dificultad para quien no está familiarizado con openssl.

4.2.4. Aprobación de solicitud del certificado

Las operaciones que el administrador de la Autoridad de Registro puede aplicar sobre una petición de certificado que llegue a su poder son:

- *Editar Peticiones*: Mediante esta función, el administrador debe ingresar las fechas de expedición y de caducidad del certificado, las cuales no deben exceder el tiempo de vida del certificado de la Autoridad Certificadora CA-UTPL, el cual es de 730 días (dos años). También se pueden revisar algunos datos que el usuario haya escrito mal o haya omitido.

- *Verificar PIN*: Aquí el administrador puede verificar que la clave de seguridad que el usuario ha ingresado al momento de solicitar su certificado concuerda con la que éste le ha proporcionado (en papel) al momento de verificar su identidad.

- *Aprobar la Petición*: Aquí el administrador propiamente aprueba la solicitud de petición del certificado. Esta opción significa que el administrador de la RA-UTPL utilizando su certificado previamente descargado en su navegador, firma la solicitud, dando mayor credibilidad a la CA-UTPL y otorgándose como único responsable de la aprobación de la solicitud.

- *Aprobar la Petición sin firmar*: Cumple la misma funcionalidad que la de aprobar la petición, con la diferencia de que el administrador no ha instalado su certificado digital en el navegador de la RA. Cualquiera de las dos alternativas es válida.

- *Eliminar Petición*: Alguna petición que no se rija a las políticas establecidas por el grupo de seguridad PKI, o que comprometa la seguridad de la misma, se debe eliminar. La petición se traslada a la sección eliminados dentro de la RA.

Se tomaron como objeto de prueba las peticiones de los usuarios señalados con anterioridad.

4.2.4.1. Resultados

Las operaciones realizadas sobre dichas peticiones por parte del administrador de RA se muestran en el cuadro 4-4.

Petición	Operación efectuada	Éxito en la operación	S=Si N= No
Usuario 1	Editar petición Aprobar petición	S S	
Usuario 2	Editar petición Verificar PIN Aprobar petición sin firma	S S S	
Usuario 3	Editar petición Aprobar petición sin firma	S S	
Usuario 4	Editar petición Aprobar petición sin firma	S S	
Usuario 5	Editar petición Aprobar petición	S S	
Usuario 6	Editar petición Aprobar petición	S S	

Cuadro 4-4 Operaciones efectuadas sobre las peticiones de certificado de usuarios

4.2.5. Intercambio de datos desde RA hacia CA

Las peticiones aprobadas por el operador de la Autoridad de Registro (RA), deben ser transferidas al servidor de la CA, para que el administrador de este servidor se encargue de la generación de los correspondientes certificados digitales. Para ello emplea el protocolo ssh[24] el cual garantiza el aseguramiento de la información intercambiada y la automatización de este proceso.

4.2.5.1. Resultados

El cuadro 4-5 muestra los resultados del intercambio de las peticiones aprobadas.

Peticiones aprobadas	Protocolo empleado en el intercambio	Éxito en el intercambio	S= Si N= No
Usuario 1 al usuario 6	ssh	S	

Cuadro 4-5 Pruebas de intercambio de peticiones aprobadas desde RA hacia CA

[24] **SSH**: Intérprete de órdenes seguro **(S**ecure **SH**ell**),** sirve para acceder a máquinas remotas a través de una red

4.2.6. Emisión de Certificado

Las operaciones que el administrador de la CA puede llevar acabo con las peticiones de certificados llegadas a su poder son:

- *Emitir certificado:* Para emitir el certificado, es preciso que el administrador proporcione la clave privada de CA-UTPL, a fin de que pueda firmar el certificado generado.

- *Eliminar petición:* También requiere que se administre la clave privada de la Autoridad Certificadora CA-UTPL a fin de comprobar la identidad del administrador de la CA.

4.2.6.1. Resultados

Las operaciones efectuadas sobre las peticiones aprobadas de los usuarios que realizaron las pruebas se muestran en el cuadro 4-6.

Peticiones aprobadas	Operaciones efectuadas	Éxito en la operación	S =Si N= No
Usuario 1 al usuario 6	Emitir certificado	S	

Cuadro 4-6 Operaciones aplicadas sobre las peticiones de usuario aprobadas

4.2.7. Intercambio de datos desde CA hacia RA

Una vez emitidos los certificados, nuevamente retornan al servidor RA, para que sean colocados en la interfaz pública a disposición del solicitante para su descarga en formato PKCS#12[25]. Los certificados generados de los usuarios fueron transferidos empleando el protocolo ssh.

4.2.7.1. Resultados

El proceso de intercambio desde CA hacia RA se muestra en el cuadro 4-7

Certificados generados	Protocolo empleado en el intercambio	Éxito en el intercambio	S= Si N= No
Usuario 1 al usuario 6	ssh	S	

Cuadro 4-7 Certificados de usuario enviados de CA hacia RA

4.2.8. Notificación de correo electrónico

OpenCA permite al administrador de la RA la automatización del envío de correo de notificación al usuario avisándole que su certificado ha sido generado en cuanto ésta acción sucede.

[25] **PKCS#12:** Estándar de sintaxis de intercambio de información personal. Define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

4.2.8.1. Resultados

Los resultados de la notificación de correo electrónico se muestran en el cuadro 4-8:

Notificación de correo	Proceso de notificación	Éxito en la notificación (llegada del e-mail al usuario)	S= Si N= No
Usuario 1 al usuario 6	automático	N	

Cuadro 4-8 Resultados de la notificación automática de correo a usuarios

En ningún caso el correo llegó a los usuarios finales, lo que involucra analizar otras alternativas:

- Notificar a cada uno de los usuarios a través de un e-mail, obteniendo la dirección de correo electrónico de la petición de certificado realizada por dichos usuarios.

- En el momento de verificar los datos contenidos en la petición de certificado para su aprobación, el administrador de la RA puede indicarle verbalmente al solicitante el tiempo en el cual su certificado estará disponible y listo para ser descargado, obviamente en el caso de que el solicitante se presente personalmente ante el administrador.

Estas dos alternativas fueron aplicadas sobre los usuarios objetos de prueba, tal como se contempla en el cuadro 4-9.

Tipo de usuario	Tipo de notificación	Éxito en la notificación	S= Si N= No
Usuario 1	Notificación por medio de e-mail	S	
Usuario 2	Al momento de presentarse ante el administrador de RA	S	
Usuario 3	Notificación por medio de e-mail	S	
Usuario 4	Al momento de presentarse ante el administrador de RA	S	
Usuario 5	Al momento de presentarse ante el administrador de RA	S	
Usuario 6	Notificación por medio de e-mail	S	

Cuadro 4-9 Alternativas de notificación de correo a usuarios

4.2.9. Descarga de certificado

Existen dos formas de descargar un certificado por parte del usuario, las cuales se detallan en el manual de usuario (**anexo [3-14]**)

La forma en que los usuarios de prueba decidieron descargar sus certificados fue completamente a su elección.

4.2.9.1. Resultados

Los resultados de cómo los usuarios intentaron descargar su certificado del repositorio de la página web de CA-UTPL se muestra en el cuadro 4-10.

Certificados	Modo de descarga	Éxito en la descarga con el modo seleccionado	S= Si N= No
Usuario 1	Segunda Forma	S	
Usuario 2	Primera Forma	S	
Usuario 3	Segunda Forma	S	
Usuario 4	Segunda Forma	S	
Usuario 5	Segunda Forma	S	
Usuario 6	Segunda Forma	S	

Cuadro 4-10 Formas de descarga de certificado empleadas por los usuarios

En este punto los usuarios de prueba formularon algunas sugerencias:

- Debe existir una mayor explicación acerca de la manera de descargar el certificado.
- Una vez conocidas las maneras de descargar un certificado, los usuarios se inclinaron por utilizar la segunda forma descrita en la guía de usuario.

4.2.10. Revocación de Certificados

La revocación del certificado la hace únicamente el administrador del servidor de RA, previa solicitud del dueño del certificado debidamente comprobada y justificada. Este administrador debe aprobar la petición de revocación, para que la Autoridad Certificadora emita el certificado revocado.

4.2.10.1. Resultados

Se efectuó la revocación del certificado de los usuarios 2 y 4, a dichos certificados se les aplicaron las operaciones descritas en el cuadro 4-11.

Petición de revocación	Operaciones aplicadas por RA	Éxito en las operaciones	S= Si N= No
Usuario 2	Editar petición Aprobar petición sin el certificado de administrador de RA	S S	
Usuario 4	Editar petición Aprobar petición con el certificado del administrador de RA	S S	

Cuadro 4-11 Revocación de certificado aprobada por RA

Al ser aceptadas las peticiones de revocación, son enviadas al administrador de la CA para que, con la clave privada de CA-UTPL, lleve a cabo la generación de la revocación y la creación de la nueva Lista de revocación de certificados (CRL). (Cuadro 4-12)

Petición de revocación	Operaciones aplicadas por CA	Éxito en las operaciones	S= Si N= No
Usuario 2	Revocar certificado	S	
Usuario 4	Revocar certificado	S	

Cuadro 4-12 Revocación de certificado generada por CA

Este proceso está ejemplificado en el manual del administrador (**anexo [3-13]**).

4.2.11. Pruebas y Validación de firma digital y encriptación de correos electrónicos empleando un certificado de usuario.

Para utilizar funcionalidades de los certificados digitales como firma digital y encriptado de mensajes, es necesario configurar apropiadamente los clientes de correo, esto es, importar los certificados tanto de la Autoridad Certificadora raíz como del usuario que desee firmar y encriptar sus correos salientes.

4.2.11.1. Resultados

Las conclusiones de las pruebas realizadas con respecto al acoplamiento de los certificados a los clientes de correo se muestran en el cuadro 4-13.

Cliente de Correo	Éxito en la importación Certificado CA	S= Si N= No	Éxito en la importación Certificado Usuario	S= Si N= No
Outlook 2007	S		S	
Outlook Express 6.0	S		S	
Thunderbird 2.0	S		S	
Evolution 2.8	S		S	

Cuadro 4-13. Importación de certificados a diferentes clientes de correo.

En los clientes de correo arriba mencionados, las pruebas de importación de certificados, tanto raíz como de usuario fue exitosa. Por supuesto en el caso de los clientes de correo Outlook necesariamente los certificados de usuario debieron haber sido solicitados en el

navegador Internet Explorer, para que la compatibilidad entre cliente de correo y navegador (ambos productos de Microsoft) sea exitosa.

De esta manera se garantiza el uso de aplicaciones en este cliente, como el firmado y cifrado de mensajes. La manera de importar los certificados en los distintos clientes de correo se describe en el **anexo [4-2]**.

4.2.11.2. Firma Digital

Las pruebas realizadas aplicando firma digital a los correos enviados utilizando distintos clientes de correo están mostradas en el cuadro 4-14:

Usuario	Navegador usado para solicitar su certificado	Cliente de correo utilizado	Correcto envío de Mensaje firmado	S= Si N= No
Usuario 1	Mozilla Firefox 3.0	Thunderbird 2.0 Evolution 2.8	S S	
Usuario 2	Internet Explorer 7.0	Outlook Express 6.0	S	
Usuario 4	Internet Explorer 6.0	Outlook	S	

Cuadro 4-14. Datos de las pruebas de firma digital en diferentes navegadores

Es necesario que tanto el remitente como el receptor del correo tengan instalados sus certificados de usuario con formato PKCS#12 en sus respectivos clientes de correo, así como el certificado raíz de CA-UTPL. **[7]**

La forma de enviar un mensaje firmado digitalmente en los diversos clientes de correo está explicada en el **anexo [4-3]**.

4.2.11.3. Encriptación de Correo Electrónico

El mensaje firmado digitalmente puede ser también cifrado usando para ello la clave pública del receptor. Luego éste lo descifra usando su clave privada (certificado en formato PKCS#12) que debe tener importado en su cliente de correo. Enviar un mensaje cifrado presenta la ventaja de que, en el poco probable caso de que éste fuera interceptado por una tercera persona, no podría ser leído.

Las pruebas de encriptación de correo electrónico fueron realizadas en los clientes de correo listados en el cuadro 4-15

.

Usuario	Navegador usado para solicitar su certificado	Cliente de correo utilizado	Correcto envío de Mensaje encriptado	S= Si N= No
Usuario 1	Mozilla Firefox 3.0	Thunderbird 2.0 Evolution	S	
Usuario 2	Internet Explorer 7.0	Outlook Express 6.0	N	
Usuario 4	Internet Explorer 6.0	Outlook	N	

Cuadro 4-15. Datos de las pruebas de encriptación de correo en diferentes navegadores

En los clientes de correo de Windows (Outlook y Outlook Express) la información encriptada, si bien es cierto llego sin inconvenientes al destinatario, no pudo ser desencriptada y por ende leída.

Además los usuarios que efectuaron pruebas de firmado y cifrado de e-mails manifestaron haber experimentado cierto grado de dificultad en la puesta en práctica de ambas aplicaciones. Por ello es necesario poner a disposición de los mismos tutoriales acerca de cómo efectuar ambas operaciones.

La manera de enviar un mensaje cifrado empleando un cliente de correo determinado se halla documentada en el **anexo [4-4]**.

De las quince pruebas aplicadas a los usuarios de certificados digitales de identidad personal, fueron exitosas en su totalidad un total de trece, equivalente a un 86,7%; mientras que las dos restantes (13,3%) cumplieron su cometido parcialmente y deberán ser perfeccionadas. De este análisis concluimos que la Infraestructura de Clave Pública ha pasado las pruebas de funcionalidad necesarias como para llevar a cabo su implementación en la Universidad Técnica Particular de Loja.

CAPÍTULO 5

PROYECCION A FUTURO DE LA PKI

5. PROYECCION A FUTURO DE LA PKI

OBJETIVO:

Analizar todas las propuestas disponibles para implementar PKI, escoger la adecuada para llevar a cabo aplicaciones como firmas digitales y autenticación de sitios seguros en el entorno de la UTPL y proyectar el campo de acción de la PKI.

5.1. Introducción

Toda la evaluación acerca de la implementación de una Infraestructura de Clave Pública (PKI) en la Universidad Técnica Particular de Loja llevada a cabo en los capítulos anteriores ha girado en torno a la herramienta opensource denominada OpenCA, que a su vez fue analizada y recomendada en investigaciones previas referentes al tema **[2]**.

Sin embargo sería un error recargar toda la responsabilidad de la implantación de una PKI únicamente en este software, sin tomar en cuenta aspectos como el hecho de que en la universidad existen servicios críticos que requieren niveles de aseguramiento de la información óptimos, niveles que solo podrían ser brindados por organizaciones comerciales reconocidas internacionalmente y con mayor experiencia en el aseguramiento de información.

Por tal motivo, este capítulo contempla diferentes alternativas evaluadas en la implementación de una PKI, y determina la más adecuada a ser llevada a la práctica, tomando lo mejor de cada una de dichas alternativas.

5.2. Análisis comparativo entre las opciones para implementar una Infraestructura de Clave Pública (PKI)

5.2.1. Opción 1: OpenCA

OpenCA es el nombre de la herramienta open-source que ha sido diseñada para establecer una Autoridad Certificadora encargada de la generación y administración de certificados digitales, y su aplicación en firmas digitales, y la cual ha sido estudiada, analizada, evaluada y configurada por el presente proyecto. Para complementar la información con algunos datos generales, se puede decir que es una contribución de OpenCA Group y data de 1999, cuando se lanzo la versión 0.2.1. Desde entonces ha sufrido modificaciones hasta la versión 1.0.2 que es la más actual. Brevemente se describen sus características principales:

- Posee una interfaz web creada en lenguaje Perl.
- Hace uso de operaciones criptográficas basadas en OpenSSL.
- Utiliza una base de datos.

A continuación se presenta el cuadro 5-1 con las características de esta alternativa y los costos que implica su implementación:

Parámetro	Observación	Costo
Permiso de AC	Lograr que la Universidad Técnica Particular de Loja se establezca como Autoridad Certificadora reconocida, para lo cual debe regirse a las disposiciones legales establecidas actualmente, que son detalladas en el **anexo [5-1]**	$ 22000,00
Servidores	Ya están destinados como se indica anteriormente. Son servidores tipo Blade (2). Salvo el caso que se quiera implementar nuevos de mayor capacidad, estos deberán ser presupuestados en lo posterior.	$ 14000,00
Personal	Dos administradores (para CA y RA). Según el precio de contrato de dos empleados si no se va a utilizar personal propio de la Universidad. Se ha presupuestado $ 500,00 mensuales por cada uno. (*)	$ 12000,00 anuales
Tokens	(opcional) Almacena credenciales de usuarios. El costo promedio es de $ 60 por cada usuario que desee utilizar estos dispositivos. Para comenzar puede considerarse un mínimo de 30 tokens.	$ 1800,00
	TOTAL	**$ 35800, 00**

Cuadro 5-1 Evaluación de la alternativa OpenCA

(*) se pueden restar $ 12000,00 del valor de costo del personal si se asigna la administración de la PKI a un administrador que ya labore en la Universidad.

Seguidamente un breve detalle de ventajas y desventajas.

- **Ventajas**
    - Al ser una herramienta open-source, su implementación y funcionamiento no significan costo alguno.
    - Todos los procesos, (verificación, aprobación y generación de certificados) son realizados por personal de la universidad.
    - La generación de certificados no reportaría costo alguno para los estudiantes ni para la universidad.

- **Desventajas**

    - Existe aun poca información de la versión de OpenCA con la que se ha trabajado en esta investigación, por lo que la capacitación y administración de la misma pueden resultar difíciles en un principio.

    - El certificado raíz de la Autoridad Certificadora CA-UTPL es *autofirmado*. Esto significa que no tiene el respaldo de una entidad certificadora confiable y reconocida, ya sea nacional o internacionalmente. Por tal razón es necesario instalar el certificado raíz de CA-UTPL en cada navegador y cliente de correo en el que se vaya a trabajar.

    - Los gastos de mantenimiento, actualización y soporte correrían a cargo de la universidad.

5.2.2. Opción 2: Certificados de E-Sign

E-Sign es un proveedor de servicios afiliado a Verisign para la emisión de certificados digitales. Posee algunos paquetes de servicios que podrían adaptarse a las necesidades de la universidad. **[8]**

5.2.2.1. Verisign MPKI:

PKI Administrado (MPKI) es un sistema de gestión de certificados con una RA local que externaliza la gestión de claves, es decir permite que una organización, como podría ser la UTPL, maneje las funciones de aprobación de certificados para sus usuarios (es decir alumnos, docentes, etc).

Requiere de un administrador de Autoridad de Registro local (LRAA), el cual interactúa con la central de Verisign MPKI a través del Centro de Control MPKI. Este administrador es proporcionado por la UTPL.

Dentro de esta solución existen dos alternativas: MPKI Lite y MPKI SSL combinadas para la generación de certificados de cliente y servidor respectivamente; y MPKI Full que es una opción más avanzada y que será analizada posteriormente.

5.2.2.2. MPKI Lite y MPKI SSL

Esta solución combinada permite emplear la solución MPKI Lite para la generación de certificados digitales individuales, en tanto que los certificados de servidor serian generados por la solución MPKI SSL.

El cuadro 5-2 presenta más detalladamente los costos de puesta en producción de esta alternativa. Los valores son a un año, y la renovación tiene el mismo valor.

Solución	Costo			Observaciones
Certificados MPKI Lite públicos	**Numero**	**Precio ($)**	**Periodo de validez**	*Públicos* significa que las CA raíces ya están incluidas en los navegadores, servidores y paquetes de correo electrónico más populares.
	25 50 100 500 1000	3800,00 5750,00 7700,00 9550,00 13100,00	365 días “ “ “ “	
Certificados MPKI SSL para servidores	**Producto**	**Paquete de 30 ($)**	**Validez**	
	MPKI SSL Premium SSL	20700,00	1 año	$ 690,00 de forma individual
	MPKI SSL Premium SSL	37000,00	2 años	$ 617,00 de forma individual
	MPKI SSL Premium SSL	49900,00	3 años	$ 554,00 de forma Individual
	MPKI SSL Premium SSL	64000,00	4 años	$ 533,00 de forma individual
Tokens**[9]** (opcional)	$ 55,00 (calculado para 30 usuarios)			$ 1650,00
TOTAL	**$ 5750,00 para 50 usuarios comunes + $ 20700,00 para 30 certificados de servidor = $ 26450,00 anuales renovables por el mismo valor.**			

Cuadro 5-2 Evaluación de la Propuesta MPKI Lite y MPKI SSL

Ventajas:

- Tiempos de respuesta rápidos, puesto que la emisión de certificados MPKI Lite públicos, una vez enrolada la solicitud de certificación, es de no más de 30 minutos.

- La universidad podrá controlar la emisión de certificados digitales para usuarios internos y externos, a la vez que externaliza las tareas de centro de proceso de datos, tales como la generación, certificación, validación, renovación y revocación de certificados digitales, de las que se ocupa VeriSign.

- Garantiza la confidencialidad de los mensajes y permite que la universidad pueda comprobar de manera confiable la identidad de los remitentes y de los destinatarios.

- En el caso de servidores, MPKI SSL permite administrar todos los certificados SSL, en toda la universidad, a través de una interfaz de navegador Web. No es necesario instalar previamente hardware ni software. La instalación se realiza en sólo unos minutos.

- El servicio MPKI para SSL está protegido con dos procesos de autentificación y cifrado SSL.

Desventajas:

- La solución MPKI Lite es limitada, solamente puede cubrir hasta 1000 certificados de usuario.

- El costo de las soluciones, puesto que son validas por un periodo de tiempo determinado, y la renovación implica otro gasto.

- La universidad no controla todos los procesos de certificación, como la generación, validación y renovación de certificados, cosa que si ocurre si la UTPL fuera Autoridad Certificadora.

5.2.2.3. MPKI Full (OnSite)

El Servicio Managed PKI (OnSite) de VeriSign permite aplicaciones corporativas seguras tales como correo electrónico seguro, intranets, extranets, y acceso a la Web con certificados digitales. El Servicio Managed PKI (OnSite) de VeriSign permite a las compañías establecer su propia Infraestructura de Llaves Públicas (PKI) (de manera rápida, fácil, y efectiva en base al costo). VeriSign brinda todos los servicios del ciclo de vida de los certificados, soporte a las aplicaciones y herramientas de administración necesarias para operar un sistema robusto de PKI. Los valores mostrados en el cuadro 5-3 son para el primer año, renovables luego de ese periodo de tiempo.

Servicio	Costo	Observaciones
MPKI Full (onsite) (Pago por set-up, una sola vez)	$ 20000,00	Incluye 10 días máximos de PSO (tiempo de Organización de Servicios Profesionales), es decir instalación del software Verisign, etc. Los días adicionales de PSO tienen un valor de $ 2000,00
MPKI Full Premium	$ 22000,00 (10% más que la solución MPKI	Permite a los clientes de MPKI obtener información más actualizada sobre el estado de

	Full)	sus certificados
	TOTAL	**$ 20000,00 anual renovable por el mismo valor.**

Cuadro 5-3 Evaluación de la propuesta MPKI Full

Ventajas:

- Ahorraría a la universidad el construir, desplegar y mantener una infraestructura interna, pero le otorga a la misma el control completo sobre el ciclo de vida de los certificados: emisión, renovación y revocación.
- Menor costo total, debido a que Verisign se encarga de la elaboración, mantenimiento, actualización, seguridad y auditorías externas de sus plataformas PKI.
- Al utilizar una marca reconocida y confiable, la UTPL garantiza la validez y confiabilidad de los certificados que genere.
- Es una solución que soporta requerimientos desde 250 hasta 500000 usuarios. Es decir posee una gran escalabilidad.

Desventajas:

- Los costos de implementación y más aun los de renegociación con Verisign son realmente elevados. Los costos arriba indicados son para 2000 usuarios.
- El traslado y gastos son adicionales para todos los compromisos de Servicios Profesionales.
- La implementación del servicio es de mínimo 90 días, es decir el tiempo de prueba de la aplicación. En caso de presentarse alguna falla en el sistema (por ejemplo el daño de un equipo) el tiempo de espera hasta la reposición del mismo puede ser considerable.

Luego de analizadas todas las alternativas disponibles, y debido a que ninguna solución por si sola podría solventar la implementación de una PKI en la universidad, especialmente si se considera proyectarla a gran escala en un mediano plazo, se decidió extraer lo mejor de cada una de ellas y amalgamar una propuesta que sea lo suficientemente sólida como para que sirva de plataforma a nuevas proyecciones de la infraestructura. Dicha propuesta es expuesta a continuación.

5.3. Elaboración de una alternativa de implementación

Puesto que la PKI se va a implementar por vez primera en la universidad, es conveniente establecer primeramente un campo operacional limitado, pero que tenga la posibilidad de expandirse a todo el entorno universitario a medida que la infraestructura se consolide y los requerimientos de certificación de usuarios de la universidad vayan en aumento.

Se ha diseñado por eso una propuesta de solución que combina lo mejor de las alternativas antes descritas, la cual es presentada a continuación.

5.3.1. Combinación OpenCA-MPKI SSL

Esta solución incorpora emplear OpenCA y sus características de generación de certificados de usuario, para emitir certificados a usuarios tales como estudiantes, docentes, administrativos y autoridades. Así como para los servidores internos y menos críticos junto con los administradores de éstos. Mientras que la generación de certificados para los servidores externos y más críticos estaría dada por el servicio MPKI SSL. De acuerdo al número de servidores externos a asegurar, se contrataría el paquete MPKI SSL más adecuado.

5.3.1.1. Certificados para usuarios comunes

Dentro de los usuarios comunes están comprendidos estudiantes, docentes, autoridades y empleados, así como administradores de servidores poco críticos o que no presten servicios externos.

Las ventajas de generar certificados de usuario por medio de OpenCA son:

- La distribución de los certificados raíz de la Autoridad Certificadora CA-UTPL entre los usuarios pertenecientes a la misma organización será más fácil.

- Verificar la autenticidad de los solicitantes de certificados y de la información que proporcionen por parte del administrador de la Autoridad de Registro (RA), ya sea en forma física (a través de una reunión con el solicitante), o consultando a Bases de Datos como el Sistema de Gestión Académica, en el caso de estudiantes que no pudieran acercarse a dialogar con el administrador de la Autoridad de Registro.

- Permite a los administradores de los servidores de CA y RA planificar de mejor forma los procesos tales como la petición de certificados por parte de los usuarios, verificación de la información, aprobación de peticiones, intercambio entre servidores y generación de certificados.

Por ejemplo si se desea elaborar un esquema para atender las peticiones de cien usuarios en una semana, se esquematizaría un cronograma como el del cuadro 5-4 Es decir, en el primer día, y luego de que hayan accedido a la interfaz de CA-UTPL y formulado su solicitud de certificado, los veinte primeros usuarios deben acercarse (si es posible) al operador de la RA, presentando sus credenciales para corroborar que efectivamente son quienes han presentado la solicitud y que pertenecen al entorno universitario. De igual forma para el resto de peticionarios los demás días.

	Día 1	Día 2	Día 3	Día 4	Día 5
Por la mañana	Usuarios del 1-20	Usuarios del 21-40	Usuarios del 41-60	Usuarios del 61-80	Usuarios del 81-100
Por la tarde	Procesos de aprobación, verificación, intercambio RA-CA y generación de certificados para estos usuarios.	Procesos de aprobación, verificación, intercambio RA-CA y generación de certificados para estos usuarios.	Procesos de aprobación, verificación, intercambio RA-CA y generación de certificados para estos usuarios.	Procesos de aprobación, verificación, intercambio RA-CA y generación de certificados para estos usuarios.	Procesos de aprobación, verificación, intercambio RA-CA y generación de certificados para estos usuarios.

Cuadro 5-4 Ejemplo de esquema de trabajo para generar certificados de usuario

Esto se hace con el fin de coordinar de mejor manera los procesos de intercambio de información entre los servidores RA y CA, evitando de esta forma una sobrecarga de trabajo en lo relacionado a aprobación, verificación y generación de los certificados.

- La generación de certificados para usuarios facilitará a éstos utilizarlos en aplicaciones como firma digital de mensajes de correo y cifrado de los mismos a otros usuarios dentro del entorno universitario.

5.3.1.2. Certificados para servidores

Para saber cuántos servidores existen en la actualidad, se toma como referencia el informe presentado con fecha 21 de mayo de 2009 acerca de la capacidad instalada a nivel de servidores de la Universidad Técnica Particular de Loja. De los 65 servidores (56 servidores y 9 equipos empleados como servidor) se seleccionó aquellos considerados más críticos, es decir, los servidores externos (cuadro 5-5).

Servidor	Servicio
GDR1.UTPL.EDU.EC	Servicio Web
ASUTPL	DEIAP; Reporting Service; Syllabus
Cajanuma	Base de Datos
DEVSERVER.OLD	Refactory
PODCASTSERVER.UTPL.EDU.EC	PodCast
Gdr2	Resolucion de nombres
Repo	FTP, Repositorio
Webmail	Servicio de correo
Gdr3	Servicio de Correo
ULoja	Baan
Eva	Eva
CA	Autoridad Certificadora
NODO1SGA	Servicios Profesor; Syllabus
WSUTPL	Servicios Web en internet(Sitio profesor,

	estudiantes, centros
PRESENTATION SERVER	Administrador Aulas Virtuales
BDVirtual	Dspace, entorno virtual de aprendizaje

Cuadro 5-5 Servidores externos y/o más críticos

Los servidores listados son 16. Si tomamos como referencia los costos establecidos en el apartado 4.2.2.1, se indica que, al no aplicar el paquete de 30 servidores, el costo individual por servidor es de $ 690,00, por lo que tendremos el siguiente resultado (cuadro 5-6).

Número de Certificados	Costo	Periodo de validez
16	$ 11040	1 año

Cuadro 5-6 Costo del aseguramiento de servidores críticos

Con esta propuesta se implementaría una PKI estable, con certificados de usuario que permitan establecer firma digital entre usuarios internos y con certificados de servidor reconocidos mundialmente para el aseguramiento de los servidores más críticos. Mientras que a medida que crezca la demanda de usuarios, la solución MPKI Full sería la más recomendable de implementar a futuro para fortalecer la Infraestructura de clave pública existente.

El costo de esta solución combinada es la mostrada en el cuadro 5-7.

Parámetro	Costo $
Para usuarios comunes (si se desea validar el certificado raíz de CA-UTPL, si no, se puede mantener el certificado raíz autofirmado exclusivamente para usuarios comunes).	**20000,00**
Para un número de 16 certificados críticos de servidor (por un tiempo de validez de un año renovable al mismo costo)	**11040,00**
TOTAL:	**31040,00**

Cuadro 5-7 Costo monetario de la propuesta combinada

CAPITULO 6

DISCUSIÓN DEL PROYECTO

6. Discusión del Proyecto

Una vez analizadas todas las fases que conformaron el proyecto que implementará una Infraestructura de Clave Pública en la Universidad Técnica Particular de Loja, así como de haber planteado una propuesta de puesta en marcha de dicha infraestructura, es momento de hacer una retrospectiva a fin de recoger las experiencias acumuladas en la realización de esta tesis y dejarlas plasmadas a continuación para futuras referencias.

El establecimiento de una PKI es una combinación de hardware y software, políticas y procedimientos de seguridad. No existe por tanto un software milagroso que por sí mismo pueda llevar a cabo esta infraestructura, sin que éste vaya acompañado de mecanismos que aseguren la integridad de la información manejada por dicho software.

Esto se comprobó al momento de controlar el acceso a los recursos críticos de la aplicación. Fue necesario coordinar acciones con los encargados de la seguridad de la red de la universidad a fin de ubicar a los dos servidores de la PKI dentro de la zona más segura y monitoreada de dicha red.

De entre las tantas opciones, se ha elegido trabajar con OpenCA que es una herramienta open-source, por tal motivo no tiene costo de adquisición pero si hay costos en lo referente a su implementación (costo de servidores en donde se alojará, mantenimiento) y capacitación interna para aprender a manejarla. Esta capacitación debe darse por medio de tutoriales y participación en foros de discusión de esta herramienta, ya que al ser open-source, no existe una capacitación proveniente de la empresa que la crea, como sucede con las herramientas privativas.

Además de ello, hay que resaltar que una de las limitantes por las cuales PKI es una infraestructura aun no muy divulgada, especialmente en nuestro medio, es en definitiva los altos precios de los certificados individuales y el poco conocimiento acerca de cómo integrar la solución a aplicaciones reales, aspectos que tratan de ser solventados en este proyecto.

Al implementar una Infraestructura de Clave Pública basada en OpenCA, se busca que la Universidad Técnica Particular de Loja, a través de su Autoridad Certificadora (CA-UTPL), sea la encargada de establecer identidades digitales entre los miembros de su comunidad, es decir asociar a sus entidades (estudiantes, docentes, administrativos o autoridades) una unicidad con el par de claves pública/privada generadas por CA-UTPL.

De esta forma CA-UTPL se convierte en la parte confiable para todos los usuarios de la Universidad Técnica Particular de Loja que soliciten su certificado de identidad digital. Dicha autoridad certificadora además será gestionada por personal administrativo propio de la universidad.

Inicialmente el costo de la generación del certificado será asumido por la universidad y su infraestructura técnica.

Por el poco trabajo que se ha desarrollado empleando la herramienta OpenCA, al menos a nivel nacional, no se tiene conocimiento a ciencia cierta de la real capacidad de generación de certificados. Sumado al hecho de que la PKI se va a implementar por vez primera en la universidad, es conveniente establecer primeramente un campo operacional limitado, pero que tenga la posibilidad de expandirse a todo el entorno universitario a medida que la infraestructura se consolide y los requerimientos de certificación de usuarios de la universidad vayan en aumento.

Por tal motivo se han analizado otras alternativas que complementen y fortalezcan las funcionalidades de OpenCA, en especial en lo relacionado a generar certificados que autentiquen servidores, dejando el manejo de certificados de usuario a la Autoridad Certificadora CA-UTPL. Estas alternativas están vinculadas a establecer convenios con organizaciones reconocidas internacionalmente y que posean experiencia en el establecimiento de PKI, experiencia que, como se manifestó anteriormente, aun es escaza.

Verisign es la organización con la cual se han mantenido contactos y que ha dado a conocer todas las soluciones que están a disposición de la universidad. Después de evaluadas todas las alternativas, se ha optado por la presentada en la propuesta de solución de este proyecto.

Entre los aspectos aún por cubrir en el futuro respecto a PKI en la universidad, está el hecho de integrar la infraestructura con otra que maneje información sobre la autenticación de usuarios, como por ejemplo el Sistema de Gestión Académica; con el objeto de agilizar el proceso de autenticación del usuario, es decir determinar si es parte del entorno universitario, sin necesidad de requerir la presencia física de dicho usuario junto con algún documento que lo acredite. O implementar OpenLDAP[26] a fin de tener un servicio de directorio ordenado y distribuido que permita buscar información referente a los certificados en un entorno de red.

Se debe buscar la manera de conseguir el reconocimiento de la Autoridad Certificadora CA-UTPL a nivel nacional ante el organismo encargado de ello, como es el CONATEL; de esta forma CA-UTPL podrá prestar en un futuro sus funciones de certificación no solo a personal de la universidad, sino a entidades públicas o privadas dentro del país. Los requerimientos que debe cumplir para tal fin están contemplados en **[17]** y **[18]**.

También está la forma de cómo el usuario pueda disponer de la lista de certificados revocados, es decir que ya no tienen usabilidad, de la manera más rápida posible (online), por medio de la implementación de protocolos como el OCSP (*Online Certificate Status Protocol*) o Protocolo en línea del estado del certificado, que informa de la forma más actualizada posible, acerca del estado de un certificado.

De las experiencias adquiridas en este proyecto, el aseguramiento de la clave privada de CA-UTPL constituye la parte fundamental de la PKI, por lo que los controles del acceso al servidor CA son fundamentales a la hora de permitir el acceso únicamente al administrador del servidor.

Se recurrió a foros y páginas de información acerca de la funcionalidad de OpenCA, pues todo lo que hasta el momento se conoce de esta herramienta, en especial de su última versión, es fruto de la retroalimentación surgida de los problemas de unos y de las soluciones que han sabido encontrar otros a esos mismos inconvenientes, en pro del mejoramiento y la expansión del software.

Por tal razón considero necesario fomentar en la comunidad universitaria la investigación y utilización de herramientas de este tipo, así como la apertura a sistemas operativos de código abierto, como GNU/Linux, a fin de que la comprensión de la configuración, instalación y funcionamiento de la Infraestructura de Clave Pública sea más fácil.

[26] **OpenLDAP** es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

- La implementación de una PKI dentro de la Universidad Técnica Particular de Loja, con el establecimiento de una Autoridad Certificadora y la emisión de certificados digitales que permitan a los usuarios funcionalidades como firma digital y cifrado de datos, constituye el inicio de una alternativa cuyos beneficios pueden incluir desde la simplificación de tareas administrativas (reducción en la cantidad de trámites en las matrículas, aprobación de solicitudes, presentación de informes), hasta la reducción de los gastos que estas mismas tareas generan en la actualidad (consumo de papel, impresora); a la vez que se contribuye con la conservación de los recursos naturales.

- Al ser PKI una plataforma compleja que involucra software, hardware y políticas de seguridad combinadas en el aseguramiento de la información de una organización, no todo debe estar basado en la herramienta OpenCA, sino que ésta debe constituir una parte de la infraestructura. Por tal motivo se ha elaborado una propuesta que incluye el apoyo de entidades más experimentadas en el campo de seguridad de datos (como es el caso de Verisign), a fin de abarcar no solo a usuarios, sino a los servidores que prestan funciones para la universidad. Asimismo se han establecido políticas de acceso a los equipos, requerimientos en cuanto a la capacidad de los mismos para una mayor agilidad en los procesos y soporte para escalabilidad de la infraestructura.

- El establecimiento de CA-UTPL como Autoridad de certificación avalada a nivel nacional mediante el cumplimiento de las disposiciones dictaminadas por el Conatel, permitirá que en poco tiempo CA-UTPL se convierta en proveedora de servicios de certificación, ya sea a entidades públicas como privadas a nivel local y nacional.

- La implementación de la PKI en la UTPL emplea un modelo de confianza jerárquico, lo que implica el establecimiento de una Autoridad Certificadora raíz (CA) con sus funciones de intercambio y de generación de certificados; y bajo la cual existe una Autoridad de Registro (RA) subordinada, encargada de la aprobación de las peticiones de certificación y de la interacción con los usuarios. Tanto CA como RA se encuentran en servidores separados.

- El empleo del protocolo ssh en el intercambio de información entre los servidores CA y RA establece una conexión cifrada y automatizada, garantizando la integridad de los datos transportados, una ventaja considerable sobre otros medios de intercambio de información como disquetes, cd roms o memorias flash.

- El campo de acción inicial de PKI está enfocado a miembros de la comunidad universitaria pertenecientes a modalidad presencial, debido a que es más fácil para el administrador de la RA verificar físicamente la identidad de un solicitante de certificado, así como su relación actual con la universidad. Queda entonces latente la posibilidad de ampliar el rango de aplicabilidad de la infraestructura mediante la integración con el Sistema de Gestión Académico, a fin de involucrar a todos los miembros de la comunidad universitaria.

RECOMENDACIONES:

- Se recomienda combinar la Infraestructura de Clave Pública con sistemas de gestión académica y de control de personal, de tal forma que la comprobación de la identidad de los solicitantes se efectúe sin la necesidad de la presencia de los mismos ante el administrador de la RA; con lo cual el campo de acción de CA-UTPL se extendería a estudiantes de modalidad a distancia.

- Conformar un equipo de trabajo de PKI que pueda expandir esta infraestructura en la universidad a la brevedad posible, a través de la difusión de su aplicabilidad en lo relacionado a firmas digitales y correo electrónico seguro.

- Mantener un contacto o establecer comunicación con el Proyecto OpenCA, a través de foros, correos electrónicos o intercambio de opiniones a fin de obtener información actualizada del software, nuevas versiones, aplicación de parches para solucionar posibles bugs, etc

- Establecer políticas de seguridad que restrinjan el acceso a los recursos que maneja la PKI tanto a nivel físico como lógico. De manera que solo los administradores y el personal autorizado pueda manejar dichos recursos.

- Al utilizar herramientas open-source en la implementación de este proyecto, se recomienda masificar el uso de este tipo de software entre los estudiantes, docentes y personal administrativo de la universidad, por medio de seminarios, cursos de capacitación, foros de discusión, etc.

- Los administradores de los servidores que conforman la PKI deben tomar en cuenta las recomendaciones que se establecen en el manual del administrador.

ANEXOS

Anexo 2

[Anexo 2-1] Algoritmos de Encriptación de clave

- **RSA**

Es un algoritmo asimétrico cifrador de bloques.

Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes.

Cuando se quiere enviar un mensaje, el emisor busca la clave pública de cifrado del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, éste se ocupa de descifrarlo usando su clave oculta.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado.

Emplea expresiones exponenciales en aritmética modular.

La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales. **[10]**

- **DSA**

Algoritmo de firma digital, que como su nombre lo indica, sirve para firmar y no para cifrar información. Requiere mucho más tiempo de cómputo que RSA **.**

Generación de llaves:

- Elegir un número primo p de L bits, donde $512 \leq L \leq 1024$ y L es divisible por 64.
- Elegir un número primo q de 160 bits, tal que $p-1 = qz$, donde z es algún número natural.
- Elegir h, donde $1 < h < p - 1$ tal que $g = h^z \pmod p > 1$.
- Elegir x de forma aleatoria, donde $1 < x < q-1$.
- Calcular $y = g^x \pmod p$.

Los datos públicos son p, q, g e y. x es la llave privada.

Firma:

- Elegir un número aleatorio s, donde $1 < s < q$.
- Calcular $s1 = (g^s \bmod p) \bmod q$.
- Calcular $s2 = s^{-1}(H(m)+s1*x) \bmod q$, donde H(m) es la función hash SHA-1 aplicada al mensaje m.
- La firma es el par (s1, s2).

Si s1 o s2 es cero, se vuelve a repetir el procedimiento.

Verificación:

- Calcular w = $(s2)^{-1}$(mod q).
- Calcular u1 = H(m)*w(mod q).
- Calcular u2 = s1*w(mod q).
- Calcular v = [$g^{u1}*y^{u2}$mod p]mod q.
- La firma es válida si v = s1. **[11]**

- **ECDSA**

El Algoritmo de Firma Digital de Curva Elíptica, por sus siglas en español, proporciona la misma seguridad que los algoritmos antes indicados con un número menor de bits. Existen dos tipos de curvas dependiendo del campo finito en el que se definan que pueden ser GF(P) o GF(2^m).

Proceso de Firma y Verificación:

Generación de llaves:

- Seleccione una curva elíptica *E*.
- Seleccione un punto *P* (que pertenezca a *E*) de orden *n*.
- Seleccione aleatoriamente un número *d* en el intervalo [1, *n - 1*].
- Calcule *Q = dP*.
- *d* será la llave privada.
- *Q* será la llave pública.

Proceso de firma

- Seleccione un número *k* de forma aleatoria.
- Calcule $kP = (x_1,y_1)$.
- Calcule $r = x_1 \bmod n$. Si *r* = 0 regresa al primer paso. (En este paso x_1 es tratado como un entero).
- Calcule $(k^{-1}) \bmod n$.
- Calcule $s = k^{-1}(H(m) + dr) \bmod n$. Si *s = 0* regrese al primer paso. (*H(m)* es el hash del mensaje a firmar, calculado con el algoritmo SHA-1).
- La firma del mensaje *m* son los números *r* y *s*.

Proceso de Verificación

- Verifique que *r* y *s* estén dentro del rango [1,*n - 1*].
- Calcule $w = s^{-1} \bmod n$.
- Calcule $u_1 = H(m)w \bmod n$.
- Calcule $u_2 = r \cdot w \bmod n$.
- Calcule $u_1P + u_2Q = (x_0,y_0)$
- Calcule $v = x_0 \bmod n$
- La firma verifica si y solo si *v = r* **[12]**

[Anexo 2-2] Generación de clave y de petición de certificado P10 con OpenSSL

La petición podrá generarse a través de OpenSSL, keytool o a través de Microsoft Internet Information Service (IIS). Aquí se describe la forma de hacerlo en OpenSSL.

El comando a utilizar será:

- `openssl req -new -nodes -keyout clave_privada.pem -out` *`pet_nombre_servidor`*`.p10`

En donde *pet_nombre_servidor* corresponde al nombre de dominio del servidor.

Una vez ejecutado este comando, se requerirán diferentes datos: Se deberá indicar en el campo *Organization* (0) UTPL. En el campo *Organizational Unit* (OU) deberá indicarse la unidad de la UTPL a la que pertenece el servidor.

Se deberá indicar el nombre de servidor en el campo Common Name (CN) de la petición.

Si el certificado tiene añadido un campo e-mail al DN, éste debe tratarse de una cuenta general del tipo webmaster@, admin@, etc. El objetivo del e-mail en el DN es primordialmente permitir que el certificado sea utilizado para firmar mensajes de correo (firmarlos con la firma del servidor, no es una firma personal). Hay algunas aplicaciones posibles, como puede ser el envío de mensajes institucionales o el uso en servidores de listas.

Los *extra attributes (opcionales)* pueden dejarse en blanco. **[13]**

Anexo 3

Anexo [3-1] Módulos Perl necesarios para instalar OpenCA.

Módulos	Versión
Authen::SASL	2.04
CGI::Session	3.95
Convert::ASN1	0.18
Digest::HMAC	1.01
Digest::MD5	2.24
Digest::SHA1	2.02
Encode::Unicode	
IO::Stringy	2.108
MIME::Base64	2.20
MIME::Lite	3.01
MIME::Tools	5.411
MailTools	1.58
NetServer	0.86
Parse::RecDescent	1.94
X500::DN	0.28
XML::Twig	3.09 (de preferencia)
Libintl::perl	1.10
Perl::LDAP	0.28
XML::Parser	2.23 (de preferencia)
URI	1.23

Anexo 3-1 Módulos Perl requeridos para instalar OpenCA

[Anexo 3-2] Archivo de configuración openca.conf

```
ScriptAlias /cgi-bin/pki/ra /usr/local/var/www/cgi-bin/pki/ra
ScriptAlias /cgi-bin/pki/pub /usr/local/var/www/cgi-bin/pki/pub
ScriptAlias /cgi-bin/pki/ldap /usr/local/var/www/cgi-bin/pki/ldap
ScriptAlias /cgi-bin/pki/scep /usr/local/var/www/cgi-bin/pki/scep

Alias /pki/ra /usr/local/var/www/html/pki/ra
Alias /pki/pub /usr/local/var/www/html/pki/pub
Alias /pki/ldap /usr/local/var/www/html/pki/ldap
```

Anexo 3-2 /etc/apache2/conf.d/openca.conf

[Anexo 3-3] Archivo de configuración menu.xml.template

```
->
–
<item>
<id>1</id>
<name>General</name>
–
<item>
<name>Not logged in</name>
```

```
<link/>
<target>main</target>
</item>
–
<item>
<name>Requerir un certificado</name>
<link>cmd=getStaticPage;name=selectCSRtype</link>
<target>main</target>
</item>
–
<item>
<name>Obtener Certificado Requerido</name>
<link>cmd=getParams;GET_PARAMS_CMD=getcert</link>
<target>main</target>
</item>
–
<item>
<name>Testear Certificado</name>
<link>cmd=test_cert</link>
<target>main</target>
</item>
–
<item>
<name>Revocar Certificado</name>
<link>cmd=revoke_req</link>
<target>main</target>
</item>
</item>
–
<item>
<id>5</id>
<name>Informacion de CA</name>
–
<item>
<name>Politica</name>
<link>@policy_link@</link>
<target>main</target>
</item>
–
<item>
<name>Obtener Certificado de CA</name>
<link>cmd=getStaticPage;name=download_cacert</link>
<target>main</target>
</item>
–
<item>
<name>Lista de Revocacion de Certificados</name>
<link>cmd=getStaticPage;name=download_crl</link>
<target>main</target>
</item>
–
<item>
<name>Version del software</name>
<link>cmd=serverInfo</link>
<target>main</target>
</item>
</item>
–
```

```
<item>
<id>10</id>
<name>Certificados</name>
–
<item>
<name>Validos</name>
<link>cmd=lists;action=certslist</link>
<target>main</target>
</item>
–
<item>
<name>Expirados</name>
<link>cmd=lists;action=certsExpiredList</link>
<target>main</target>
</item>
–
<item>
<name>Suspendidos</name>
<link>cmd=lists;action=suspendedlist</link>
<target>main</target>
</item>
–
<item>
<name>Revocados</name>
<link>cmd=lists;action=revokedlist</link>
<target>main</target>
</item>
–
<item>
<name>Busqueda</name>
<link>cmd=getStaticPage;name=search_cert</link>
<target>main</target>
</item>
</item>
–
<item>
<id>15</id>
<name>Peticiones</name>
–
<item>
<name>Peticiones de Certificado</name>
<link>cmd=lists;action=newReqs</link>
<target>main</target>
</item>
–
<item>
<name>Peticiones de Revocacion de Certificado</name>
<link>cmd=lists;action=newCRRs</link>
<target>main</target>
</item>
</item>
```

Anexo 3-3 /usr/local/etc/openca/menu.xml.template

[Anexo 3-4] Archivos de configuración del directorio /usr/local/etc/openca/access_control

```
<database>internal</database>
        <passwd>
          <!--
             the initial user root has the passphrase root
             you can use the script openca-digest to create the passphrases
             if you want to add another user simply create a second user
structure
             <user>...</user>
          -->
          <user>
             <name>admin</name>
             <algorithm>sha1</algorithm>
             <digest>0DPiKuNIrrVmD8IUCuw1hQxNqZc</digest>
             <role>CA Operator</role>
          </user>

        </passwd>
      </login>
      <acl_config>
        <acl>yes</acl>
        <list>/usr/local/etc/openca/rbac/acl.xml</list>
        <command_dir>/usr/local/etc/openca/rbac/cmds</command_dir>
        <module_id>@node_module_id@</module_id>
        <map_role>yes</map_role>
        <map_operation>yes</map_operation>
      </acl_config>
```

Anexo 3-4.1 /usr/local/etc/openca/access_control/node.xml.template

```
<openca>
  <access_control>
    <channel>
      <type>mod_ssl</type>
      <protocol>.*</protocol>
      <source>.*</source>
      <asymmetric_cipher>.*</asymmetric_cipher>
      <asymmetric_keylength>0</asymmetric_keylength>
      <symmetric_cipher>.*</symmetric_cipher>
      <symmetric_keylength>0</symmetric_keylength>
    </channel>

    <login>
      <type>none</type>
      <!--
        x509-base login:
        <type>x509</type>
        <chain>/usr/local/var/openca/crypto/chain</chain>

        passwd login:

        <type>passwd</type>
        <database>internal</database>
        <passwd>

          <user>
            <name>root</name>
```

```
            <algorithm>sha1</algorithm>
            <digest>3Hbp8MAAbo+RngxRXGbbujmC94U</digest>
            <role>CA Operator</role>
          </user>

          <user>...</user>
          ...
        </passwd>
```

Anexo 3-4.2 /usr/local/etc/openca/access_control/pub.xml.template

```
<user>
          <name>admin</name>
          <algorithm>sha1</algorithm>
          <digest>0DPiKuNIrrVmD8IUCuw1hQxNqZc</digest>
          <role>CA Operator</role>
        </user>
      </passwd>
    </login>

    <acl_config>
      <acl>yes</acl>
      <list>/usr/local/etc/openca/rbac/acl.xml</list>
      <command_dir>/usr/local/etc/openca/rbac/cmds</command_dir>
      <module_id>@ra_module_id@</module_id>
      <map_role>yes</map_role>
      <map_operation>yes</map_operation>
    </acl_config>

  </access_control>
  <token_config_file>/usr/local/etc/openca/token.xml</token_config_file>
</openca>
```

Anexo 3-4.3 /usr/local/etc/openca/access_control/ra.xml.template

[Anexo 3-5] Archivo de configuración del directorio /agreements

```
<span class="head3">Acuerdo de Certificado de Usuario</span><br>
<br>
<b>Acuerdo de Certificado de Usuario Final<br />
  (Nivel General de Fiabilidad)</b><br>
<br />

ESTE ACUERDO DE CERTIFICADO DE USUARIO FINAL (&amp;quot;Agreement&amp;quot;) es llevado a cabo entre @ca_organization@ (&amp;quot;@ca_organization@&amp;quot;) y un cierto solicitante de certificado (&amp;quot;Cliente&amp;quot;). En consideracion de las promesas en este Acuerdo, y con la intención de quedar vinculado legalmente, las partes acuerdan lo siguiente:
<br />
<br />

<pre>

DECLARACION DE PRACTICAS DE CERTIFICACION (CPS)
```

Los Servicios Públicos de Certificación de @ca_organization@ están regidos por la CPS de @ca_organization@.

Usted se compromete a utilizar el Certificado Digital y cualquier servicio prestado por la CA únicamente en acuerdo con la CPS. El mismo esta publicado en el sitio en Internet de la @ca_organization@, en el enlace @policy_link@

DERECHOS, OBLIGACIONES & COMPROMISOS DE @ca_organization@

@ca_organization@ provee garantías limitadas, renuncia a cualquier otra garantia, incluyendo garantias de comerciabilidad o idoneidad para un fin particular, limita y excluye de toda responsabilidad por cualquier incidente, consecuencia, y daños punitivos, como se indica en la CPS.

Toda la informacion provista por el suscriptor en esta aplicacion sera mantenida de forma confidencial y no sera divulgada a ninguna otra tercera parte a menos que:

* Sea autorizado por derecho escrito para ser usado para otros propositos; o

* La persona involucrada de su consentimiento por escrito para que sus datos sean usados para otros propositos.

DERECHOS, OBLIGACIONES & COMPROMISOS DEL SUSCRIPTOR

Usted deja por sentado el conocimiento y aceptación de los términos de este acuerdo, ya sea por el envío de solicitud de certificado digital, o el uso del mismo, lo que ocurra primero.

Notificación de Aceptación
La siguiente información será incorporada en su certificado digital generado por @ca_organization@:

El numero serial del certificado;
* el nombre del suscriptor;
* el nombre distintivo del suscriptor;
* la clave publica correspondiente a la clave privada;
* un identificador de los algoritmos con los cuales la clave publica del suscriptor esta destinada a ser usada;
* periodo de validación de los certificados;
* el nombre distintivo de @ca_organization@;
* un identificador del algoritmo(s) usado(s) para firmar el certificado;
* una declaración indicando la localización de la CPS de @ca_organization@, el método o procedimiento por el cual este puede ser obtenido, su forma y estructura, su autoría y su fecha

Anexo 3-5 /usr/local/etc/openca/agreements/general.html.template

[Anexo 3-6] Archivos de configuración del directorio /servers

```
## RA-node:
## --------
EXPORT_IMPORT_UP_DEVICE "/home/openca/openca.tar"
EXPORT_IMPORT_UP_START  ""
EXPORT_IMPORT_UP_STOP   ""
EXPORT_IMPORT_UP_EXPORT "/bin/tar -cvpf @__DEVICE__@ -C @__SRC__@ ."
EXPORT_IMPORT_UP_IMPORT "/bin/tar -xvf @__DEVICE__@ -C @__DEST__@"
EXPORT_IMPORT_UP_TEST   "/bin/tar -tvf @__DEVICE__@"
## you can use mountable devices like CD-RWs too
## states when the export from the database should be performed

EXPORT_IMPORT_MODULES
LOG_DOWNLOAD_DIR "/usr/local/var/openca/log/download"
LOG_ENROLL_DIR "/usr/local/var/openca/log/enroll"
LOG_RECEIVE_DIR "/usr/local/var/openca/log/receive"
LOG_UPLOAD_DIR "/usr/local/var/openca/log/upload"

ENROLL_CA_CERTIFICATE_STATES VALID
ENROLL_CERTIFICATE_STATES    VALID
ENROLL_CRL_STATES          VALID
ENROLL_CRR_STATES          ARCHIVED DELETED APPROVED SIGNED PENDING
NEW
ENROLL_CSR_STATES          ARCHIVED DELETED
ENROLL_MAIL_STATES

RECEIVE_CRR_STATES  PENDING NEW
RECEIVE_CSR_STATES  PENDING RENEW NEW

DOWNLOAD_CA_CERTIFICATE_STATES VALID
DOWNLOAD_CERTIFICATE_STATES    VALID
DOWNLOAD_CRL_STATES          VALID
DOWNLOAD_CRR_STATES          ARCHIVED DELETED APPROVED
DOWNLOAD_CSR_STATES          ARCHIVED DELETED
DOWNLOAD_MAIL_STATES         CRINS DEFAULT
```

Anexo 3-6.1 /usr/local/etc/openca/servers/node.conf.template

```
## ================== [ End General Section ] ========================

## ==================== [ Requests Section ] ========================

## The Supported Requests option will let you choose which requests
## are supported on your system

SupportedRequests "BrowserRequest" "ServerRequest"
.
.
## These are the options for the default Browser request

BrowserRequestConfig "/usr/local/etc/openca/browser_req.xml"
BrowserRequestCommand "advanced_csr"
BrowserRequestTitle "Peticion de Certificado de Navegador"
BrowserRequestDescription "Forma de Peticion con deteccion automatica de navegador"

## These are the options for the default Server request

ServerRequestConfig "/usr/local/etc/openca/server_req.xml"
```

```
ServerRequestCommand "pkcs10_req"
ServerRequestTitle "Peticion de Certificado de Servidor"
ServerRequestDescription "Subir Formulario de Peticion en formato PKCS#10 PEM"
.
.
SupportedKeyStrengths    "Weak" "Base" "Strong" "Advanced" "Strongest"

## Default Registration Authorities List

RegistrationAuthority "RA-UTPL"

## Minimum Length for the PIN used by the user to authenticate the
## request (in case of Server-Side key generation, this is also the
## Password that will be used to encrypt the private key - and also
## used to retrieve it)

MinPinLength                10

## ================== [ End Requests Section ] ========================
```

Anexo 3-6.2 /usr/local/etc/openca/servers/pub.conf.template

```
## Crypto Section
## ==============

openssl             "/usr/bin/openssl"
sslconfig           "/usr/local/etc/openca/openssl/openssl.cnf"
OCSPindex           "/usr/local/var/openca/crypto/ocsp_index.txt"
MakePath            "/usr/bin/make -s"

## General Section
## ===============

DEFAULT_LANGUAGE "es_ES"
DEFAULT_CHARSET  "UTF-8"

CgiLibPath                  "/usr/local/lib/openca/functions"
CgiServerType               "ra"
CgiServerName               "ra"
HtdocsUrlPrefix             "/pki/ra"
EtcPrefix                   "/usr/local/etc/openca"
SessionDir     /usr/local/var/openca/session/cookie
SessionLifetime 1200
ModuleID          1
ModuleShift       13
AccessControlConfiguration "/usr/local/etc/openca/access_control/ra.xml"
SoftwareConfiguration     "/usr/local/etc/openca/config.xml"
RoleConfiguration         "/usr/local/etc/openca/rbac/roles.xml"
ModuleConfiguration       "/usr/local/etc/openca/rbac/modules.xml"
TokenConfiguration        "/usr/local/etc/openca/token.xml"
LogConfiguration          "/usr/local/etc/openca/log.xml"
MenuConfiguration         "/usr/local/etc/openca/menu.xml"
LOAConfiguration          "/usr/local/etc/openca/loa.xml"

# New Browser Configuration

BrowserRequestConfig      "/usr/local/etc/openca/browser_req.xml"
```

```
DBmodule        "DBI"
CertDir         "/usr/local/var/openca/crypto/certs"
TempDir         "/usr/local/var/openca/tmp"
MaxReturnedItems 20

## ==================== [ LOA Support ] ========================
## USE_LOAS takes either YES or NO

USE_LOAS            "yes"
```

Anexo 3-6.3 /usr/local/etc/openca/servers/ra.conf.template

[Anexo 3-7] Archivo de configuración config.xml

```
<!-- =============== -->
<!-- general options -->
<!-- =============== -->
<option>
<name>default_language</name>
<value>es_ES</value>
</option>

<option>
<name>default_charset</name>
<value>UTF-8</value>
</option>

<option>
<!--
.
.
<name>organization</name>
<value>UTPL</value>
</option>

<option>
<name>ca_organization</name>
<value>CA-UTPL</value>
</option>

<option>
<name>ca_locality</name>
<value>Loja</value>
</option>

<option>
<name>ca_state</name>
<value>Loja</value>
</option>

<option>
<name>ca_country</name>
<value>EC</value>
</option>

<option>
```

```
<name>sendmail</name>
<value>/usr/lib/sendmail -n -t </value>
</option>

<option>
<name>send_mail_automatic</name>
<value>yes</value>
</option>

<option>
<name>service_mail_account</name>
<value>beleon@utpl.edu.ec</value>
</option>

<option>
<name>policy_link</name>
<value>https://repo.utpl.edu.ec/pki/pub/policy.html</value>
</option>
<!-- ======================== -->
<!-- web server configuration -->
<!-- ======================== -->
<option>
<name>httpd_protocol</name>
<value>https</value>
</option>

<option>
<name>httpd_host</name>
<value>repo.utpl.edu.ec</value>
</option>

<option>
<name>httpd_port</name>
<value>:443</value>
</option>
.
.
<!-- ====================== -->
<!-- database configuration -->
<!-- ====================== -->
<option>
<name>dbmodule</name>
<value>DBI</value>
</option>

<option>
<name>db_type</name>
<value>mysql</value>
</option>

<option>
<name>db_name</name>
<value>openca</value>
</option>

<option>
<name>db_host</name>
<value>localhost</value>
```

```
</option>

<option>
<name>db_port</name>
<value>3306</value>
</option>

<option>
<name>db_user</name>
<value>openca_ur</value>
</option>

<option>
<name>db_passwd</name>
<value>raopenca</value>
</option>
```

Anexo 3-7 /usr/local/etc/openca/config.xml

[Anexo 3-8] Archivo de configuración browser-req.xml

```
<input>
<name>cn</name>
<label>Nombre de Usuario</label>
<type>textfield</type>
<charset>UTF8_LETTERS</charset>

<value>
$ADDITIONAL_ATTRIBUTE_FIRSTNAME $ADDITIONAL_ATTRIBUTE_LASTNAME
</value>
<minlen>3</minlen>
<required>YES</required>
</input>

<input>
<name>ou</name>
<label>Grupo de Peticion de Certificado</label>
<type>select</type>
<charset>UTF8_MIXED</charset>
<value>Users</value>
<value>Employees</value>
<value>Partners</value>
<value>Applications</value>
<minlen>5</minlen>
<required>YES</required>
</input>
</dn>

<subjectAltNames>
<name>Caracteristicas Avanzadas</name>

<input>
<name>EMAIL_ATTRIBUTE_0</name>
<label>E-Mail</label>
```

```
<type>textfield</type>
<charset>EMAIL</charset>
<value>$ADDITIONAL_ATTRIBUTE_EMAIL</value>
<minlen>3</minlen>
<required>YES</required>

<!--
 Value Type specifies the type of value that is present
          in this field. The possible value types are the ones
          supported by OpenSSL. Most commonly used are:
          - email
                    - otherName
          - IP
                    - DNS
                    - DirName
                    - RID
                    - URI
-->
<valueType>email</valueType>
</input>

<!--
 You can add many different input here such an IP address
        or a DNS name for the subject alt name field
-->

<input>
<name>OTHER_NAME_1</name>
<label>Identificador de Usuario (opcional)</label>
<type>textfield</type>
<charset>UTF8_MIXED</charset>
<value>$ADDITIONAL_ATTRIBUTE_UID</value>
<minlen>0</minlen>
<required>NO</required>
<valueType>otherName</valueType>

<!--
 This OID is for the M$ Global User Identifier (GUID)
-->
<prefix>1.3.6.1.4.1.311.25.1;UTF8:</prefix>
</input>

<!--
      <input>
       <name>OTHER_NAME_1</name>
       <label>IP Address (for servers only)</label>
       <type>textfield</type>
       <charset>IPV4_ADDRESS</charset>
       <value>0.0.0.0</value>
       <minlen>7</minlen>
       <required>NO</required>
            <valueType>IP</valueType>
      </input>
-->
</subjectAltNames>

<details>
<name>Detalles Adicionales</name>
```

```
<input>
<name>role</name>
<label>Tipo de Certificado</label>
<type>select</type>
<charset>UTF8_LETTERS</charset>
<value>$EXEC::loadRoles()</value>
<minlen>2</minlen>
<required>YES</required>
</input>

<input>
<name>ra</name>
<label>Seleccionar Autoridad de Registro</label>
<type>select</type>
<charset>UTF8_LETTERS</charset>
<value>$CONFIG::RegistrationAuthority</value>
<minlen>5</minlen>
<required>YES</required>
</input>

</details>
<extras>
<name>Acuerdo de Politica de Usuario</name>

<input>
<name>loa</name>
<label>Nivel de Fiabilidad</label>
<info img="bulb.png">?cmd=viewLoas</info>
<type>select</type>
<charset>UTF8_LETTERS</charset>
<value>$EXEC::loadLoa()</value>
<minlen>1</minlen>
<required>YES</required>
</input>

<input>
<name>genkey</name>
<label>Modo de Generacion de Clave</label>
<type>select</type>
<charset>LATIN1_LETTERS</charset>
<value>Browser (Your Computer)</value>
<value>Server (Our Server)</value>
<!--   <value>$EXEC::loadKeygenMode()</value> -->
<minlen>3</minlen>
<required>YES</required>
</input>
</extras>
</certificate>
<!-- Key Generation Details -->

<keygen>

<key>
<name>Detalles de Generacion de Clave</name>

<input>
<name>keytype</name>
```

```
<label>Algoritmo de Firma</label>
<type>select</type>
<charset>LATIN1_LETTERS</charset>
<value>$EXEC::loadKeyTypes()</value>
<minlen>3</minlen>
<required>YES</required>
</input>

<input>
<name>strength</name>
<label>Nivel de la Clave</label>
<type>select</type>
<charset>UTF8_LETTERS</charset>
<value>$EXEC::loadKeyStrengths()</value>
<minlen>0</minlen>
<required>NO</required>
</input>
</key>

<pin>
<name>PIN de Verificacion de Peticion</name>

<input>
<name>passwd1</name>

<label>
PIN (Minimo 5 caracteres) <br />
        [verifica la peticion de certificado]
</label>
<errlabel>PIN</errlabel>
<type>password</type>
<charset>UTF8_LETTERS</charset>
<value/>
<minlen>5</minlen>
<required>YES</required>
</input>

<input>
<name>passwd2</name>

<label>
PIN (Minimo 5 caracteres) <br />
        [ingresar nuevamente para comprobacion]
</label>
<errlabel>PIN (verify)</errlabel>
<type>password</type>
<charset>UTF8_LETTERS</charset>
<value/>
<minlen>5</minlen>
<required>YES</required>
</input>
</pin>
</keygen>
```

Anexo 3-8 /usr/local/etc/openca/browser_req.xml

[Anexo 3-9] Archivo de configuración loa.xml

```
<loa>
<level>2</level>
<name>Medium</name>
–
<description>

   Este nivel de seguridad es usado por usuarios y servidores.

</description>
<agreement>/usr/local/etc/openca/agreements/general.html</agreement>
<!-- Requirements section for this level of Assurance -->

<!--
 Supported Checks:
      =================
      * algorithm - list of accepted algorithms for this request
      * keygen - key generation mode (e.g., server or browser)
  -->
<requires>
<!--
 Algorithm:
       * name - name of the algorithm (eg., rsa, dsa, ecdsa, .. )
       * keysize - minimum number of bits for the algorithm
-->
<strength>
<name>Base</name>
<allowed>RSA+1024</allowed>
<allowed>DSA+1024</allowed>
<allowed>ECDSA+224</allowed>
</strength>

<strength>
<name>Strong</name>
<allowed>RSA+2048</allowed>
<allowed>DSA+2048</allowed>
<allowed>ECDSA+256</allowed>
</strength>

<strength>
<name>Advanced</name>
<allowed>RSA+4096</allowed>
<allowed>ECDSA+384</allowed>
</strength>

<!--
    <strength>
          <name>Strongest</name>
          <allowed>RSA+8192</allowed>
          <allowed>ECDSA+521</allowed>
    </strength>
-->
<!--
 Keygen:
       * mode - generation mode (eg., Browser or Server)
       If omitted, any key generation mode (Browser or Server)
       is accepted.
```

```
-->
<keygen>
<mode>Browser (Your Computer)</mode>
<mode>Server (Our Systems)</mode>
</keygen>
</requires>

<cert>
<ext>
<name>certificatePolicies</name>
<!--
 list all the policy OIDs here that are below
        and equevilant to this level of assurance for example
        loa basic has policy oid 1.2.3.4 , and basic is
        higher than test and rudimentary and basic, so the
        line would look like this
          <CP>
            <value>1.2.3.1</value>
            <value>1.2.3.3.5</value>
            <value>@psec</value>
          <CP>
        ..... where
        1.2.3.1 is the oid for test loa and 1.2.3.2 is for
        Rudimantary. you get the picture NOTE they must be
        COMMA separated
-->
<CP>
<value>1.2.3.3.4</value>
<value>1.2.3.3.5</value>
<value>1.2.3.3.6</value>
</CP>

<section>
<name>psec</name>
<policy_ID_tag> policyIdentifier</policy_ID_tag>

<CPS>
<URI>
CPS.1 ="https://repo.utpl.edu.ec/pki/pub/policy.html"
</URI>
</CPS>
</section>
</ext>
</cert>
</loa>
```

Anexo 3-9 /usr/local/etc/openca/loa.xml

[Anexo 3-10] Archivo de configuración server_req.xml

```
DN_TYPE_PKCS10_REQUIRED_ELEMENTS "CN" "OU" "O" "C"
DN_TYPE_PKCS10_BASE    "O" "C"

## YES, EXIST, NO

DN_TYPE_PKCS10_ENFORCE_BASE "EXIST"
```

```
DN_TYPE_PKCS10_BASE_1 "UTPL"
DN_TYPE_PKCS10_BASE_2 "EC"

ADDITIONAL_REQUEST_ATTRIBUTES  "requestercn" "email" "department" "telephone"
ADDITIONAL_ATTRIBUTES_DISPLAY_VALUE  "Nombres y Apellidos" "Email" "Departamento"
"Telefono"
ADDITIONAL_REQUEST_ATTRIBUTES_STRING_TYPE "LATIN1_LETTERS" "EMAIL" "LATIN1_LETTERS"
"LATIN1_LETTERS"
```

Anexo 3-10 /usr/local/etc/openca/server_req.xml

[Anexo 3-11] Archivo de configuración del directorio /access_control (en la CA)

```
<openca>
<access_control>
<channel>
<type>mod_ssl</type>
<protocol>.*</protocol>
<source>.*</source>
<asymmetric_cipher>.*</asymmetric_cipher>
<asymmetric_keylength>0</asymmetric_keylength>
<symmetric_cipher>.*</symmetric_cipher>
<symmetric_keylength>0</symmetric_keylength>
</channel>
<login>
<type>passwd</type>
<!--
        x509-base login:
        <type>x509</type>
        <chain>/usr/local/var/openca/crypto/chain</chain>

        passwd login:
        <type>passwd</type>
        <database>internal</database>
        <passwd>
          <user>
            <name>root</name>
            <algorithm>sha1</algorithm>
            <digest>3Hbp8MAAbo+RngxRXGbbujmC94U</digest>
            <role>CA Operator</role>
          </user>
          <user>...</user>
          ...
        </passwd>
        no authentication:
        <type>none</type>
-->
<database>internal</database>
<passwd>
<user>
<name>root</name>
<algorithm>sha1</algorithm>
<digest>3Hbp8MAAbo+RngxRXGbbujmC94U</digest>
<role>CA Operator</role>
</user>
```

```
<user>
<name>mysecret11</name>
<algorithm>sha1</algorithm>
<digest>9FKQ/uv5yAcjUoxfCnncepSopx4</digest>
<role>CA Operator</role>
</user>
</passwd>
</login>

<acl_config>
<acl>yes</acl>
<list>/usr/local/etc/openca/rbac/acl.xml</list>
<command_dir>/usr/local/etc/openca/rbac/cmds</command_dir>
<module_id>3</module_id>
<map_role>yes</map_role>
<map_operation>yes</map_operation>
</acl_config>

<session>
<directory>/usr/local/var/openca/session/cookie</directory>
</session>
</access_control>
<token_config_file>/usr/local/etc/openca/token.xml</token_config_file>
</openca>
```

Anexo 3-11 /usr/local/etc/openca/access_control/(ca.xml y node.xml)

[Anexo 3-12] Archivo de configuración del directorio /servers (en la CA)

```
## CA-node:
## --------

EXPORT_IMPORT_DOWN_DEVICE "openca.tar"
EXPORT_IMPORT_DOWN_START  ""
EXPORT_IMPORT_DOWN_STOP   ""
EXPORT_IMPORT_DOWN_EXPORT "/bin/tar -cvpf /usr/local/var/openca/tmp/@__DEVICE__@ -C
@__SRC__@ ." "/usr/bin/scp /usr/local/var/openca/tmp/@__DEVICE__@
openca@172.16.50.71:/home/openca/@__DEVICE__@" "rm
/usr/local/var/openca/tmp/@__DEVICE__@"
EXPORT_IMPORT_DOWN_IMPORT "/usr/bin/scp openca@172.16.50.71:/home/openca/@__DEVICE__@
/usr/local/var/openca/tmp/@__DEVICE__@" "/bin/tar -xvf /usr/local/var/openca/tmp/@__DEVICE__@
-C @__DEST__@" "rm /usr/local/var/openca/tmp/@__DEVICE__@"
EXPORT_IMPORT_DOWN_TEST   ""
```

Anexo 3-1 /usr/local/etc/openca/servers/node.conf)

[Anexo 3-13] Manual del Administrador (archivo anexo)

[Anexo 3-14] Guía de Usuario (archivo anexo)

[Anexo 3-15] Manual de Procedimientos (archivo anexo)

Anexo 4

Anexo [4-1] Importar certificado CA-UTPL raíz en:

Navegador Mozilla Firefox

En este navegador, se puede obtener el certificado digital de la Autoridad Certificadora CA-UTPL:

- Seleccionando el formato CRT, se presenta una ventana indicándole al usuario que se trata de una nueva Autoridad Certificadora y si desea confiar en ella. Además se muestran las opciones de confianza del certificado. Habilitamos por lo menos las dos primeras opciones (identificar sitios web y usuarios de correo). De esta manera el certificado aparecerá instalado automáticamente en el navegador Mozilla Firefox. Ver la figura 4-1.

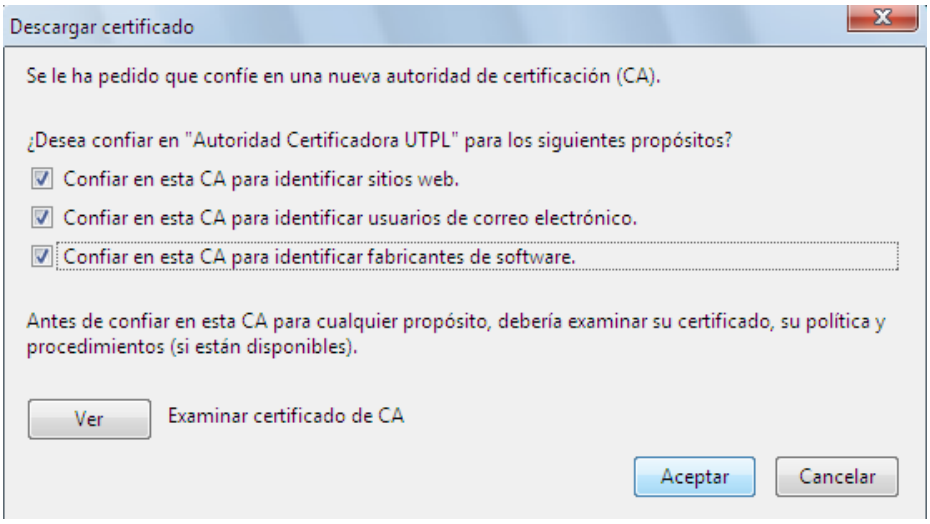


Fig. 4-1. Instalación del certificado de CA-UTPL en el navegador Mozilla Firefox

Podemos comprobar que la instalación ha sido exitosa accediendo al menú *Herramientas/Opciones/Avanzadas/Encriptación/Ver Certificados*. En la etiqueta *Autoridades* debe estar presente el certificado de la CA-UTPL.

- Descargando el certificado raíz de CA-UTPL en formato DER, este tipo de formato presenta el certificado como un archivo, se procede entonces a descargarlo en cualquier sitio del computador para posteriormente instalarlo en el navegador de la siguiente manera:

    - Se accede a *Herramientas/Opciones/Avanzadas/Encriptación/Ver Certificados*. En la etiqueta *Autoridades*, en la parte inferior seleccionamos *Importar*, localizamos el archivo descargado anteriormente y damos click en *Abrir.*

    - Para comprobar que en efecto se ha instalado el certificado, se procede igual que lo realizado para el formato CRT.

Luego de haber instalado el certificado raíz, debemos modificar las opciones de confianza del mismo, de otra forma seria como no haberlo instalado. Para ello se selecciona el certificado instalado y se da click en la pestaña *Editar*. Posteriormente habilitamos por lo menos las dos primeras opciones (identificar sitios web y usuarios de correo). De esta forma el certificado raíz queda correctamente instalado.

Navegador Internet Explorer

Para este navegador están disponibles los certificados raíz de CA-UTPL en formato CRT, CER y DER, cualquiera sea el tipo que se seleccione, el navegador pedirá guardar el certificado en algún sitio del computador para su posterior instalación.

Una vez guardado, se puede instalar el certificado de dos formas:

- Dando doble click en el certificado. A continuación se mostrará una ventana presentando información acerca del certificado. Al presionar la opción de *Instalar el certificado*, se iniciará un asistente que ayuda a completar el proceso. Se debe seleccionar las opciones predeterminadas y al final se mostrará un mensaje indicando la correcta instalación del certificado.

- Dirigiéndose a Herramientas/Opciones de Internet/Contenido/Certificados/Autoridades Certificadoras Raíz de Confianza, seleccionar la opción Importar en la parte inferior, se iniciará el mismo asistente que en el paso anterior.

Se comprueba que efectivamente el certificado se encuentra instalado en el navegador Internet Explorer en la opción *Herramientas/Opciones de Internet/Contenido/Certificados/Entidades Emisoras Raíz de Confianza*; mostrando el certificado instalado.

Navegador Opera

En el caso del navegador Opera, se puede descargar e instalar el certificado raíz de CA-UTPL en los formatos CRT y DER. Al igual que para Mozilla Firefox, el predeterminado es el formato CRT. Se mostrará una ventana de instalación automática del certificado que permitirá integrar el certificado de CA-UTPL a los de las Autoridades Raíz del navegador.

Se puede comprobar la correcta instalación del certificado dirigiéndose a *Herramientas/Opciones/Avanzado/Seguridad/Administrar Certificados/De Autoridades*.

Anexo [4-2] Instalación de certificados de usuario y de la Autoridad raíz CA-UTPL en:

Mozilla Thunderbird.

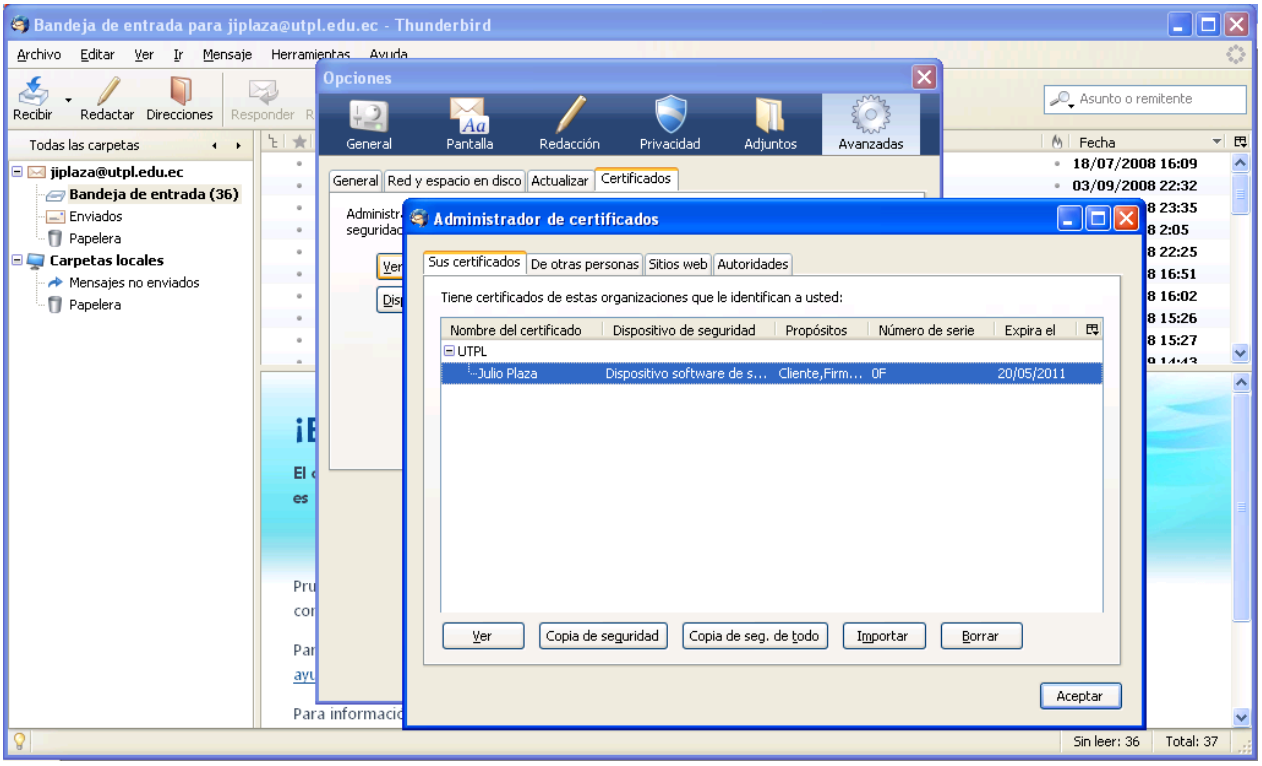
Descargar el instalador de Mozilla Thunderbird de **[14]**

Se tomó como referencia información de **[15]**

- **Instalación del certificado de usuario**

El usuario, dentro del cliente de correo Mozilla Thunderbird, debe ir a **Herramientas -> Opciones -> Avanzadas.** En la etiqueta **Certificados**, dar click en **Ver Certificados.** En la parte superior seleccionamos la etiqueta **Sus Certificados**, y luego damos click en la parte inferior en **Importar**. Una vez localizado el archivo que contiene el certificado digital de usuario (extensión **p12**) damos click en **Abrir.** Se debe introducir la contraseña de seguridad del certificado, misma que se usará cuando vayamos a enviar mensajes firmados digitalmente desde Mozilla Thunderbird.

Por último se debe dar click en **Aceptar.** Quedará de esta forma importado el certificado digital en el cliente de correo



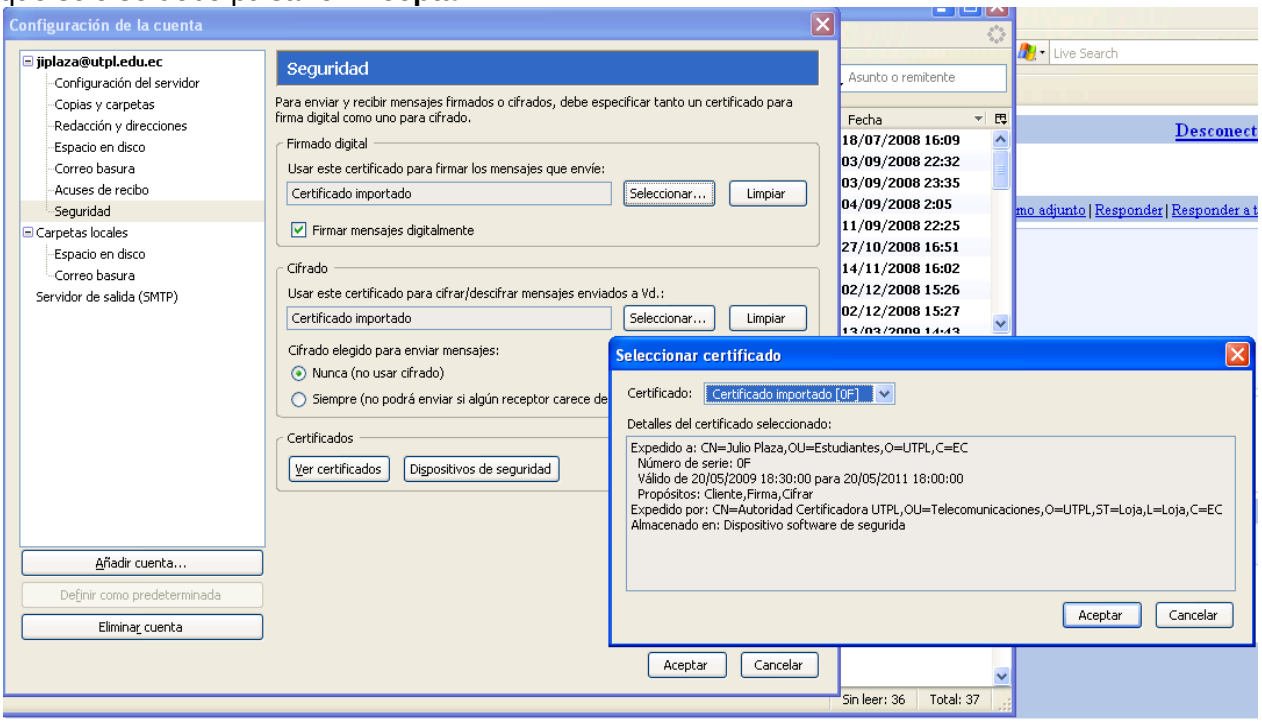
- **Instalación del certificado de la Autoridad Certificadora CA-UTPL**

Para importar el certificado de la Autoridad Certificadora CA-UTPL, el proceso es similar al de importación de certificado de usuario, únicamente en la parte superior se selecciona **Autoridades** en lugar de Sus Certificados, y al dar click en **Importar**, buscamos el archivo ***cacert.der*** de CA-UTPL que tenemos guardado en el computador.

- **Habilitar el certificado de usuario instalado para firma digital**

Para ello se debe seleccionar el certificado digital que acabamos de adjuntar. Acceder a **Herramientas -> Configuración de la cuenta**. En la parte izquierda, en la cuenta del usuario, dar click en **Seguridad**.

En la sección **Firmado Digital** pulsamos **Seleccionar.** Se abrirá una nueva ventana en donde aparecerá seleccionada la firma digital que el usuario instaló anteriormente, por lo que solo se debe pulsar en **Aceptar**.



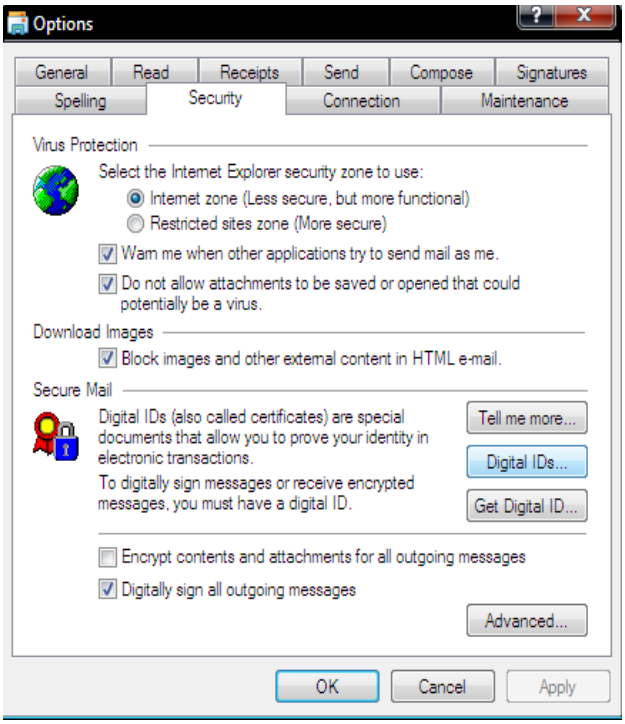
Hacemos lo mismo en la parte de **Cifrado**, pulsamos **Seleccionar** y de esta manera adjuntamos el mismo certificado de usuario para cifrar la información que enviemos.

Outlook Express

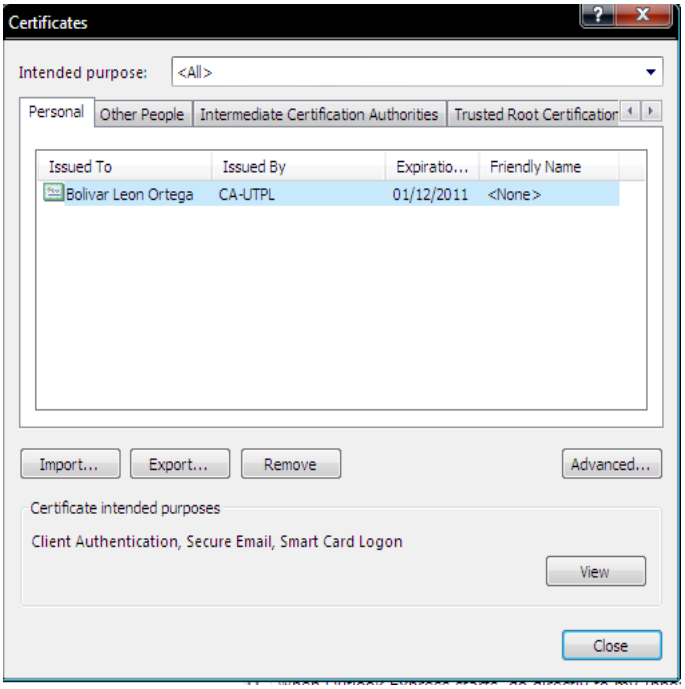
- **Instalación del certificado de usuario**

Ir a **Herramientas (Tools)** -> **Opciones (Options)**

En la etiqueta **Seguridad (Security)**, esta la sección **Correo Seguro (Secure Mail)**. Dar clic en **Digital IDs**



Dentro de la etiqueta **Personal,** damos clic en **Importar (Import)**. Seleccionamos el certificado que aparece por defecto y damos clic en **Aceptar.**

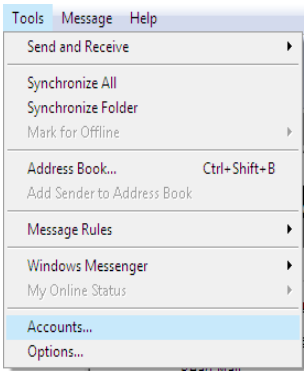


- **Instalación del certificado raíz de CA-UTPL**

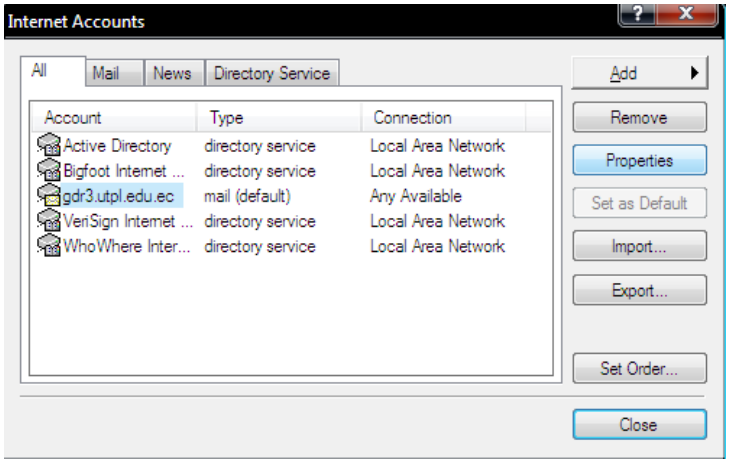
En lugar de ubicarse en la etiqueta **Personal**, nos dirigimos a **Autoridades de Certificación raíz confiables (Trusted Root Certification Authorities)** y desde ahí importamos el certificado raíz de CA-UTPL que se tiene almacenado.

- **Habilitar el certificado de usuario instalado para firma digital**

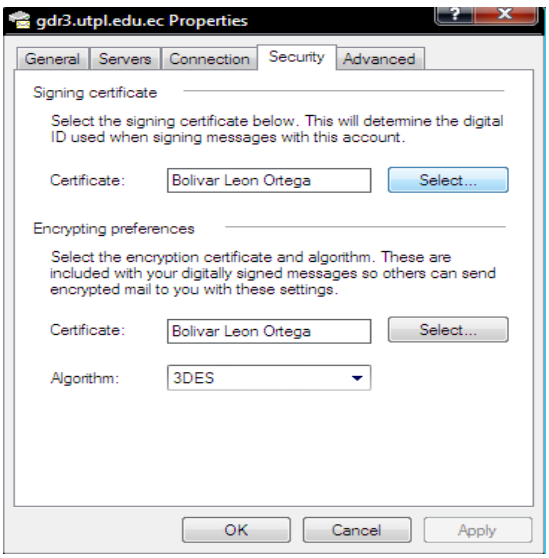
Ir a **Herramientas (Tools)** -> **Cuentas (Accounts)**



Seleccionar la cuenta que hemos configurado y dar clic en **Propiedades (Properties)**



En la siguiente ventana dar clic en **Seguridad (Security)**. Junto al parámetro **Certificado de Firma (Signing certificate)** se encuentra el botón **Seleccionar**. Al darle clic aparece el certificado de usuario predeterminado que usaremos para realizar el proceso de firma, lo seleccionamos. Igual proceso hacemos para el certificado de **Encriptación (Encrypting preferences).**

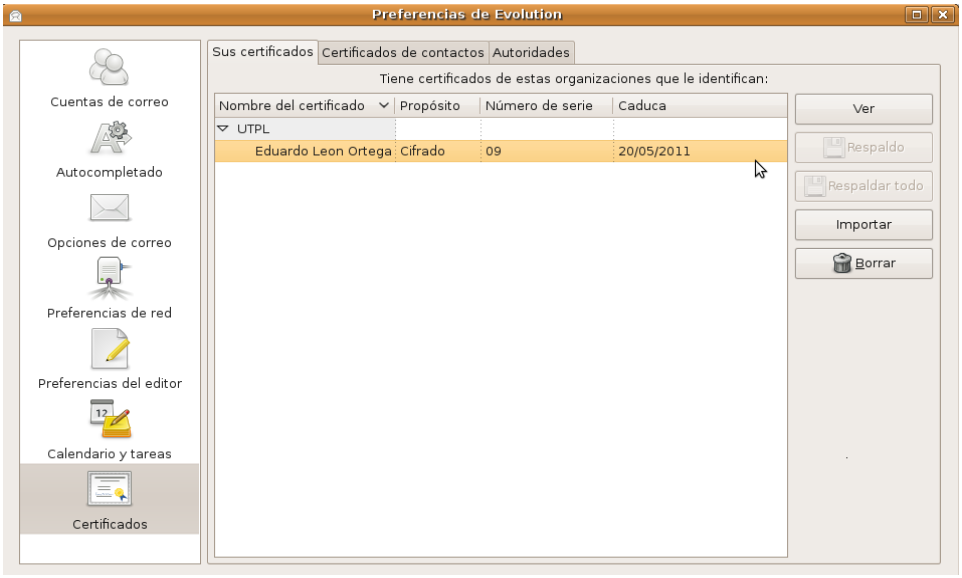


Evolution

El proceso es similar al de Mozilla Thunderbird.

- **Instalación del certificado de usuario**

Una vez dentro del cliente de mensajería, nos ubicamos en **Editar-> Preferencias.** En la parte inferior izquierda seleccionamos **Certificados.** En la pestaña **Sus certificados** damos click en **Importar.** Ubicamos el certificado de usuario con extensión *p12*, damos click en **Aceptar** y de esta forma el certificado ha sido importado al servidor de correo.

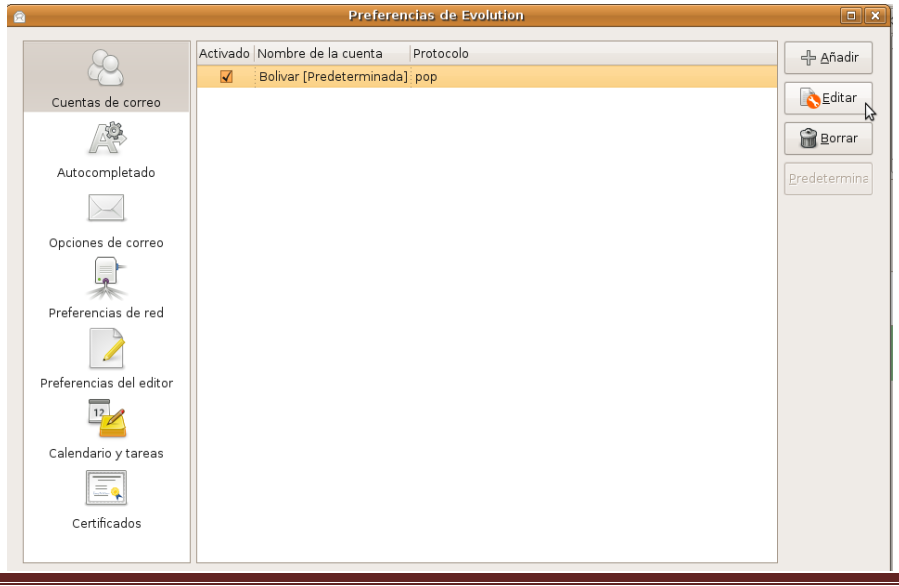


- **Instalación del certificado de CA-UTPL**

En lugar de la pestaña Sus certificados seleccionamos **Autoridades.** A continuación se da click en **Importar** para adjuntar el certificado *cacert* con extensión crt, cer o der.

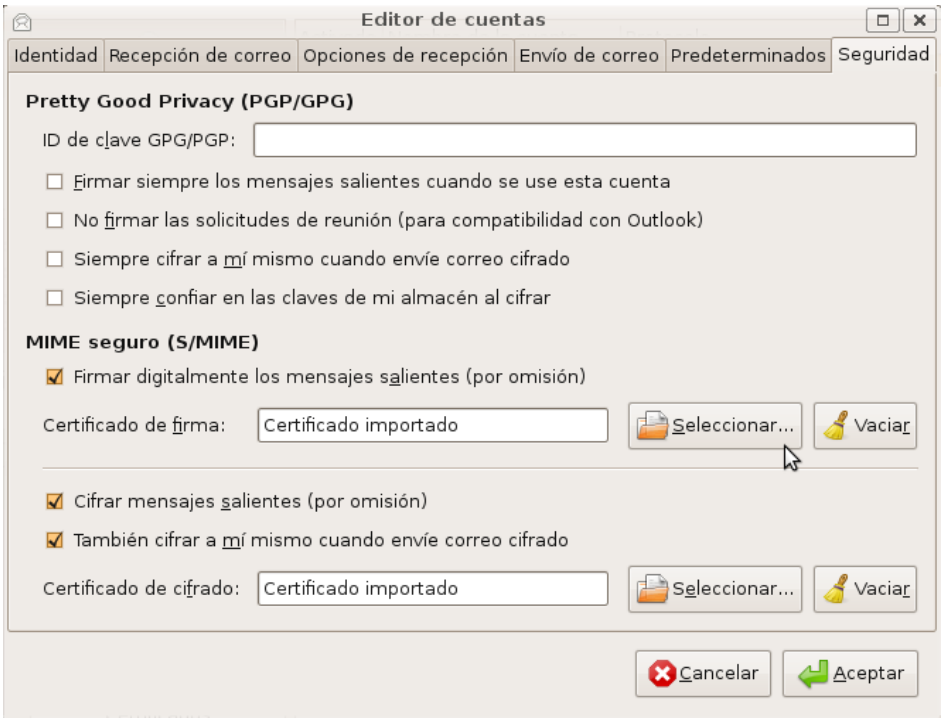
- **Habilitar el certificado de usuario para firma digital**

En la etiqueta **Editar-> Preferencias**, seleccionamos en la parte superior izquierda la etiqueta **Cuentas de Correo**. Ubicamos nuestra cuenta y damos click en **Editar**.



En la parte superior escogemos la etiqueta **Seguridad**. Ubicamos la sección **MIME Seguro (S/MIME)** y presionamos **Seleccionar**, tanto para *Firmar digitalmente los mensajes salientes* como para *Cifrar los mensajes salientes.*

En ambos casos se trata del mismo certificado de usuario, por lo que solamente se debe dar click en **Aceptar**. De esta manera se pueden firmar y cifrar mensajes en este cliente de correo.



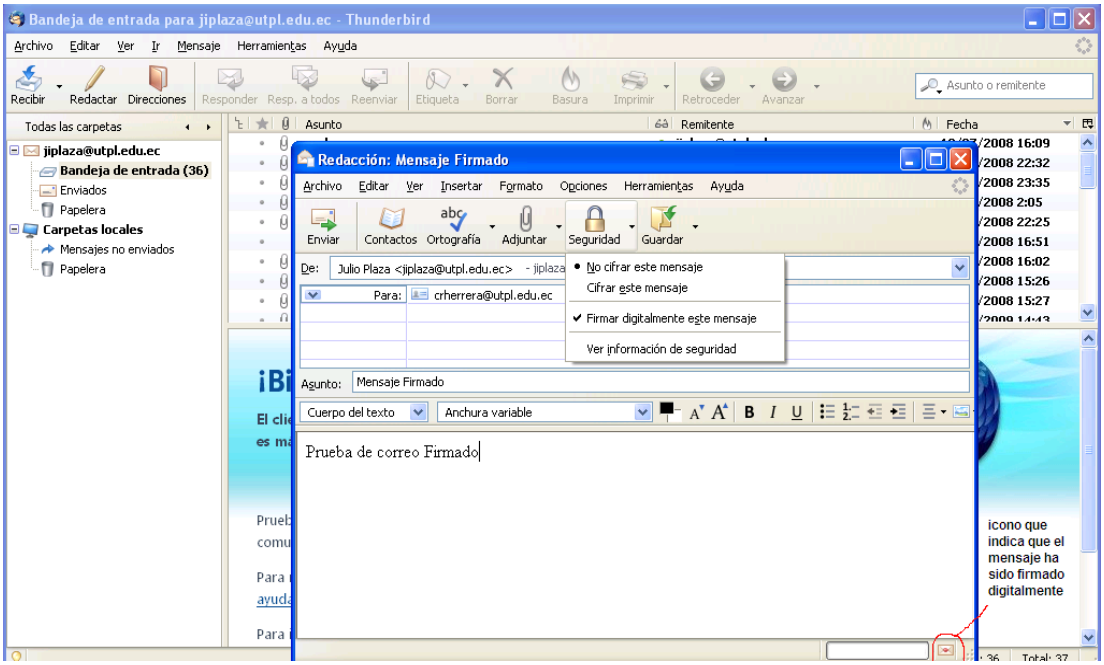
Anexo [4-3] Firma digital utilizando el cliente de correo:

Mozilla Thunderbird

- **Envío de un correo firmado digitalmente**

Se tomó información de **[16]**

Para escribir un mensaje de correo firmado, dentro del cliente de correo Thunderbird se debe pulsar en **Redactar** para crear un nuevo mensaje. Para firmarlo digitalmente basta con pulsar en la flecha que hay justo a la derecha del botón **Seguridad** y marcar la casilla **Firmar digitalmente este mensaje**. Sabremos que ha sido firmado porque en la esquina inferior derecha de la ventana de redacción, aparecerá una imagen de un sobre.

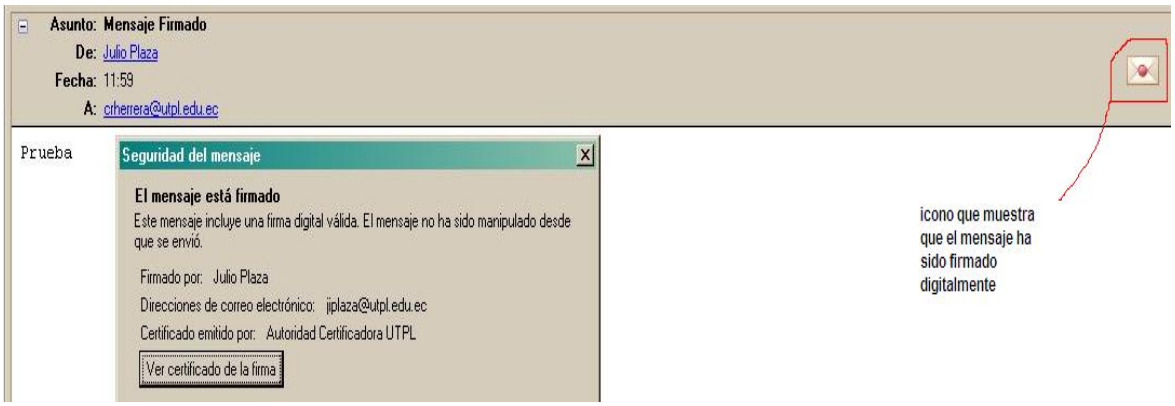


Para cifrar el mensaje, en el mismo botón **Seguridad** únicamente hay que habilitar la opción **Cifrar este mensaje**, y de esta manera el mensaje también viajará cifrado.

- **Recepción de mensajes firmados digitalmente**

Cuando un usuario de certificado digital de CA-UTPL envíe un mensaje firmado digitalmente a otro usuario, para que éste pueda comprobar la validez de dicha firma, es necesario que el receptor tenga instalado en su programa cliente de correo (en este caso Thunderbird), el certificado digital de la entidad emisora del certificado con el que el mensaje ha sido firmado, es decir, el certificado digital de la Autoridad Certificadora CA-UTPL.

Una vez llegado el mensaje, el receptor puede constatar que efectivamente el mensaje ha sido firmado por el emisor al dar click sobre el icono de sobre ubicado en la parte derecha del asunto del mensaje.

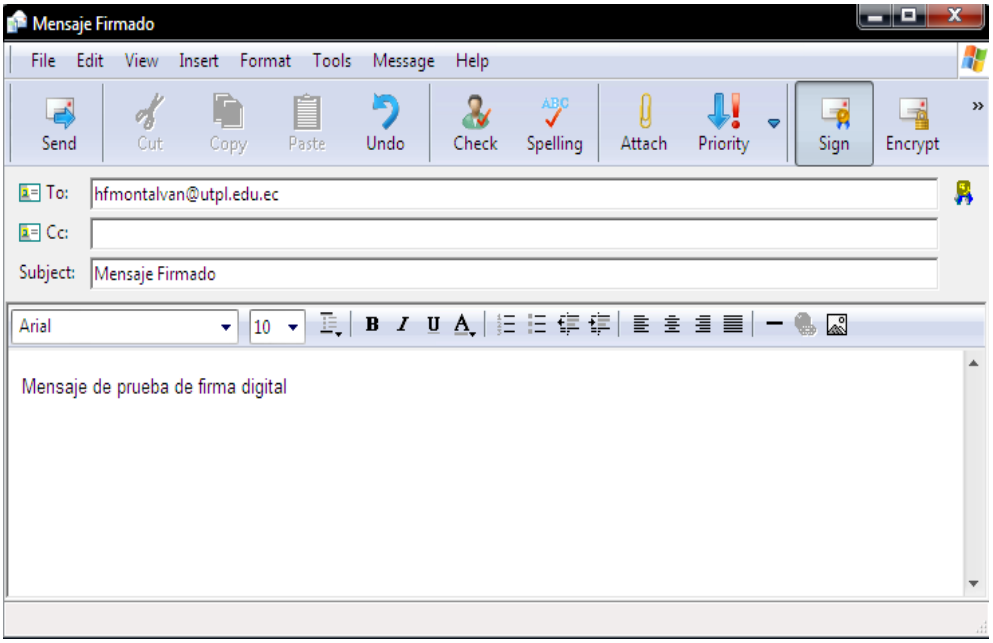


Outlook Express

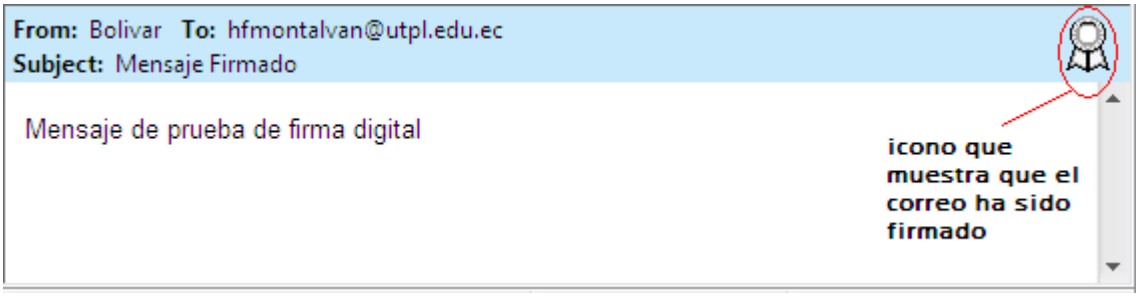
- **Envío de un correo firmado digitalmente**

Dentro del cliente de correo Outlook Express, seleccionamos **Crear Correo (Create Mail).**

Nos aparece la sección en donde escribimos nuestro correo, junto con el destinatario y el asunto. Luego de que hayamos redactado el mail, en la parte superior derecha del panel seleccionamos **Firmar (Sign)** para firmar digitalmente el correo; y **Encriptar (Encrypt)** en caso de que lo queramos encriptar.



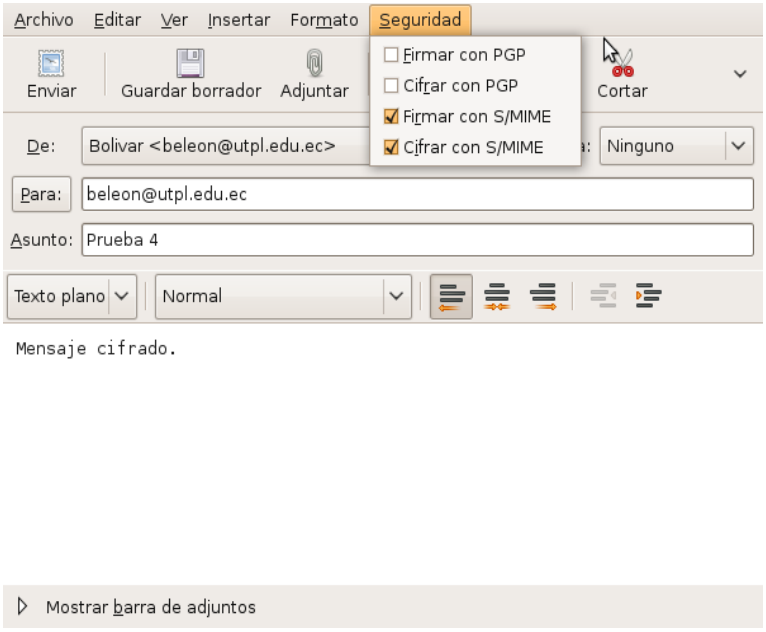
El receptor observará así su mensaje:



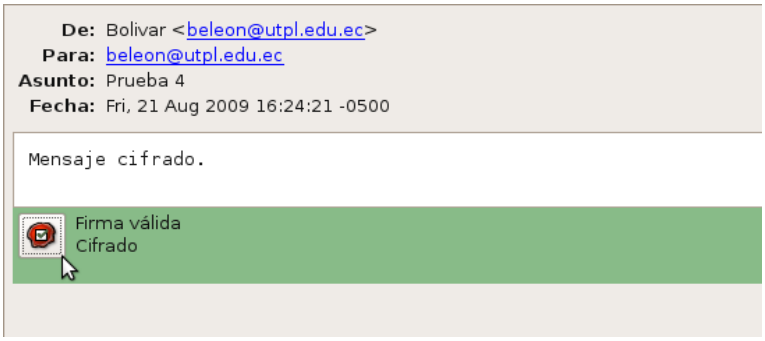
Anexo [4-4] Firmado y Cifrado de datos utilizando el cliente de correo:

Evolution.

Para firmar y cifrar un mensaje en Evolution, primeramente componemos uno. Para ello damos click en **Nuevo-> Componer**. Una vez redactado, seleccionamos la etiqueta **Seguridad** activamos las opciones **Firmar con S/MIME y Cifrar con S/MIME**. Posteriormente damos click en **Enviar**.

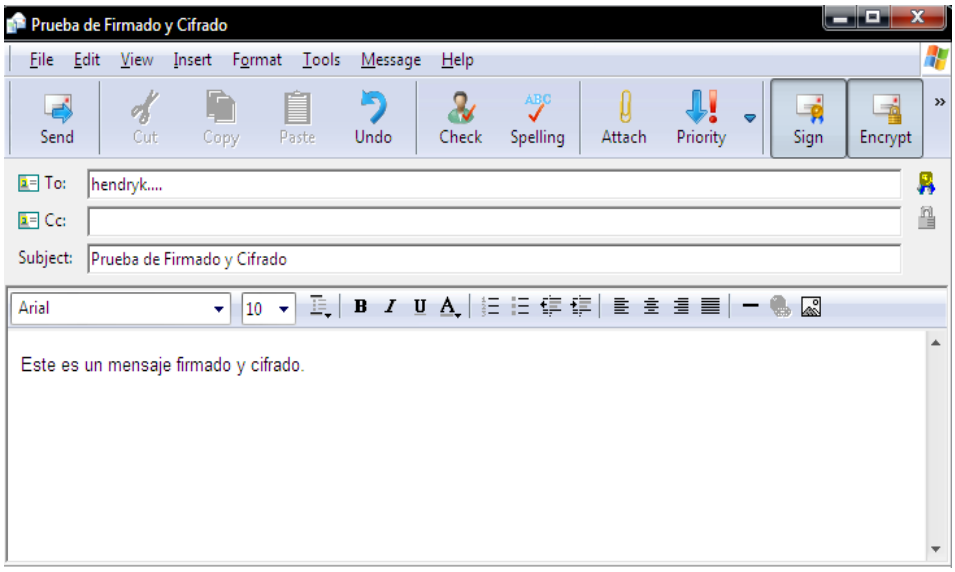


El receptor constatará que el mensaje ha sido firmado y cifrado por el icono mostrado en la parte inferior del mensaje, al cual puede darle click para constatar.

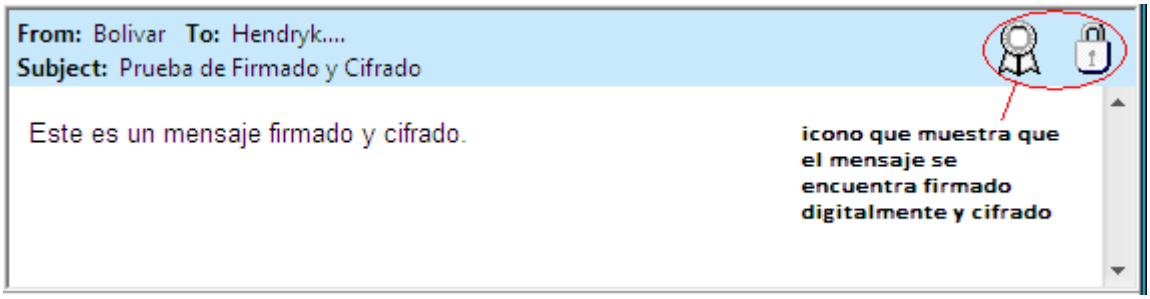


Outlook Express

Para enviar un mensaje cifrado, simplemente componemos un nuevo correo, y una vez redactado, nos ubicamos en la sección derecha del panel. Junto al botón **Firmar (Sign)** se encuentra el de **Encriptar (Encrypt)**. Lo activamos y posteriormente presionamos **Enviar (Send)**.



El receptor del mensaje lo recibe con una notificación que le indica que el correo que ha recibido se encuentra firmado y cifrado.



Anexo 5

Anexo [5-1] Disposiciones Legales para el establecimiento de una Autoridad Certificadora en el Ecuador.

A continuación se presenta un extracto de la Resolución 480-CONATEL-2008 del 8 de octubre de 2008. La resolución completa esta disponible en **[17]**

"Resolución 480-CONATEL-2008

CONSEJO NACIONAL DE TELECOMUNICACIONES

CONATEL

CONSIDERANDO:

Que mediante Ley 67, publicada en el suplemento del Registro Oficial 577 de 17 de abril de 2002 se expidió la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos…

… En ejercicio de sus atribuciones,

RESUELVE:

ARTICULO UNO. Acoger la recomendación formulada en memorando DGGST-2008-0949 de 03 de octubre de 2008, y fijar los valores que se deberán cancelar en la Secretaria Nacional de Telecomunicaciones, por la Acreditación de una Entidad de Certificación de Información y Servicios Relacionados, previo a que se realice el registro respectivo, en la suma de VEINTE Y DOS MIL DOLARES DE LOS ESTADOS UNIDOS DE NORTEAMERICA (USD $ 22,000), desglosados de acuerdo al detalle constante en la siguiente tabla:

Concepto	**Valor USD $**
Emisión de Acreditación y Registro	10.000
Prestación de Servicios de Certificación de Información y Servicios Relacionados que incluye: Emisión de firmas electrónicas, Sellado electrónico de tiempo, Conservación segura de mensajes de datos y Otros servicios relacionados	6.000
Costos y gastos de administración del CONATEL y de la SENATEL	3.000
Costos y gastos de control de la SUPERTEL	3.000
TOTAL	**22.000**

La presente Resolución es de ejecución inmediata, sin perjuicio de su publicación en el Registro Oficial.

Dado en Guayaquil 8 de octubre de 2008.”

Suscriben el Presidente y la Secretaria de la CONATEL.

Además existen otras disposiciones contempladas en **[18]**.

BIBLIOGRAFÍA

BIBLIOGRAFIA:

[1] CAICEDO, M. A. (2007): "La Infraestructura de Clave Pública PKI y el diseño de un modelo para su implementación en la Universidad Técnica Particular de Loja". Quito, UTPL. Escuela de Sistemas Informáticos y computación. Área de Seguridades.

[2] QUISHPE, M. y SANCHEZ, M. (2008): "Implementación de una Infraestructura de Clave Pública (PKI) para la Universidad Técnica Particular de Loja". Loja, UTPL. Escuela de Ciencias de la Computación.

[3] CUESTA RUIZ, J. y PUNALES CASQUERO, M. (curso 2001-2002): *PKI Infraestructura de Clave Pública.* Formato de archivo: PDF/Adobe Acrobat. Disponible en *asignaturas.diatel.upm.es/seguridad/trabajos/trabajos/.../pki.pdf*

[4] NASH, A., DUANE, W., JOSEPH, C., y BRINK, D. (2002): *PKI La mejor tecnología para implementar y administrar la seguridad electrónica de su negocio.* Colombia: Ed. McGraw-Hill.

[5] OpenCA Group. Información acerca de la herramienta OpenCA. Disponible en internet *en* http://www.openca.org/

[6] BANNON, D. (2007, diciembre 11): *The APAC-GRID Certificate Authority Complete process*. Disponible en internet en la página web *http://wiki.arcs.org.au/bin/view/Main/CertHandling.html*

[7] FRAUEL, Y. (2007 semestre uno). *Protocolos de Correo e Infraestructura de Clave Pública (Principios, herramientas y protocolos de criptografía)*. Documento pdf.

[8] VERISIGN MANAGED PKI. (2008 Noviembre). Documento informativo de Verisign en formato pdf, Víctor González, ESign S. A. Afiliado de Verisign Inc. Santiago, Chile.

[9] MACRO SEGURIDAD. *Firma Digital y PKI.* Página informativa ubicada en *http://www.macroseguridad.com/index.php?option=com_content&view=article&id=52&Itemid=79&lang=es.* Joaquín Requena 1346, Tel: +598 (2) 400-2961 CP: 11200, Montevideo – Uruguay.

[10] WIKIPEDIA Foundation, Inc., Algoritmo de encriptación RSA. Página disponible en internet en *http://es.wikipedia.org/wiki/RSA.*

[11] WIKIPEDIA Foundation, Inc., Algoritmo de encriptación DSA. Página disponible en internet en *http://es.wikipedia.org/wiki/DSA.*

[12] WIKIPEDIA Foundation, Inc., Algoritmo de encriptación ECDSA. Página disponible en internet en *http://es.wikipedia.org/wiki/ECDSA.*

[13] ESCERT (Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas). Pagina web disponible en *http://escert.upc.edu/index.php/web/es/*

[14] Página de descarga de Thunderbird. Disponible en: *http://www.mozilla-europe.org/es/products/thunderbird/*

[15] Configuración Avanzada de Mozilla Thunderbird 1.0.2. *Área de Comunicaciones - Servicio de Tecnología de la Información y las Comunicaciones.* Universidad de Almería, España. Formato de archivo: PDF/Adobe Acrobat. Disponible en: *http://cms.ual.es/idc/groups/public/@serv/@stic/documents/documento/correo_es_avanzada_thunderbird.pdf*

[16] Uso básico de Mozilla Thunderbird 1.0.2. *Área de Comunicaciones - Servicio de Tecnología de la Información y las Comunicaciones.* Universidad de Almería, España. Formato de archivo: PDF/Adobe Acrobat. Disponible en: *cms.ual.es/idc/groups/public/.../correo_es_uso_thunderbird.pdf*

[17] RESOLUCION 480-CONATEL-2008 Consejo Nacional de Telecomunicaciones. Formato de archivo: PDF/Adobe Acrobat. Disponible en *www.conatel.gov.ec/site_conatel/.*

[18] Decreto Ejecutivo N^{o} 1356. Formato de archivo: PDF/Adobe Acrobat Disponible en *www.lexis.com.ec/lexis/.../DECRETO%201356%2009-2008.pdf*

[19] Descarga de paquetes OpenCA (source files) de la página oficial: *http://www.openca.org/projects/openca/downloads_sources_1.0.2.shtml*

[20] Instalación de OpenCA (2009 julio). Disponible en: *http://wiki.lsc.dc.uba.ar/index.php/Instalacion_de_OpenCA*

[21] ESTEVES JORGE, J. M., *Departamento de Ingeniería y Arquitecturas Telemáticas. E.U.I.T. de Telecomunicación. Universidad Politécnica de Madrid. "Seguridad en Redes Telemáticas- Creación de una CA con OpenCA"*. Formato de archivo: PDF/Adobe Acrobat. Documento disponible en internet en *http://asignaturas.diatel.upm.es/seguridad/trabajos/*

[22] OpenCA-Guide for Version 0.9.2+. Guía de instalación de OpenCA, disponible en: http://www.openca.org/projects/openca/

[23] DARTMOUTH, University of *Dartmouth. PKI Lab. Howto to install Openca.* Formato de archivo: HTML. Disponible en *www.cs.dartmouth.edu/~pkilab/index.shtml*

[24] Nabble - *openca-users forum & mailing list.* Foro de ayuda a usuarios de OpenCA. Disponible en: *www.nabble.com/openca-users*.

AUTORIDAD CERTIFICADORA

CA-UTPL

MANUAL DEL ADMINISTRADOR

INDICE:

1. Información General

Todo el entorno que involucra PKI se concentra en dos servidores, cuya función es detallada a continuación:

Servidor	Sistema Operativo	Direccionamiento IP	Dominio	Función
CA	Debian	172.16.52.21	ca.utpl.edu.ec	Alojar la Autoridad Certificadora CA
RA	Ubuntu	172.16.50.71	repo.utpl.edu.ec	Alojar la Autoridad de Registro (RA) y la Interfaz Pública (PUB)

1.1. **La Autoridad certificadora CA** es la encargada de firmar y generar los certificados solicitados por los usuarios y que han sido aprobados por la Autoridad de Registro RA. Esta CA debe ser accesada únicamente por el administrador de CA.

1.2. **La Autoridad de Registro RA** es la encargada de aprobar las peticiones de certificados y dirigirlas a la Autoridad Certificadora CA para la generación de dichos certificados de usuario. El acceso a la RA es exclusivo del administrador de la RA.

1.3. **La Interfaz Pública** es el sitio web a donde se dirigen los usuarios para llenar la solicitud de petición de certificado, como su nombre lo indica, esta interfaz es de acceso público para todos aquellos miembros de la universidad que requieran un certificado digital.

Para la administración de estos servidores se requieren dos administradores, que a la vez serán los operadores de las funciones que cada servidor debe realizar, por lo que de aquí en adelante los términos administrador y operador en este manual serán equivalentes.

Los nombres de archivos, configuraciones y comandos en el presente manual, se encuentran con un tipo de letra diferente, en cursiva y/o negrita.

2. Instalación de OpenCA

La versión de la herramienta OpenCA que se emplea es la **1.0.2**.

Se utilizaron dos archivos fuente para su instalación:

Openca-base-1.0.2.tar.gz, que contiene todos los archivos de configuración de la herramienta.

Openca-tools-1.1.0.tar.gz, que reúne ciertos complementos para el funcionamiento de OpenCA.

Al tratarse de archivos fuente, en primer término se descargaron ambos paquetes de **[21]**, y luego se descomprimieron en el directorio /usr. Para ello se realizo lo siguiente:

- Ubicarse en el directorio /usr:
  - `cd /usr`

- Descomprimir el paquete openca-tools**:**
  - `tar  zxvf openca-tools-1.1.0.tar.gz`

- Ubicarse en el directorio recién creado, y compilar e instalar la herramienta.

  - `cd openca-tools-1.1.0`
  - `make clean`
  - `./configure`
  - `make`
  - `make install`

Posterior a esto, se descomprime el paquete openca-base-1.0.2.tar.gz dentro del mismo directorio /usr, pero ahora se utilizan algunas opciones de configuración para instalar primero en el servidor de RA. **[22]**:

```
o  cd /usr
o  tar  zxvf openca-tools-1.1.0.tar.gz
o  cd openca-tools-1.1.0
o  make clean
o  ./configure
        --with-httpd-user=www-data \
        --with-httpd-group=www-data \
        --with-openca-prefix=/usr/local/ \
        --with-etc-prefix=/usr/local/etc/ \
        --with-httpd-fs-prefix=/usr/local/var/www/ \
        --with-node-prefix=ra-node \
        --with-engine=no \
        --with-web-host=repo.utpl.edu.ec\
        --enable-ocspd \
        --enable-dbi \
        --disable-rbac \
o  make
o  make install-online
```

Ahora de igual manera pero esta vez para el servidor de CA:

```
o  ./configure \
      --with-httpd-user=www-data \
      --with-httpd-group=www-data \
      --with-openca-prefix=/usr/local/ \
      --with-etc-prefix=/usr/local/etc/ \
      --with-httpd-fs-prefix=/usr/local/var/www/ \
```

```
        --with-node-prefix=ca-node \
        --with-engine=no \
        --with-web-host=ca.utpl.edu.ec \
        --enable-ocspd \
        --enable-dbi \
        --disable-rbac \
```

- `make`
- `make install-offline`

Luego de haber instalado la herramienta, se configuran otros parámetros, como es el caso de la base de datos. Se utiliza MySQL como motor de base de datos, para ello luego de haber instalado los paquetes *mysql-server* y *mysql-client,* (si no lo están) cambiamos el password del usuario *root*:

- `#mysql –u root –p`
- `Passwd xxxx`

Se crean dos bases de datos, una para la parte offline[1] y otra para la online[2], en ambos casos la base de datos se denominará ***openca***. Para cada base de datos creamos un usuario: *openca_u* con password *caopenca* para la parte offline; y *openca_ur* con password *raopenca* para el servidor online, con todos los privilegios:

- `mysql> CREATE DATABASE openca;`
- `mysql> CREATE DATABASE openca;`
- `mysql> GRANT all PRIVILEGES ON openca.* TO openca_u@localhost IDENTIFIED BY "caopenca"`
- `mysql> GRANT all PRIVILEGES ON openca.* TO openca_ur@localhost IDENTIFIED BY "raopenca"`

Para comprobar las bases de datos creadas se realiza lo siguiente:

- `#mysql –u usroffline –p`
- `password : adminca`

Se reinicia el servicio de base de datos para guardar los cambios:

- `# /etc/init.d/mysql restart`

Una vez hecho esto, nos enfocamos en configurar el servidor apache2 para que soporte el modulo ssl. Posterior a la instalación del paquete *apache2,* tomando como guía a **[23]**, se crea un archivo llamado **openca.conf** con soporte SSL[3] y se lo ubica dentro del directorio **/etc/apache2/conf.d**. Dicho archivo contiene la información adjunta en el **anexo [3-2]**.

---

[1] **offline:** Se refiere al modo de instalación de la CA. Quiere decir que no posee contacto con ninguna red externa, salvo con el servidor de RA.

[2] **online:** Se refiere al modo de instalación de la RA, al contener también la interfaz pública, debe tener contacto con el exterior.

[3] **SSL:** Nivel de conectores seguro (**S**ecure **S**ocket **L**ayer).

Dentro del archivo principal de apache (**apache2.conf**)**,** activamos la línea de tal forma que reconozca el archivo openca.conf.

- `Include /etc/apache2/conf.d`

3. Configuración de OpenCA

3.1. Configuración del intercambio de datos

Ahora se configura propiamente el software OpenCA. Para ello nos ubicamos en el archivo de configuración `/usr/local/etc/openca/config.xml` (en el servidor de CA) Para configurar el intercambio de los datos a un nivel inferior de la CA, se utiliza el "template" número 1, se descomenta ésta opción, la cual posee las siguientes características **[24]**:

```
1. the node acts as CA only
the node exports to one or several RAs only
the node can export to LDAP too
```

Además se ubica la sección `'dataexchange configuration'` dentro de ella realizamos lo siguiente:

`dataexchange_device_down`: Reemplazamos `/dev/fd0` por `/usr/local/var/openca/tmp/openca.tar`

`dataexchange_device_local`: Reemplazamos `/dev/fd0` por `/usr/local/var/openca/tmp/ra-local`

Ahora nos ubicamos en el archivo `/usr/local/etc/openca/config.xml` (en el servidor de RA) Para configurar el intercambio de los datos a un nivel superior de la CA, se utiliza el "template" número 2, se descomenta ésta opción y tiene las siguientes características:

```
2. the node acts as RA only
the node exports to one or several RAs only
the node can export to LDAP too
```

Ubicamos la sección `'dataexchange configuration'` y modificamos:

`dataexchange_device_up`: Reemplazamos `/dev/fd0` por `/home/openca/openca.tar`

`dataexchange_device_down`: Reemplazamos `/dev/fd0` por `/usr/local/openra/openca/var/tmp/ra-down`

El valor realmente importante es el relacionado a `dataexchange_device_down` en el caso de la CA; y `dataexchange_device_up` cuando se trata de la RA.

3.2. Configurar Sendmail

Para verificar que Sendmail esté trabajando bien:
Primero, encontrar el valor de *Sendmail,* tanto para el servidor de la CA como para el de RA:

- `grep -w sendmail /usr/local/etc/openca/config.xml`
- `grep -w sendmail /usr/local/etc/openca/config.xml`

El valor por defecto es: `/usr/lib/sendmail -n –t`

Luego, nos ubicamos en `/usr/local/etc/openca/config.xml`, buscamos la sección `<name>service_mail_account</name>` y escribimos entre `<value></value>` el valor correspondiente al remitente de correo. Hacemos esto para ambos servidores.

Habilitamos el envío automático de correos. Para ello, en el archivo `/usr/local/etc/openca/config.xml` de los dos servidores, localizamos la entrada `<name>send_mail_automatic</name>` y cambiamos su valor a ***yes***.

3.3. Configuración del control de acceso

Tiene por objeto establecer las claves de acceso tanto al servidor de RA como al de CA. Para ello seguimos los parámetros de **[25]**:

Cambiamos el password de usuario *root* en la interfaz de RA:

- `cd /usr/local/lib`
- `./bin/openca-digest sha1 'mypasswd'`

(Seleccionar la cadena de password que se encuentra entre comillas simples).

Luego ubicarse en el directorio `cd /usr/local/etc/openca/access_control`

Reemplazar TODOS los valores entre `<digest></digest>` con el nuevo hash generado, en todos los archivos de ese directorio con el comando:

- `vi `grep -li '<digest>' *.template``

Cambiamos el password de usuario *root* en la interfaz de CA:

- `cd /usr/local/lib`
- `./bin/openca-digest sha1 'mysecret'`

(Seleccionar la cadena de password que se encuentra entre comillas simples).

Ubicarse en el directorio `cd /usr/local/etc/openca/access_control`

Reemplazar TODOS los valores entre `<digest></digest>` con el nuevo hash generado en todos los archivos.

- `vi `grep -li '<digest>' *.template``

Deshabilitar el botón de logout para la interfaz **pub** en RA. (Saltar este paso si el **digest** en *pub.conf.template* está comentado).

Editar el archivo `/usr/local/etc/openca/menu.xml.template` (**anexo [3-3]**)

Localizar la sección `<interface><name>@pub_prefix@</name>`

Una vez localizada, observar el subbloque `<name>General</name>`.

Dentro de éste, observar la sección `<name>Logout<name>`

Cambiar `Logout` a `Not logged in`

Borrar el valor de `<link>` de modo que luzca vacio `<link></link>`

Cambiar `_top` a `main` para el campo `<target>`

Esto es, en líneas generales, lo que se debe de hacer en ambos servidores como paso siguiente a la instalación de OpenCA en lo relacionado a acceso a los mismos y otros detalles.

3.4. Configuración de archivos importantes de OpenCA

Ahora se va a indicar detenidamente cómo esta constituido cada servidor por separado, a través del analisis de los archivos que lo conforman, así como de las modificaciones a hacer en los mismos para que se adapten a nuestras necesidades.

Los archivos modificables que constituyen OpenCA se denominan *.templates,* a partir de los cuales se generan los requerimientos de usuario, tanto en la CA como en la RA.

Una vez modificados los datos relevantes de estos templates, se requiere compilar el software, por medio de la ejecución del script *`configure_etc.sh`*, ubicado dentro del directorio `/etc`.

Para empezar, inicializamos OpenCA (en el servidor RA) por medio del script *`./openca_start`* y testeamos la configuración tecleando en el navegador:

```
https://repo.utpl.edu.ec/ra
https://repo.utpl.edu.ec/node
https://repo.utpl.edu.ec/pub
```

Ahora en el servidor CA, luego de haber configurado todos los *.templates,* resta inicializar los servicios de este servidor, para lo cual ejecutamos:

- `cd /usr/local/etc/openca/`
- `./configure_etc.sh`
- `./openca_start`

El comando *`./configure_etc.sh`* como dijimos carga los valores de los archivos *templates* modificados recientemente en el archivo central *`config.xml.`*

Testeamos desde el navegador:

`http://ca.utpl.edu.ec/ca`
`http://ca.utpl.edu.ec/node`

Se nos mostrara una pantalla de logueo, que nos pide ingresar la clave de acceso a dicha interfaz.

Fig. 1 Pantalla de logueo de las interfaces CA y RA

4. Inicialización de OpenCA

Una vez instalada y configurada, a continuación detallamos los pasos de iniciación de la herramienta OpenCA como Autoridad Certificadora.

4.1. Configuración basada en web para CA

La configuración siguiente esta basada en **[26].**

Escribimos en el navegador http://ca.utpl.edu.ec/ca, se debe loguear para ingresar al nodo.

Nos dirigimos a la sección:

`Init & Config PKI -> Initialization -> Initialize the Certification Authority`

Se presenta una ventana como la de la figura 2. Dentro de la cual realizamos lo siguiente:

`-> Initialize Database`

Se muestra un mensaje que nos indica que la Base de Datos fue inicializada exitosamente.

`-> Generate new CA secret key`

Fig. 2 Inicialización de la CA

En esta parte se genera la clave secreta de la nueva Autoridad Certificadora, para ello se debe introducir una clave lo suficientemente segura, al momento en que se nos pida hacerlo.

`-> Generate new CA Certificate Request (use generated secret key)`

Llenamos la forma que se nos muestra, y volvemos a ingresar la clave que introdujimos en el paso anterior.

`-> Self Signed CA Certificate (from already generated request)`

Esta opción es empleada si nosotros mismos firmamos nuestra solicitud de certificación, es decir para una Autoridad Certificadora autofirmada. (Aceptar el valor por defecto)

`-> Rebuild CA Chain`

Con esta opción se construye la jerarquía de la nueva CA.

Ahora se requiere generar el primer certificado, que será asignado al administrador de la CA. Para ello en la sección:

-> Init & Config PKI -> Initialization -> Initialize the CA Administrator

Realizar:

-> Create a new request
Aquí se nos pide los datos del administrador de la interfaz CA, llenar la forma para generar el requerimiento de certificado para dicho administrador.

-> Edit the request (Esto es opcional).

-> Issue the certificate
Se nos muestra el certificado de administrador generado.

-> Handle the certificate
(Ubicarse en Certificate and Keypair, PKCS#12, y dar clic en Download. Guardar la descarga como caadmin.p12).

Dar doble click en caadmin.p12 e importarlo en el navegador. Luego reiniciar el mismo.

Ahora, si deseamos, podemos crear un certificado para el administrador de la RA. Para ello en la sección:

-> Init & Config PKI -> Initialization -> Initialize the RA Administrator

Hacer lo siguiente:

-> Create a new request
Llenar la forma presentada. En la opción Role escoger RA Operator, lo cual generara un CSR para el operador de la RA.

-> Edit the request (Este parámetro es opcional).

-> Issue the certificate
Aquí se genera el certificado de operador de RA.

-> Handle the certificate
Escoger Certificate and Keypair, PKCS#12, dar click en Download. Guardar como raop.p12)

Dar doble clic en raop.p12 para de esta forma importarlo en el navegador. Reiniciar el mismo.

4.2. Sincronizar configuración entre CA y RA

A través de esta función, se testea si el intercambio entre los nodos del servidor de la CA y RA se realiza de forma óptima.

Para ello, primero nos ubicamos en la interfaz *node* del servidor de la CA.

Ir a `http://ca.utpl.edu.ec/node`

Click en `Node Ops -> Import/Export Data`

Click en `Enroll data to a lower level of the hierarchy -> Configuration.`

A través de esta opción, los datos son enviados desde el servidor de la CA al nodo del servidor de la RA, puesto que la interfaz RA se encuentra subordinada a la Autoridad Certificadora CA.

Ahora es necesario recibir dicha información de testeo en el servidor RA. Para ello nos dirigimos al servidor RA, concretamente al nodo de intercambio:

`https://repo.utpl.edu.ec/node`

Click en `Node Ops -> Import/Export Data`

Click en `Download data from a higher level of the hierarchy -> Configuration`

Si en el cuadro de logs no observamos ningún mensaje de error, consideramos que la configuración de intercambio es correcta.

4.3. Sincronización completa entre CA y RA

Lo anterior sirve para comprobar la configuración de intercambio. Ahora es el momento de enviar la información creada anteriormente en el servidor CA hacia el servidor RA, es decir datos como el certificado recién generado de la Autoridad Certificadora y los certificados de administrador de la CA y RA, para que se pongan a disposición de los usuarios en general.

Nuevamente nos dirigimos al nodo de intercambio de CA, así:

Ir a `http://ca.utpl.edu.ec/node`

Click en `Node Ops -> Import/Export Data`

Click en `Enroll data to a lower level of the hierarchy -> All`

Retornar al servidor RA, a su nodo de intercambio, para recibir los datos procedentes del servidor jerárquicamente superior, es decir el de la CA:

Ir a `https://ra.utpl.edu.ec/ra-node`

Click en `Node Ops -> Import/Export Data`

Click en `Download data from a higher level of the hierarchy -> All`

Observar el cuadro de logs para chequear posibles errores surgidos, si no existieran, los datos han sido transferidos correctamente.

4.4. Generar el primer certificado de cliente para prueba

Para probar la fluidez de los procesos, se requiere generar una solicitud de firma de certificado (CSR) en la interfaz pública.

Ir a `https://repo.utpl.edu.ec/pub`

`Mis Certificados -> Requerir un Certificado -> Petición de Certificado de Navegador`

Completar lo solicitado. Observar el número serial, el cual es el número serial de requerimiento.

Aprobar el requerimiento
Ir a `https://repo.utpl.edu.ec/ra`

Activar `RA Operations -> Certification Request -> New -> Search`

Clic en `serial number`, es decir el número serial arriba descrito.
Clic en `Approve Request without signing`

Exportar el requerimiento desde RA:

Ir a `https://repo.utpl.edu.ec/node`

`Node Ops -> Import/Export Data -> Upload data to a higher level -> requests`

Importar el requerimiento en CA:

Ir a `http://ca.utpl.edu.ec/node`

`Node Ops -> Import/Export Data -> Receive data from a lower level -> requests`

Generar el certificado:

Ir a `http://ca.utpl.edu.ec/ca`

`CA Operations -> Certification Request -> Approved`

Click en `serial number` y luego click en el botón `Issue certificate`

Exportar el certificado desde la CA:

Ir a `http://ca.utpl.edu.ec/node`

`Node Ops -> Import/Export Data -> Enroll data to a lower level -> Certificates`

Importar el certificado en RA:

Ir a `https://repo.utpl.edu.ec/node`

`Node Ops -> Import/Export Data -> Download data from a higher level -> Certificates`

Recoger el certificado en PUB:

Ir a `https://repo.utpl.edu.ec/pub`

`Información -> Certificados Validos`

Dar clic en `more` y luego de revisar el certificado, dar clic en `Install the certificate.`

4.5. Generar la nueva Lista de Revocación de Certificados (CRL[4])

Ahora, como propietario del certificado generado anteriormente, se debe presentar el requerimiento de revocación de certificados (CRR[5]) para revocar dicho certificado. Posterior a esto, el administrador debe loguearse para ingresar a la RA, aprobar la CRR sin firmar, subirla a la CA desde el nodo de la RA y luego descargarla a la CA desde el nodo de esta. Luego se aprueba la CRR desde la interfaz de la CA.

---

[4] **CRL:** Lista de revocación de certificados (**C**ertificate **R**evocate **L**ist)

[5] **CRR:** Requerimiento de revocación de certificados **(C**ertificate **R**evocate **R**equest**)**

Para ello vamos a:

`http://ca.utpl.edu.ec/ca`

Luego de loguearse, se muestra una pantalla como la de la figura 3, ante la cual el administrador debe dirigirse a:

`Usual Operations -> Issue new CRL`

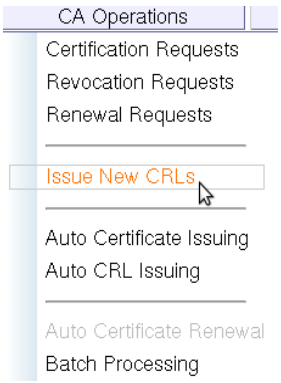


Fig. 3 Generar nueva Lista de revocación de certificados

Seguidamente se requiere indicar el periodo de validez de la CRL (figura 4)

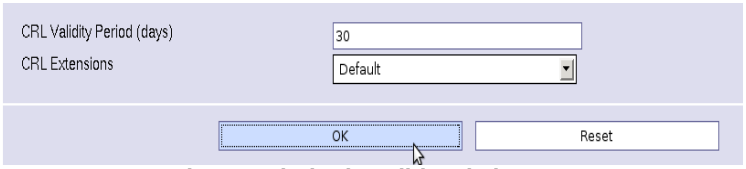


Fig. 4 Periodo de validez de la CRL

Luego de presentar las credenciales (clave secreta de CA-UTPL), se genera la nueva CRL, como se muestra en la figura 5.

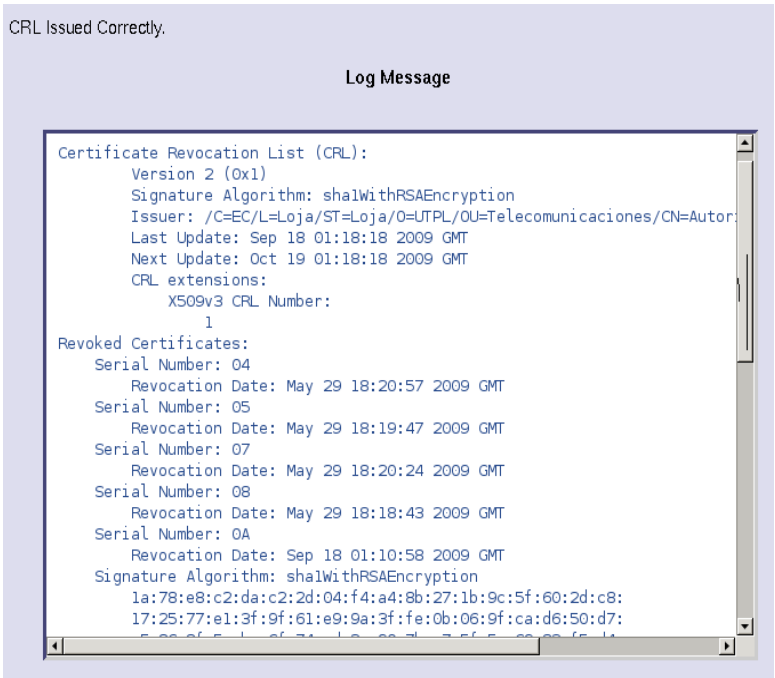


Fig. 5 CRL generada correctamente

Después de generar la nueva CRL desde la interfaz CA, el administrador de CA debe loguearse para acceder a la interfaz de nodo de CA, y enrolarla a la RA (figura 6).

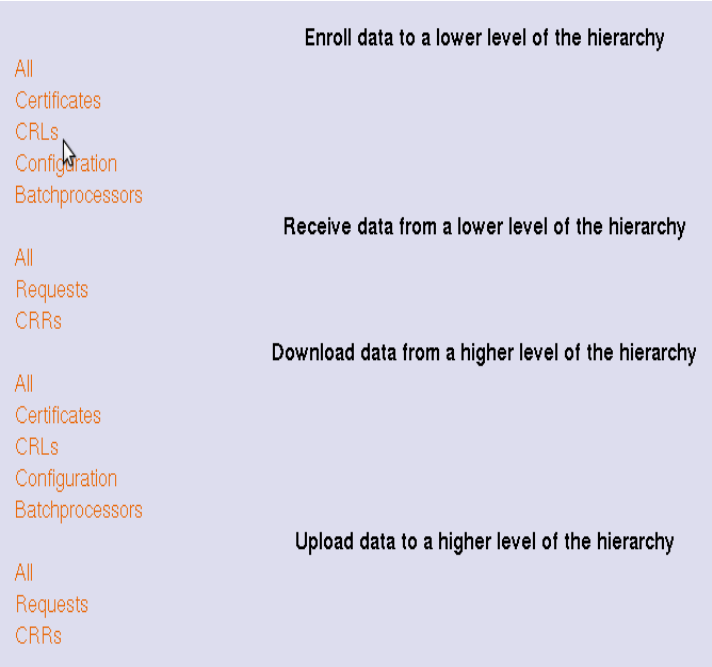


Fig. 6 Enrolar la CRL al servidor de RA

Se muestra el archivo de logs mostrando el correcto enrolamiento de la CRL (figura 7).

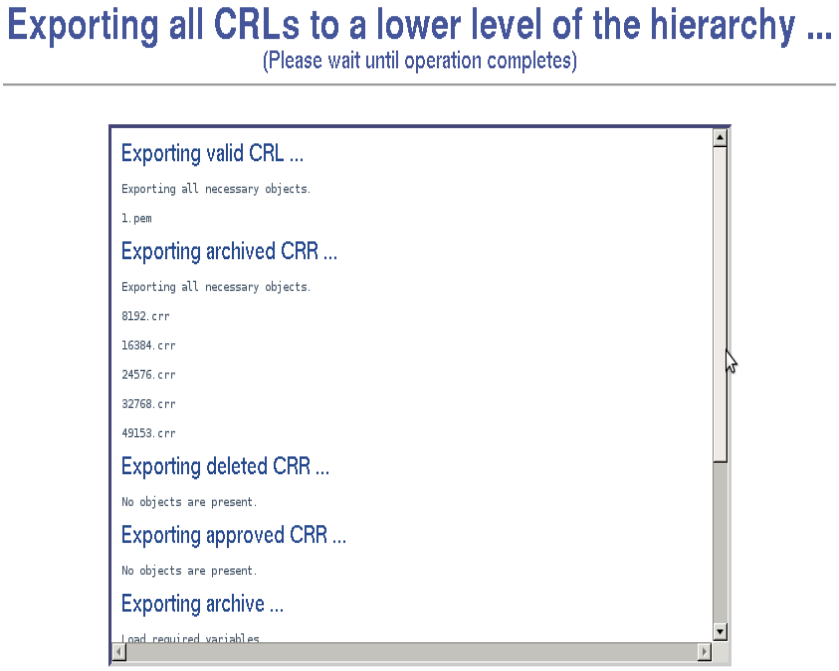


Fig. 7 Archivo de logs de la exportación de la CRL

El administrador de RA debe loguearse en el nodo de la RA y descargar dicha CRL (figura 8)

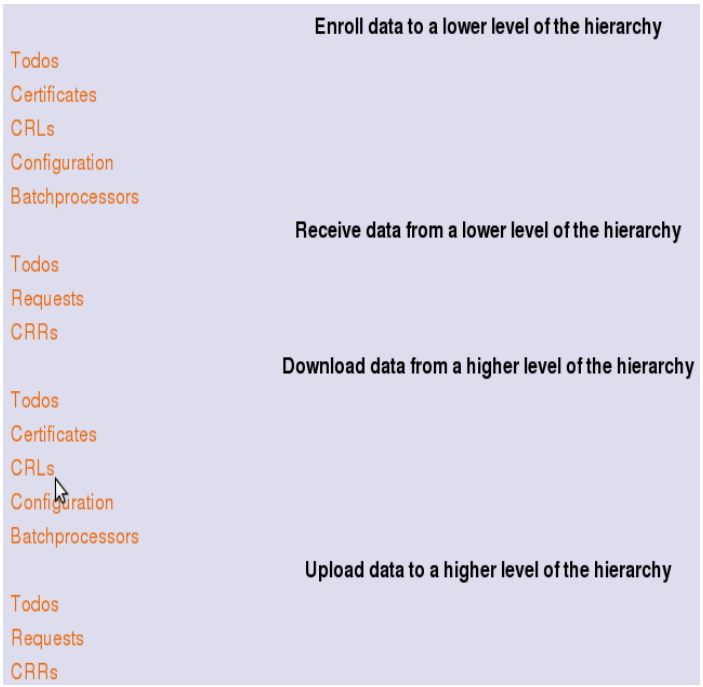


Fig. 8 Descargar la CRL desde el servidor de CA

Una vez seleccionada la opción de descarga de la CRL, una vez más se muestra el archivo de logs del servidor RA (figura 9).

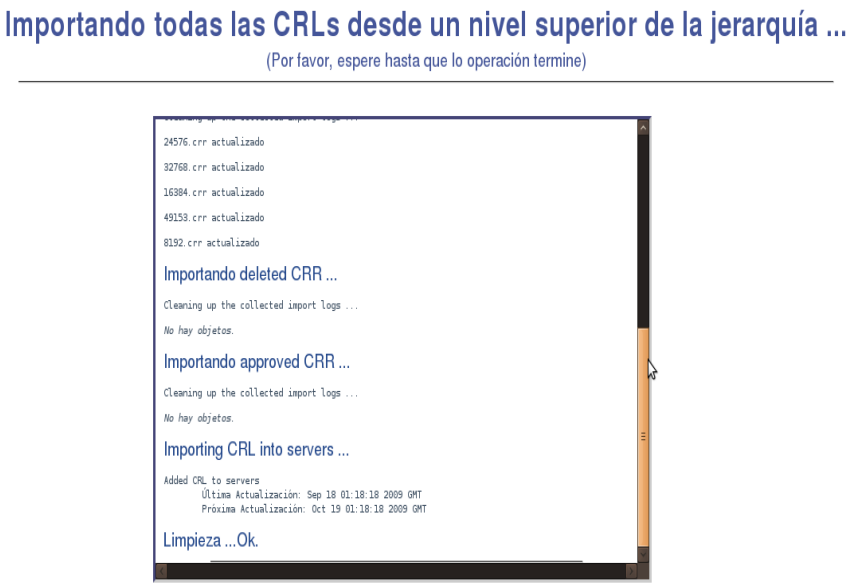


Fig. 9 Archivo de logs de la importación de CRL

Esto crea y muestra una nueva CRL. Esto se hace con el fin de generar una nueva CRL antes de producir certificados reales, puesto que varios clientes, como Outlook, tratan de obtener la CRL de URLs publicadas en CDPs, es decir puntos de distribución de certificados.

OpenCA está lista para la generación de certificados reales para propósitos de producción.

5. Procesos de certificación

5.1. Aprobación de la Solicitud de Certificado (administrador de RA)

Una vez que el usuario ha generado su petición de firma de certificado (CSR[6]), dicha petición es tratada en primer término por el operador de la Autoridad de Registro RA-UTPL, quien debe autenticarse para acceder al nodo correspondiente a la RA (figura 10).

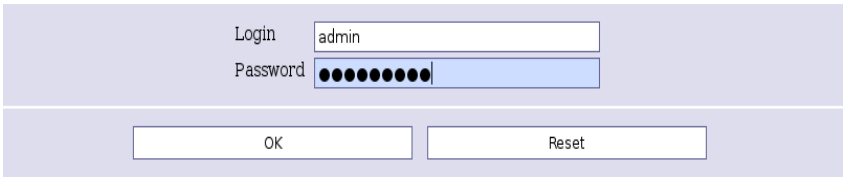


Fig. 10 **Pantalla de logueo a la interfaz RA**

Luego de ingresado, el administrador debe dirigirse a ***RA Operations***, localizar la pestaña ***Certification Requests***, y seleccionar la etiqueta ***New*** (figura 11).

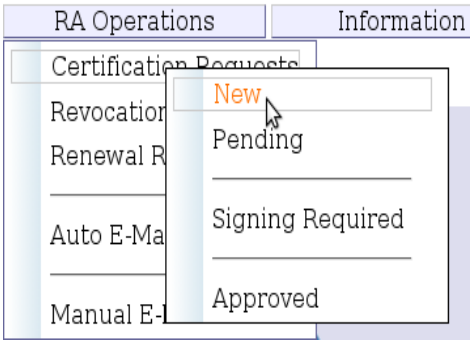


Fig. 11 Solicitudes de certificación nuevas

Seleccionar ***Todos*** en cada una de las cajas de texto**,** y dar click en ***Search*** (figura 12).

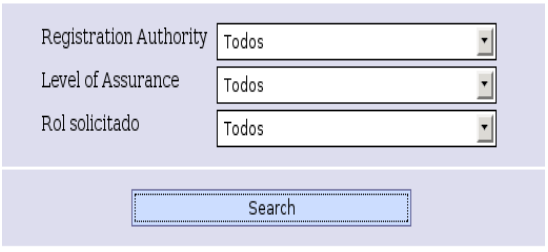


Fig. 12 Buscar solicitudes de certificación nuevas

Acto seguido se muestran todas las peticiones de certificados por atender. Entonces se da un clic en el **Serial** del certificado que se quiere aprobar (figura 13).

---

[6] **CSR:** Requerimiento de firma de certificado (**C**ertificate **S**ign **R**equest)

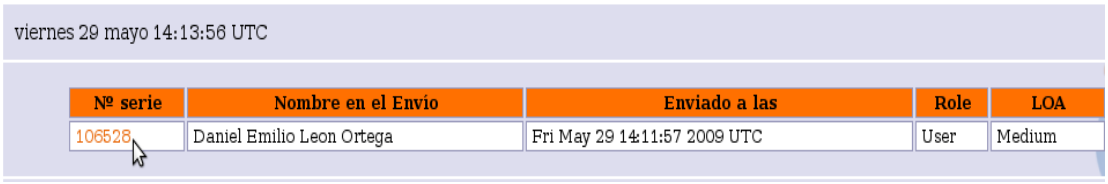


Fig. 13 Seleccionar el serial del certificado

En la parte inferior de la pantalla generada, se presentan varias opciones: (figura 14)

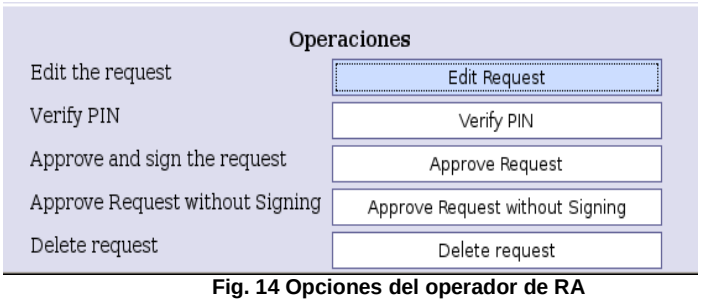


Fig. 14 Opciones del operador de RA

- *Edit Request*.- Aquí se puede modificar algún aspecto de la petición que este errado o que haya sido omitido. En especial los campos relacionados a los días de vigencia del certificado, la fecha de iniciación y de caducidad del mismo. Es de gran importancia destacar que la fecha de validez de un certificado debe ser inferior al certificado de la Autoridad Certificadora CA-UTPL (figura 15).

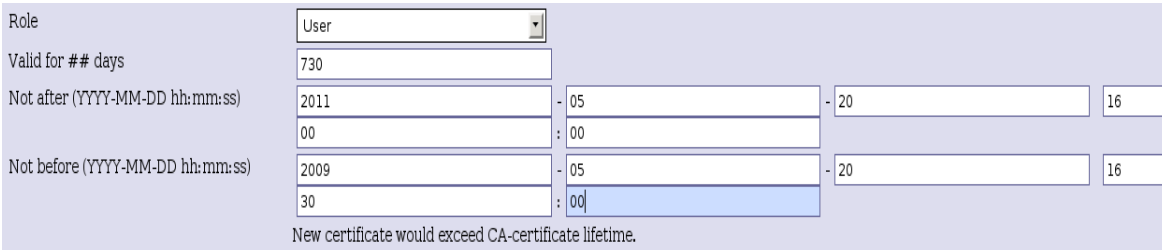


Fig. 15 Editar el tiempo de vida del certificado

Luego de haber hecho las modificaciones necesarias, seleccionamos la pestana ***Submit the changed request*** y damos click en ***OK*** (figura 16).

Fig. 16 Mantener los cambios del certificado

- *Verify PIN*.- En verificar PIN, el Operador de la RA debe asegurarse de que el PIN coincida con el solicitado al usuario (figura 17).

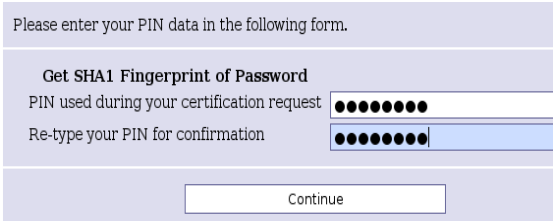


Fig. 17 Verificación del PIN

Si coincide el PIN ingresado con el PIN entregado por el usuario, se presentara una ventana en la cual se corrobora la coincidencia del PIN (figura 18).

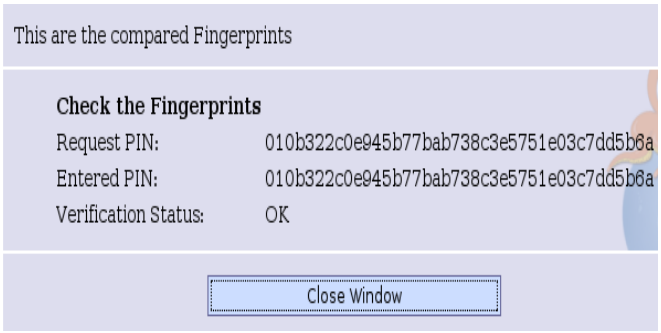


Fig. 18 PIN comprobado correctamente

- *Approve and Sign the Request / Approve request without signing*.- La diferencia entre estas 2 opciones radica en que la segunda no requiere que el certificado de operador de la RA esté instalado en el navegador. El primero de ellos le da un poco mas de credibilidad a la CA-UTPL. Sin embargo, las pruebas realizadas se efectuaron con la segunda opción.

Una vez seleccionada dicha opción, se muestra una ventana como esta: (figura 19)

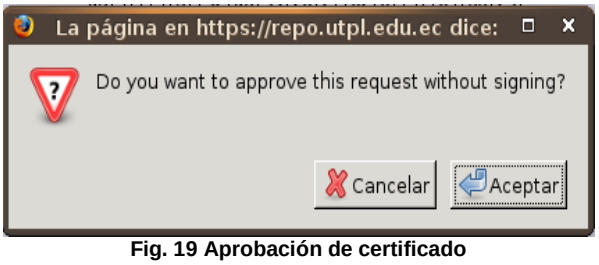


Fig. 19 Aprobación de certificado

Al dar clic en ***Aceptar***, se muestra una comprobación de que la solicitud ha sido firmada, y que se encuentra lista para ser enviada al servidor de la CA a espera de la generación del certificado (figura 20).

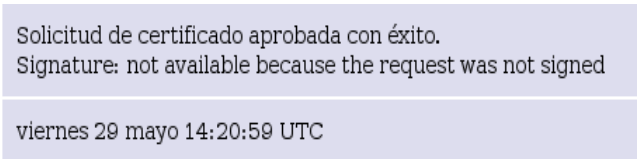


Fig. 20 Solicitud aprobada exitosamente

- *Delete Request*.- Simplemente descarta la petición de certificación de acuerdo a algún término escrito en la CP/CPS. La RA tiene total autoridad para anular una petición si esta va en contra de algún aspecto contemplado en las Políticas de Certificación.

La petición aprobada ahora es enviada al operador de CA para que este emita el certificado correspondiente.

5.2. Intercambio de Datos de RA-CA

En esta interacción se procede a transferir las solicitudes aprobadas por la RA hacia el operador de la CA para la respectiva generación de los certificados.

Este proceso es uno de los más importantes en el establecimiento de la PKI, puesto que maneja la sincronía en la transferencia de información entre los dos servidores, el de la CA y el de RA. Esta configuración se encuentra en los archivos **node.conf** en ambos servidores.

El administrador de la RA, luego de autenticarse para acceder al nodo de intercambio, se encuentra con la opción ***Node Ops*****,** seleccionar ***Import/Export Data*** (figura 21).

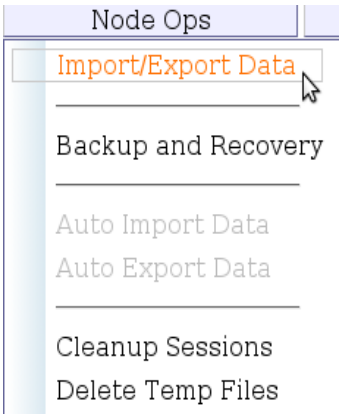


Fig. 21 Transferencia de datos de RA a CA

Aparece una pantalla de verificación en la cual se le advierte al administrador que revise el soporte de configuración, es decir si existen los archivos de intercambio. Damos clic en ***OK*** (figura 22).

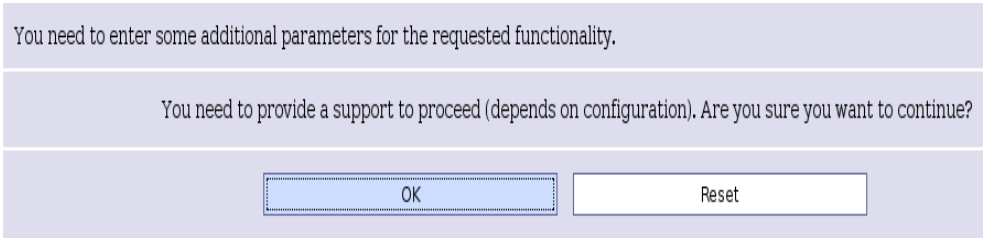


Fig. 22 Pantalla de Verificación

En la sección inferior de la nueva pantalla se divisa la opción ***Upload data to a higher level of the hierarchy*** (Subir datos al nivel más alto de la jerarquía) es decir al nodo de la CA. Se da clic en el tag ***Request*** (Requerimientos) (figura 23).

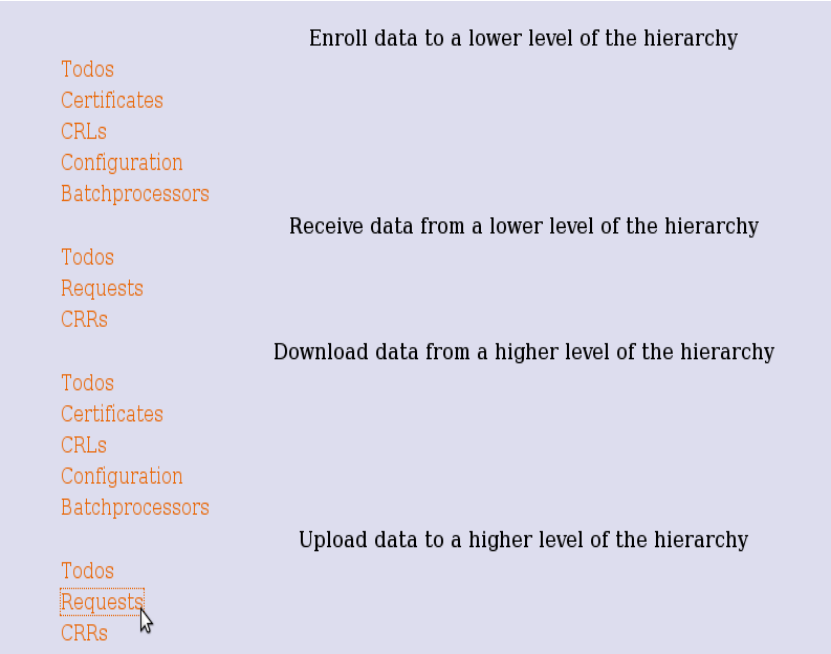


Fig. 23 Subir requerimientos desde RA a CA

Se nos muestra una ventana de logs, en la cual se detalla todos los procedimientos realizados, al final de la misma sale un mensaje de *OK*, el mismo que es la confirmación de que todos los procesos de intercambio fueron realizados exitosamente (figura 24).

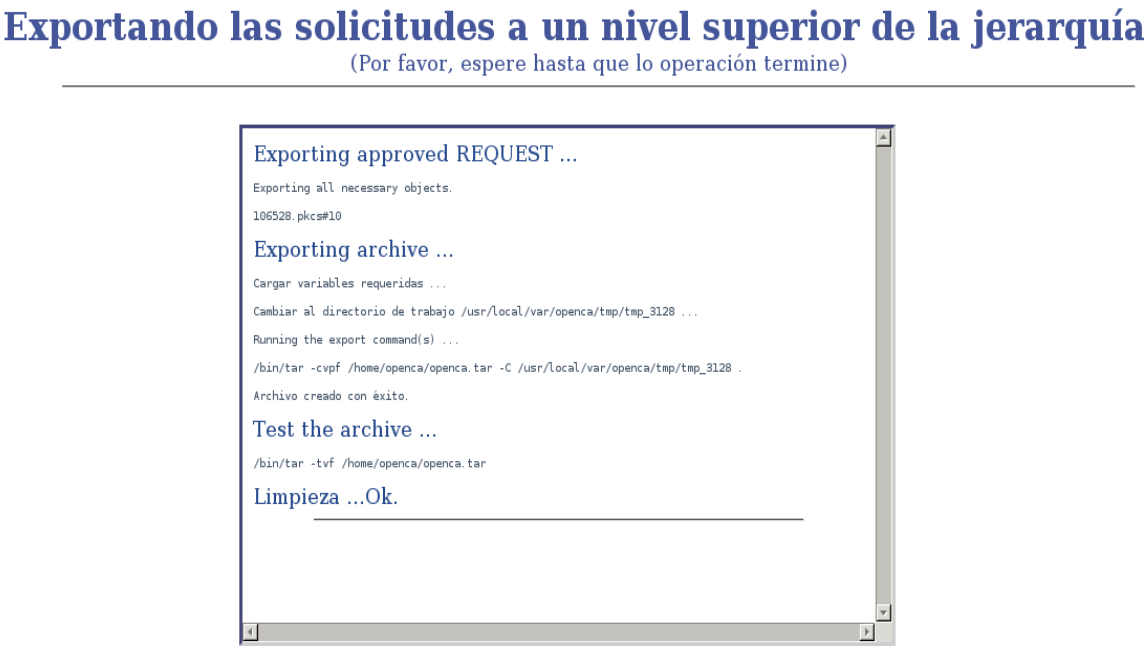


Fig. 24 Cuadro de logs de las solicitudes exportadas

Ahora es el turno del operador de la CA, el cual asimismo debe loguearse para ingresar al nodo de intercambio CA (figura 25).

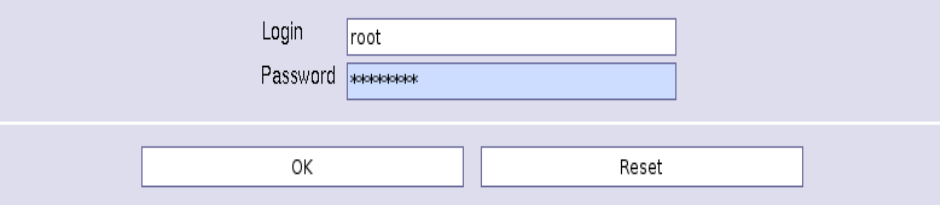


Fig. 25 Pantalla de logueo del operador de CA

Se encuentra con una pantalla similar al del operador de la RA. Pero ahora escoge la opción ***Receive data from a lower level of the hierarchy*** (Recibir datos desde el nivel más bajo de la jerarquía) es decir, desde el nodo de la RA. Se da clic en el tag ***Request*.** Y posteriormente ***Aceptar***.

Luego de esto se muestra el cuadro de logs que informa todo el proceso de intercambio, así como de algún posible error surgido. Se observa en la penúltima fila el número de petición de certificado junto con el tipo (pkcs#10) (figura 26).

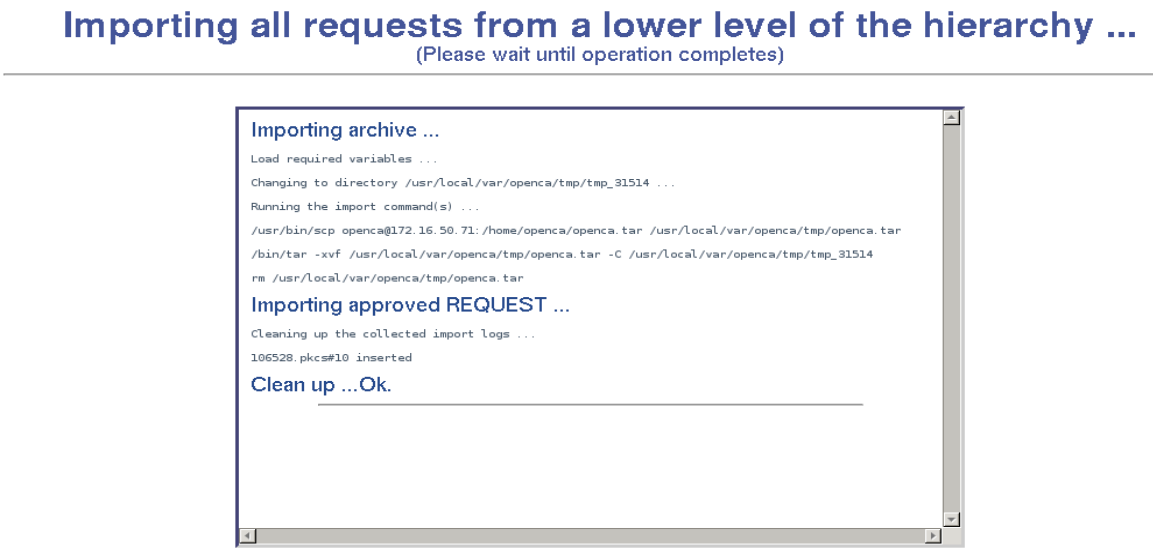


Fig. 26 Cuadro de logs de las solicitudes importadas

Con esto se garantiza que los datos han sido intercambiados con éxito entre los dos servidores.

5.3. Generación de certificados (Operador de CA)

Ahora el operador de la CA debe loguearse e ingresar al nodo de la CA, para que pueda firmar las solicitudes. Una vez dentro de la interfaz CA, debe ingresar a ***CA Operations***, clic en ***Certification Requests***, en la etiqueta ***Approved*** (figura 27).

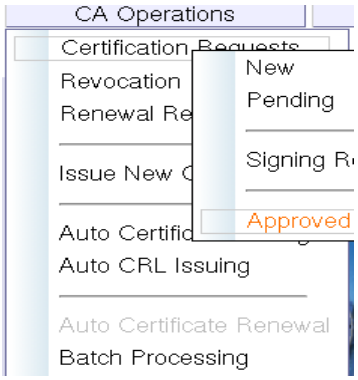


Fig. 27 Búsqueda de peticiones aprobadas

Se puede observar el requerimiento aprobado por la RA en espera de ser firmado. Entonces se da un clic al **Serial** de dicho requerimiento a generar (figura 28).

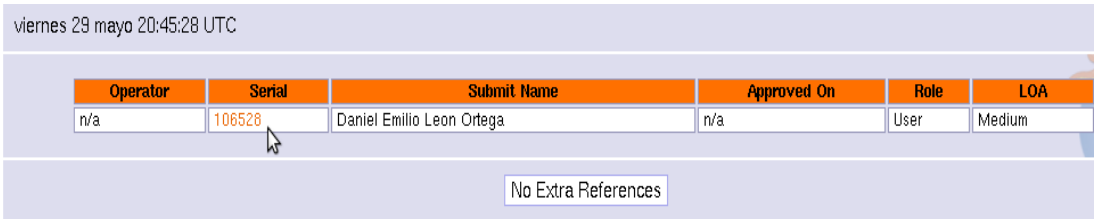


Fig. 28 Selección de la petición aprobada

Una vez se nos presente la siguiente pantalla, en la parte inferior debemos seleccionar ***Issue Certificate*** (figura 29).

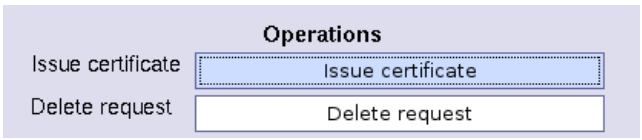


Fig. 29 Generar el certificado

A continuación se pide presentar las credenciales de operador de la CA (la clave privada) Con esto el certificado ha sido generado (figura 30).

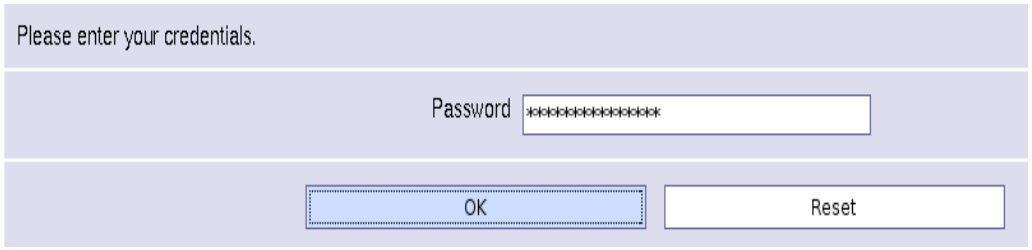


Fig. 30 Presentar las credenciales del operador

Este es una imagen del certificado generado (figura 31).

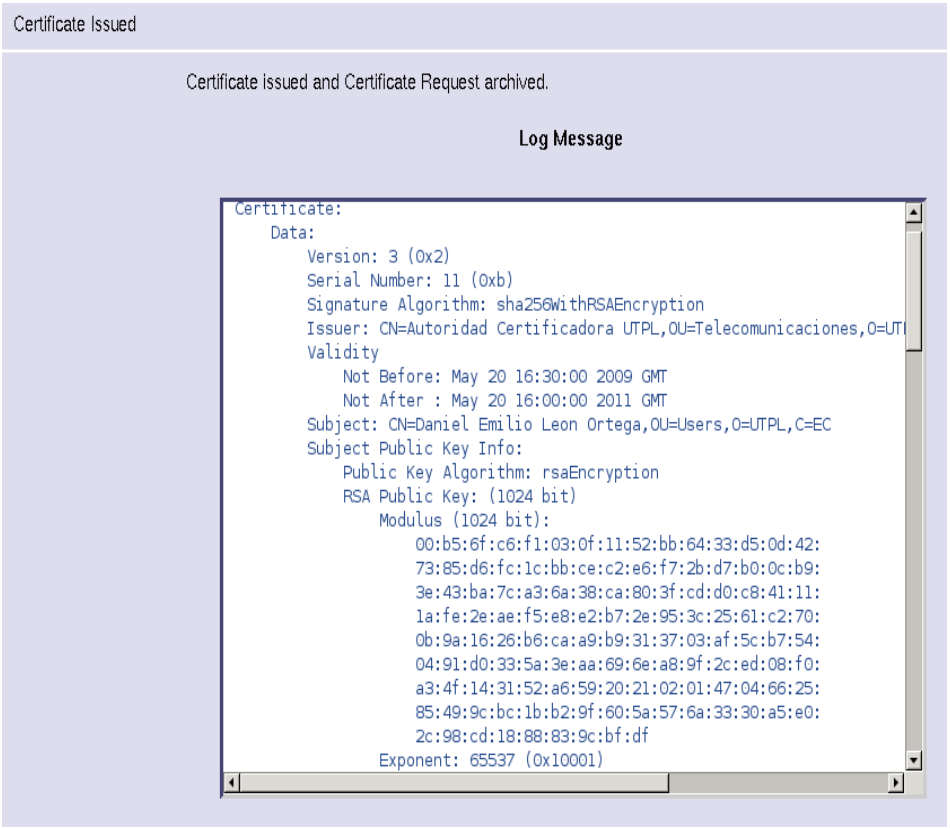


Fig. 31 Certificado generado

5.4. Intercambio de Información de CA-RA

El siguiente paso a seguir es el reenvío de esta información generada al servidor de la RA para su publicación en el sitio web de CA-UTPL. Para ello nuevamente el operador de la CA se acredita para acceder al nodo de intercambio de CA (figura 32).

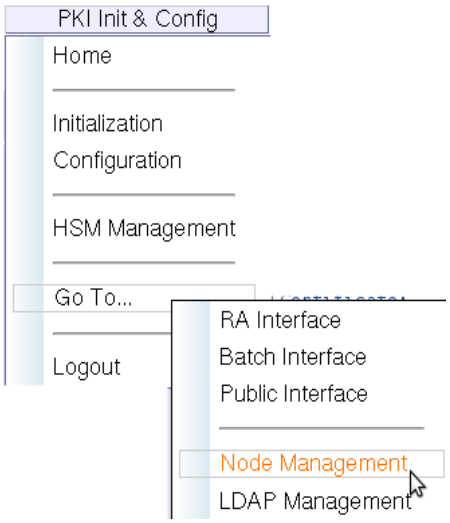


Fig. 32 Acceder al nodo de CA

En la sección ***Import/Export data*** se le presenta otra vez la pantalla de intercambio. Solo que en esta ocasión debe seleccionar la opción ***Enroll data to a lower level of the hierarchy*** y dar clic en el tag ***Certificates*****.** Con ello se repite el proceso de intercambio de información, esta vez desde la CA hacia la RA ahora con la lista de certificados emitidos (figura 33).

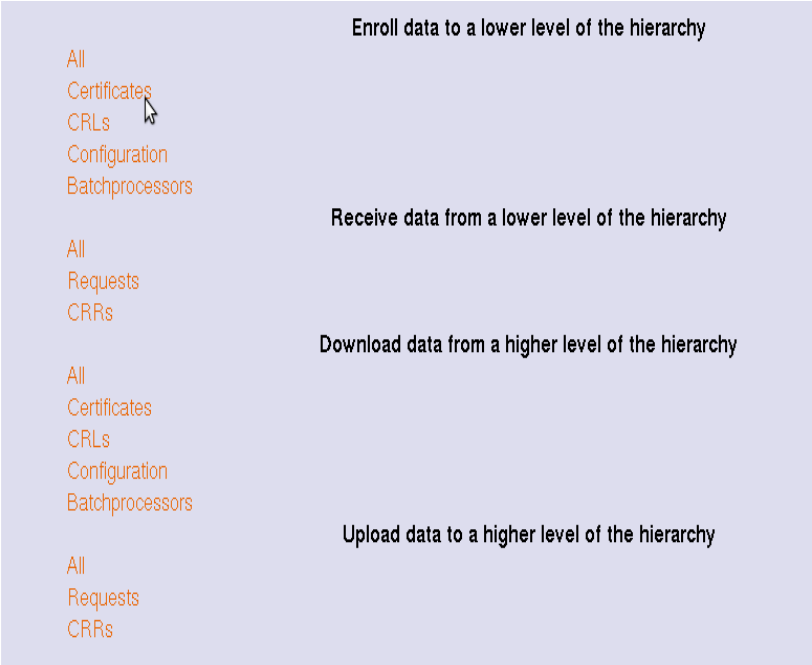


Fig. 33 Enviar certificados aprobados a la RA

En la pantalla de logs se muestra todos los certificados validos que serán transportados a la interfaz pública. Esto se puede ver en la etiqueta ***Exporting valid CERTIFICATE*** (figura 34).

Fig. 34 Certificados enviados a la RA

Es ahora el administrador de la RA el encargado de recibir esta información intercambiada. Para esto accede al nodo de intercambio de la RA y, al presentársele

una pantalla similar a la de la figura 25, escoge esta vez la opción ***Download data to a lower level of the hierarchy*** y da clic en el tag ***Certificates*** (figura 35).

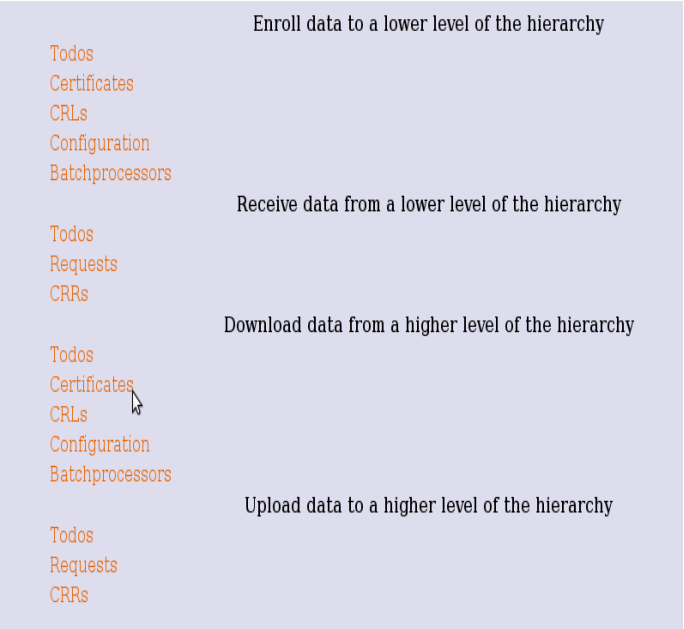


Fig. 35 Recibir certificados aprobados desde la CA

Nuevamente se nos muestra la ventana de logs informándonos de los certificados recibidos, así como los correos listos para ser enviados a sus destinatarios, es decir, información de certificados actualizada (figura 36).

Fig. 36 Certificados recibidos por la RA

En este punto el Operador de la RA es el encargado también de enviar un correo electrónico al solicitante del certificado, indicando la generación exitosa de su certificado. Luego envía un segundo mail, el cual es un CRIN (PIN de revocación cifrado) para la revocación del certificado en caso de así requerirlo (figura 37).

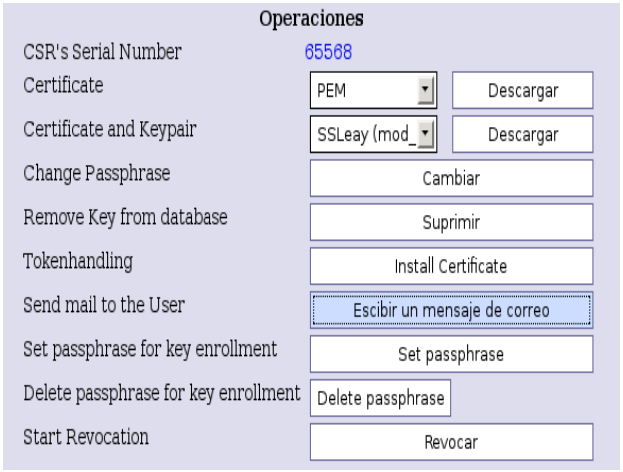


Fig. 37 Envío de e-mail al usuario

Al dar clic en ***Escribir un mensaje de correo*****,** se muestra una ventana subsiguiente, en donde se observa el email del destinatario, el número de certificado y el contenido del e-mail (figura 38).

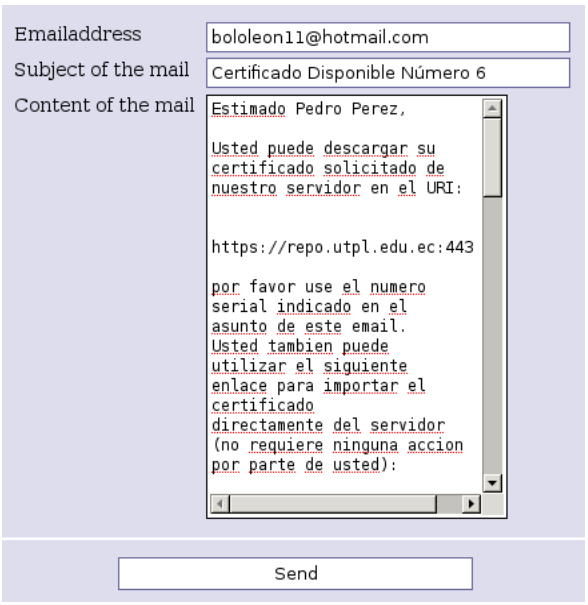


Fig. 38 Detalle del correo

Al dar clic en ***Send***, se presenta una pantalla de logs indicando el correcto envío del correo electrónico (figura 39).

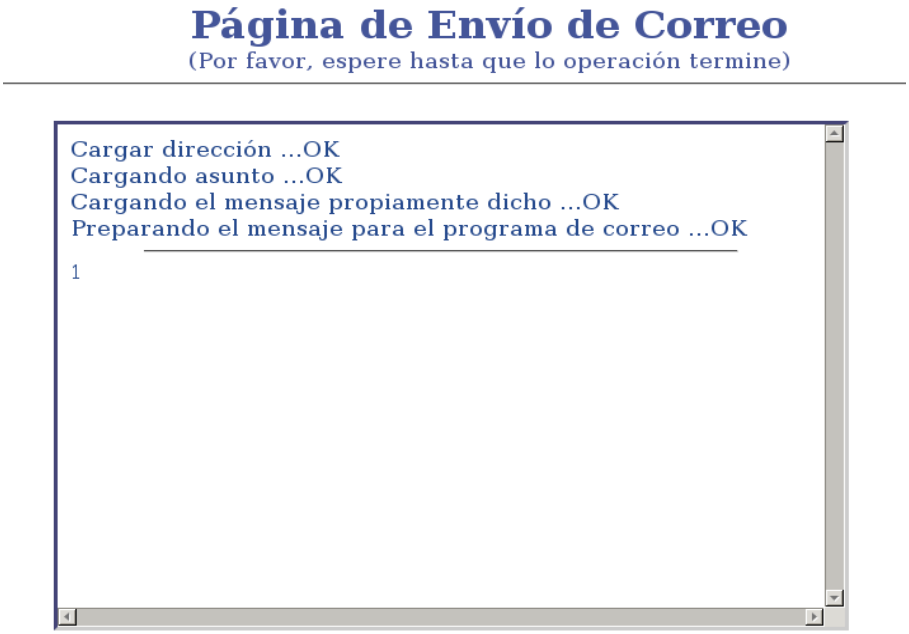


Fig. 39 Ventana de logs de e-mails enviados

5.5. Ubicación del certificado generado

Ahora el usuario puede dirigirse a la interfaz pública para comprobar que efectivamente el certificado ha sido generado. Para ello se ubica en ***Mis Certificados*** y da click en ***Certificados Validos*** (figura 40).

Fig. 40 Buscar certificados validos

Se presenta un listado con todos los certificados validos, listos para su descarga (figura 41).

Fig. 41 Lista de certificados generados

Al dar clic en el serial del certificado, se procede a ver información del mismo, así como a las opciones de descarga. Esto se encuentra detallado en el manual de usuario.

Para mejorar aun más la sincronización de la información entre los dos servidores, es una buena idea, ya en un entorno de producción, establecer dos periodos de tiempo determinados, (uno matutino y el otro vespertino) de tal forma que en el primero el servidor de la RA pueda aprobar todos los requerimientos que pueda atender. Mientras que en el segundo, el servidor de la CA puede aceptar las peticiones firmadas por la RA y generar los respectivos certificados.

6. RECOMENDACIONES FINALES

- Los servidores destinados a alojar la PKI deben estar en todo momento seguros, tanto físicamente como en lo relacionado al acceso a sus recursos lógicos. En especial el servidor que almacena la CA puesto que protege la clave privada de la CA-UTPL, cuya importancia se mencionó anteriormente.

- Se recomienda que cada servidor cuente con un administrador u operador, el cual se encargue de las operaciones inherentes a dichos servidores.

- Se debe establecer un horario entre los operadores tanto de CA como de RA, a fin de sincronizar de mejor manera las tareas de intercambio de información entre los dos servidores.

- El levantamiento de los servicios en el servidor de CA debe hacerse exclusivamente cuando se deba atender pedidos de firmas de certificados por parte del servidor RA. Es decir, es preferible que el servicio NO esté todo el tiempo activo.

- En cambio los servicios en el servidor de RA, puesto que aparte de alojar el nodo de RA contiene la interfaz pública que atiende los pedidos de los usuarios, deben estar permanentemente activos, o por lo menos el tiempo que determine el establecimiento de un horario de atención por parte del operador de RA.

- Los usuarios que requieran certificados digitales de la Autoridad Certificadora CA-UTPL deben estar informados acerca de las políticas y los procedimientos impuestos por el grupo de seguridad de PKI, lo cual implica el conocimiento de la forma de obtención y uso de sus certificados, detallados en el manual de usuario.

- Los administradores de servidores deben realizar periódicamente respaldos de información, en especial de los archivos de configuración más importantes de la aplicación.

CA – UTPL

AUTORIDAD CERTIFICADORA DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

MANUAL DE USUARIO

INDICE

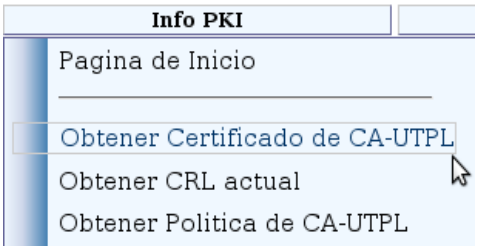
1. Sitio Web de CA-UTPL

Para obtener un certificado de CA-UTPL, ingresamos al siguiente enlace:

Se nos presenta una pantalla como la mostrada a continuación:

2. Certificado de la Autoridad Certificadora CA-UTPL

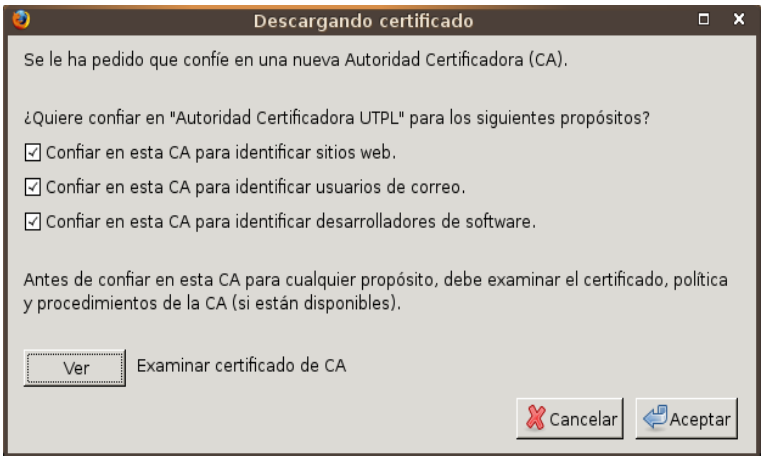
En primer lugar, antes de solicitar la generación de un certificado de usuario, debemos tener instalado en nuestro navegador el certificado de la Autoridad Certificadora en la cual confiaremos, en este caso CA-UTPL. Para lo cual nos dirigimos a ***Info PKI***, en la pestaña ***Obtener Certificado de CA-UTPL***:



Esta opción nos muestra todas las posibilidades de obtener el certificado de la Autoridad Certificadora CA-UTPL.

Seleccionamos la opción ***CA Certificate in format CRT***, para poder descargarlo en el navegador.

Aparecerá una pantalla de confirmación, en donde marcamos los tres casilleros en blanco, y pulsamos ***Aceptar***.



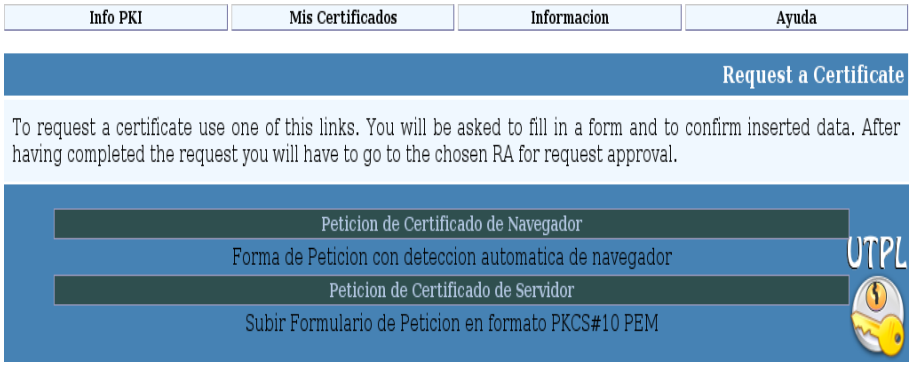
3. Solicitud de Certificado

La Autoridad Certificadora CA-UTPL puede expedir dos tipos de certificados: de usuario y de servidor.

3.1. Certificado de Usuario

Para solicitar un certificado de usuario, ingresamos a ***Mis Certificados***, y escogemos la opción ***Requerir un Certificado***.

A continuación, seleccionamos la opción ***Petición de Certificado de Navegador***.



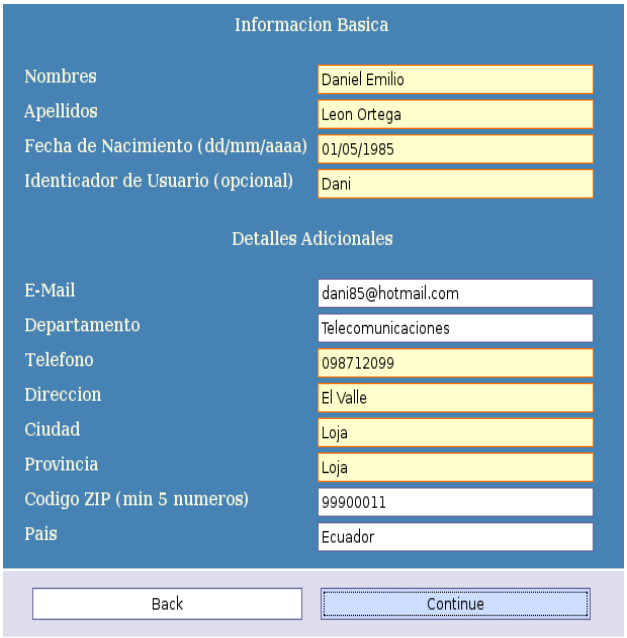
Se le presenta al usuario una nueva pantalla que contiene los siguientes campos que el usuario debe llenar:

- Información Básica

    - Nombres
    - Apellidos
    - Fecha de Nacimiento
    - Identificador de usuario (este campo es opcional)

- Detalles Adicionales

    - E-Mail (obligatoriamente la cuenta de correo de la universidad)
    - Departamento (si es estudiante becario, en el departamento en el cual presta servicios)
    - Teléfono
    - Dirección
    - Ciudad
    - Provincia
    - Código ZIP (el cual consta mínimo de 5 números a voluntad del usuario)
    - País



Al pulsar ***Continue***, se le muestra al usuario otra interfaz, en la cual el usuario debe seleccionar:

- Grupo de Petición de certificado:

El usuario debe escoger entre ESTUDIANTES, DOCENTES, ADMINISTRATIVOS Y AUTORIDADES, según su rol dentro del quehacer universitario.

- Tipo de certificado:

    - Los estudiantes, docentes, administrativos y autoridades deben seleccionar la opción ***USER*.**

    - Los administradores de servidor deben escoger cualquiera de las otras opciones presentadas, según la función que desempeñen (web, mail, etc).

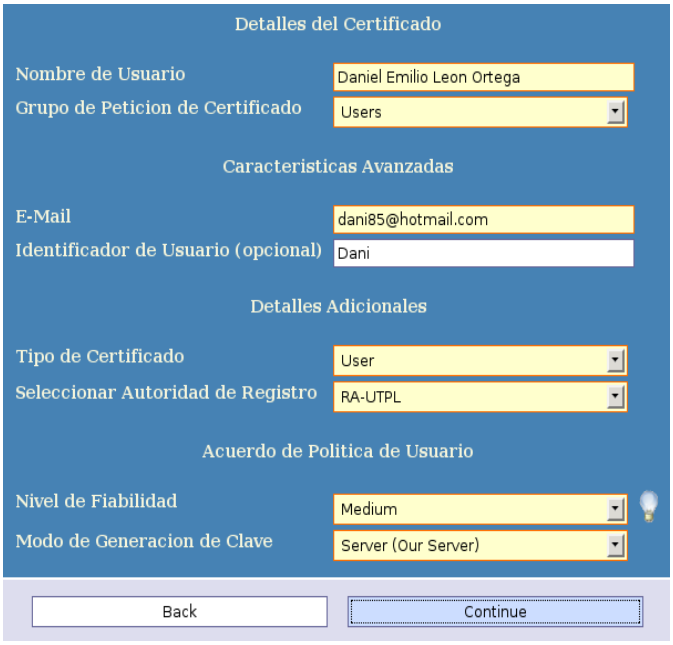
- Nivel de Fiabilidad:

De entre las varias opciones (LOW, MEDIUM, HIGH, VERY HIGH y TEST), los usuarios (estudiantes, docentes, administrativos y autoridades) pueden escoger entre ***MEDIUM*** y ***HIGH***.

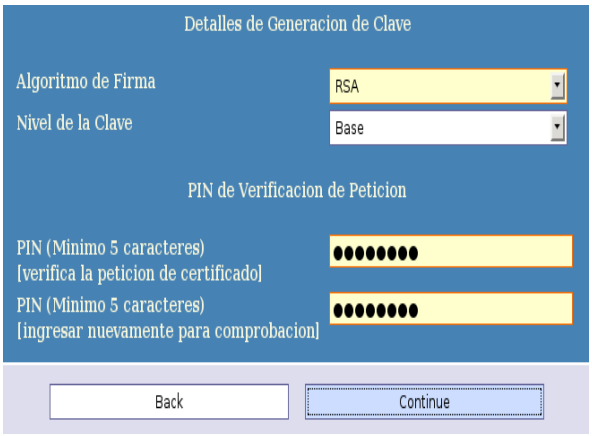
El nivel ***VERY HIGH*** es empleado para certificados destinados a administradores de servidores.

- Modo de Generación de Clave:

Hay dos alternativas, ***BROWSER*** y ***SERVER***, este último es el recomendado para todos los usuarios.



Al dar "Continue", una tercera pantalla se presenta, en la cual se muestran Detalles de la Generación de Clave, con los campos:



- Algoritmo de Firma:

Existen tres opciones (RSA, DSA y ECDSA), la más recomendable es RSA.

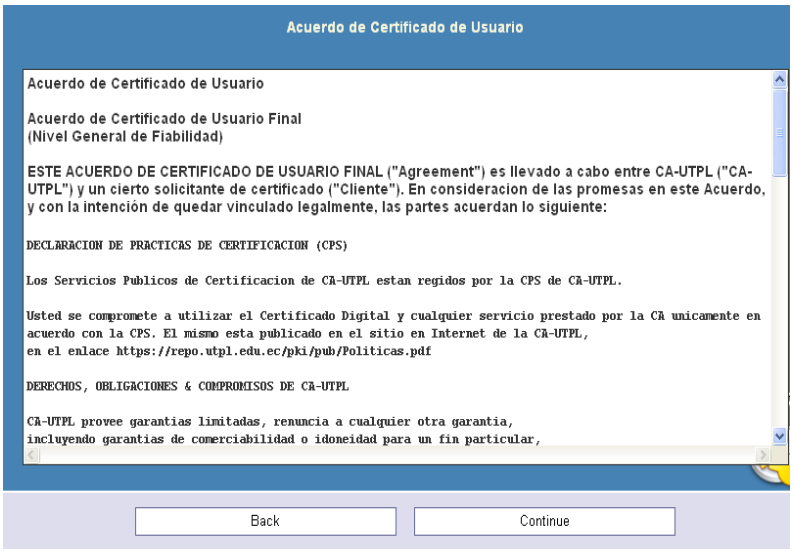
- Nivel de la Clave:

Para RSA existen tres niveles: BASE, STRONG y ADVANCED, el nivel ***BASE*** es el predeterminado.

- PIN de verificación de Petición:

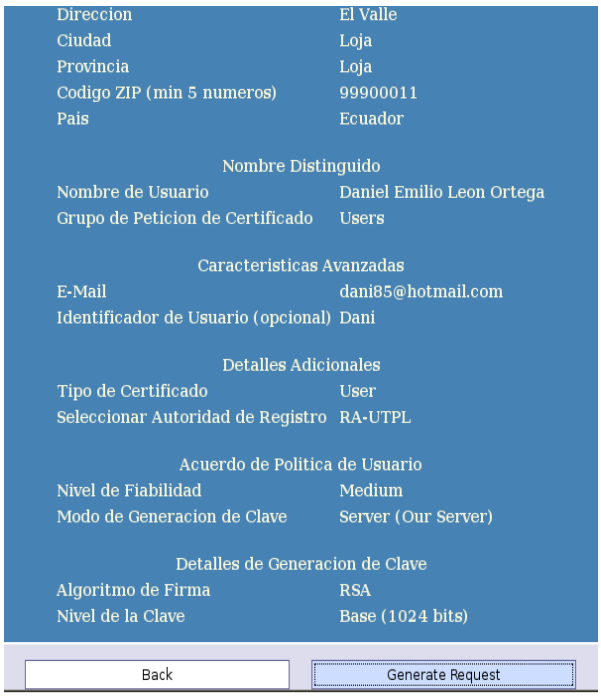
El Pin es la clave que el usuario debe ingresar para la generación de su certificado y que debe guardar celosamente.

Posteriormente está el Acuerdo de Certificado de Usuario, el cual muestra el convenio que se lleva entre la CA-UTPL y el usuario de certificado.

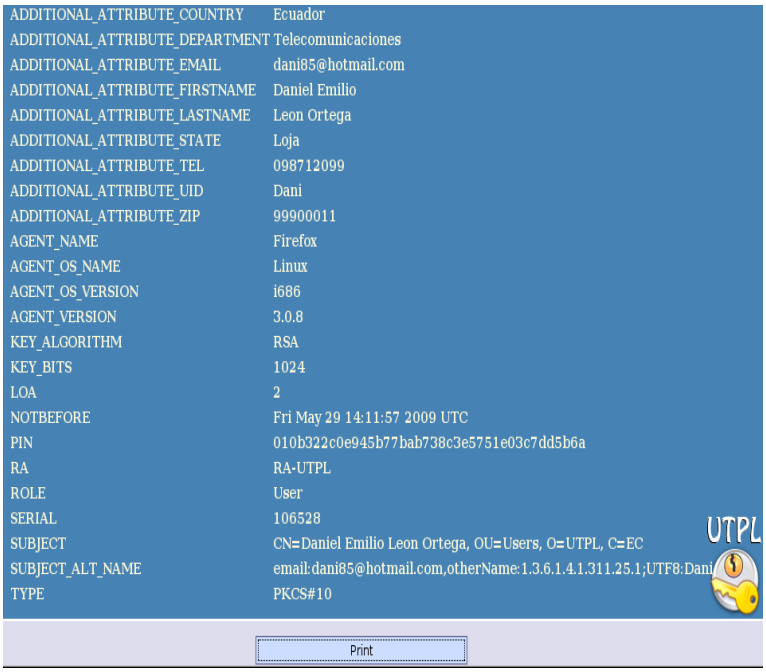


Al aceptar el anterior Acuerdo, finalmente se muestra un resumen de la Petición de Certificado que el usuario puede revisar y corregir si no esta de acuerdo haciendo click en "Back" y retornando a la página en la cual desea hacer las rectificaciones.

Si esta de acuerdo con los detalles de la petición, debe dar click en Generate Request, y asi quedara formulada su solicitud de petición de certificado para ser atendida por la CAUTPL.



Luego de haberse generado el requerimiento, existe la posibilidad de imprimir la solicitud de certificado.



3.1.1. Descarga e Instalación del Certificado

Una vez que tengamos constancia de que nuestra solicitud fue aprobada por la Autoridad Certificadora CA-UTPL, volvemos a ingresar a la interfaz de la Autoridad Certificadora CAUTPL para instalar nuestro certificado en el navegador.

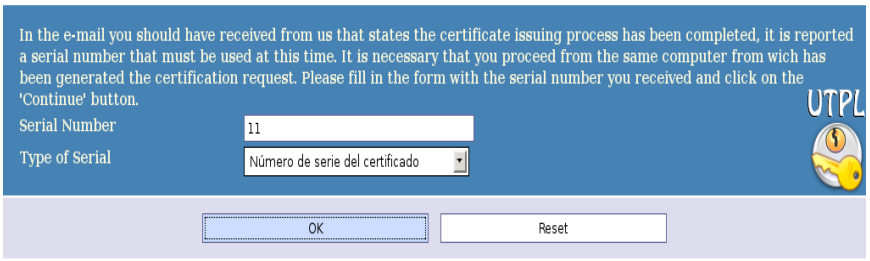
Es importante resaltar que la descarga e instalación del certificado debe realizarse en el mismo navegador en el que fue hecha la solicitud de certificación.

Existen dos formas de hacerlo:

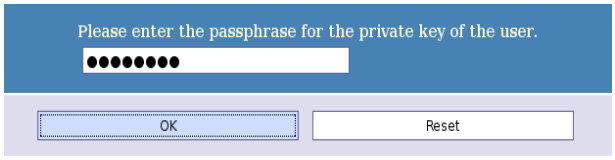
3.1.1.1. Primera Forma

Nos dirigimos a ***Mis Certificados***, a la pestaña ***Instalar mi Certificado***

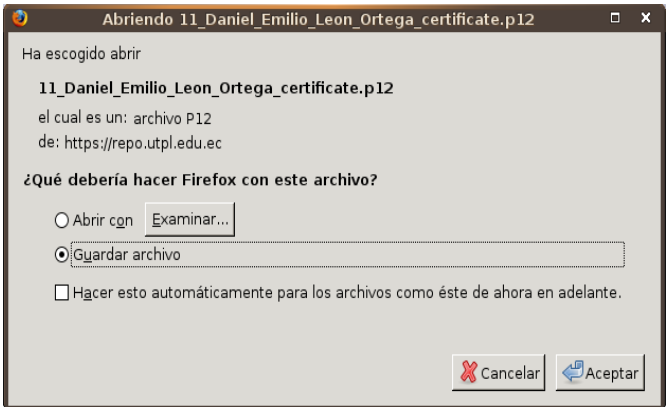
Ingresamos el ***Número de Serie del Certificado***, con lo cual nos permitirá guardar nuestro certificado para luego ser instalado en el navegador.



Se nos pide ingresar la *clave privada* del certificado.

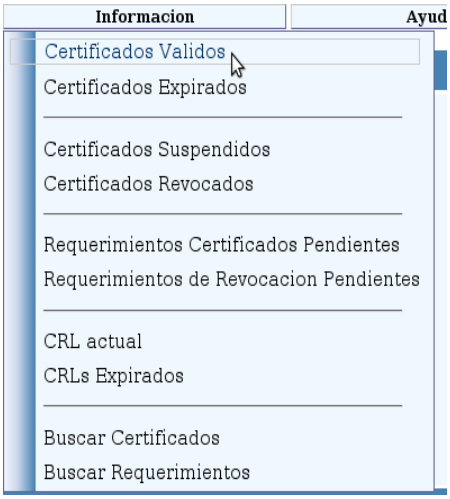


Una nueva ventana nos informa lo que debemos hacer con el certificado, marcamos *Guardar Archivo* y pulsamos *Aceptar*.



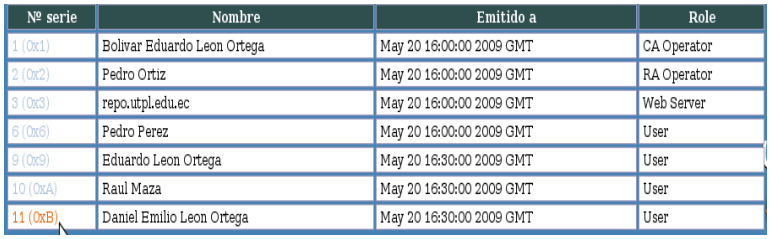
3.1.1.2. Segunda Forma

La segunda forma es ingresar en **Información** y seleccionar **Certificados Validos**



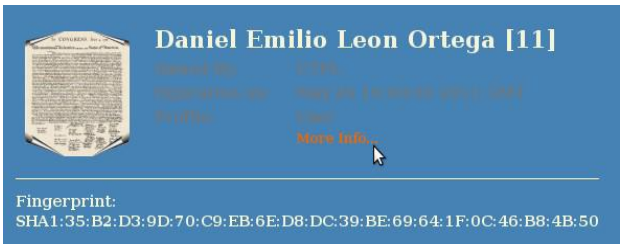
Se nos presenta una lista con todos los certificados generados por CA-UTPL.

Seleccionamos nuestro certificado y damos click en el ***Número de serie*** del mismo



Nº serie	Nombre	Emitido a	Role
1 (0x1)	Bolivar Eduardo Leon Ortega	May 20 16:00:00 2009 GMT	CA Operator
2 (0x2)	Pedro Ortiz	May 20 16:00:00 2009 GMT	RA Operator
3 (0x3)	repo.utpl.edu.ec	May 20 16:00:00 2009 GMT	Web Server
6 (0x6)	Pedro Perez	May 20 16:00:00 2009 GMT	User
9 (0x9)	Eduardo Leon Ortega	May 20 16:30:00 2009 GMT	User
10 (0xA)	Raul Maza	May 20 16:30:00 2009 GMT	User
11 (0xB)	Daniel Emilio Leon Ortega	May 20 16:30:00 2009 GMT	User

Aparece el encabezado del certificado, con información del mismo, damos click en ***More Info***.

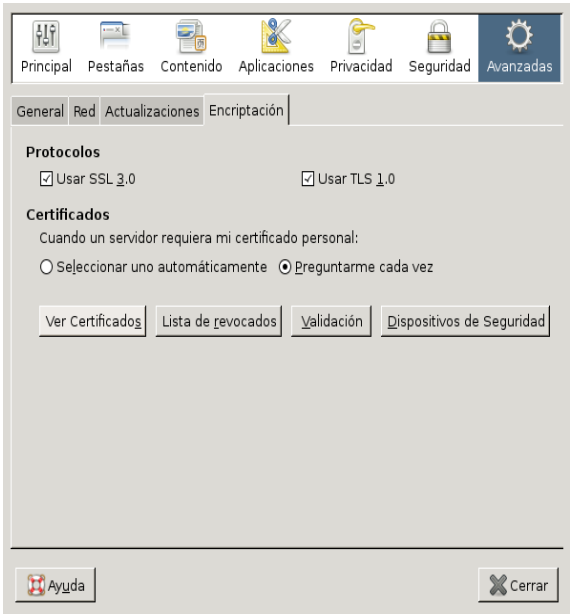


En la parte inferior de la nueva pantalla se le presenta al usuario la opción *Operaciones*.

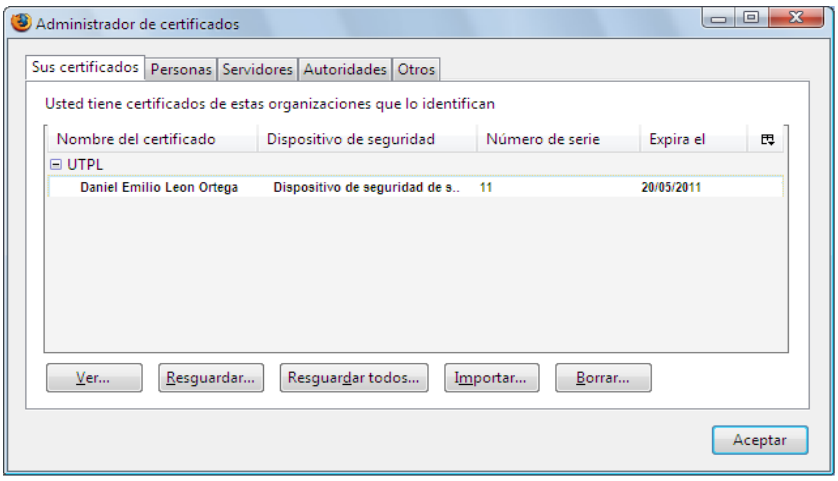
Vamos a la etiqueta ***Certificate and Keypair***, seleccionamos ***PKCS#12*** y luego presionamos ***Descargar***. Aparecerá una ventana que nos pedirá ingresar la clave privada del certificado y luego nos indicará donde guardar dicho certificado, tal como se indicó para la primera forma de descarga.

Cualquiera haya sido la forma en que instalamos el certificado, podemos constatarlo ubicándonos en el navegador en

Editar ---> Preferencias ---> Avanzadas ---> Encriptación ---> Ver Certificados

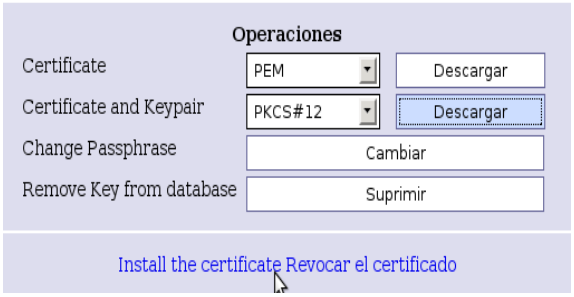


Nos ubicamos en la pestaña ***Sus Certificados*** y podemos observar el certificado ya instalado.

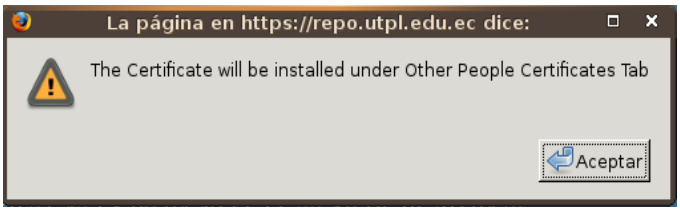


Si queremos instalar el certificado público de otro usuario de CA-UTPL para poderle, por ejemplo, enviar un mensaje firmado o cifrado, lo que debemos hacer es, en la interfaz de CA-UTPL dirigirse a ***Información-> Certificados Válidos***. Ubicamos al

usuario y damos click en su ***Número de serie***. Luego seleccionamos ***More Info***, presentándose nuevamente la pantalla *Operaciones*. Pero esta vez seleccionamos ***Install the certificate*.**



Una ventana nos indica donde será instalado el certificado. Pulsamos ***Aceptar***.

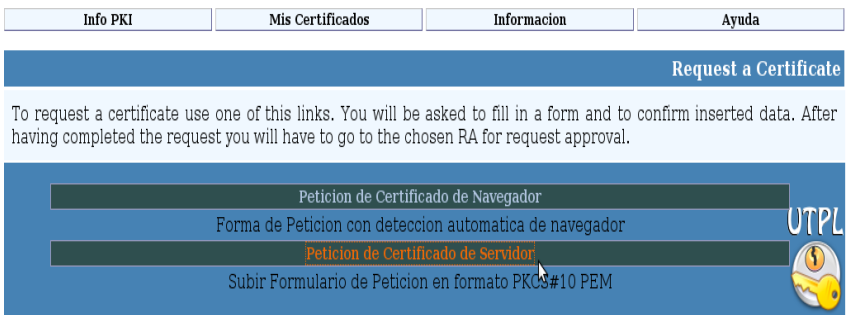


Nos ubicamos en ***Personas***, en el ***Administrador de certificados***, y allí constataremos la presencia del certificado.

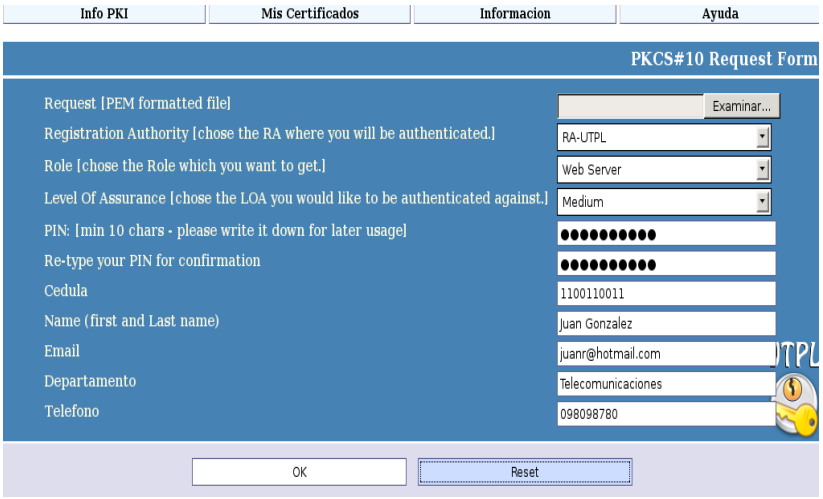
3.2. Certificado de Servidor

Para obtener un certificado de servidor, en la interfaz de CA-UTPL, El ADMINISTRADOR del servidor ingresa a ***Mis Certificados***, y escoge la opción ***Requerir un Certificado***.

Seguidamente escoge la opción ***Petición de Certificado de Servidor***.



Llenamos los datos que se nos solicitan. El archivo en formato PEM (PKCS#10) debe ser generado previamente por el administrador del servidor y adjuntado.



- *Registration Authority*: Es el nombre de la Autoridad de Registro, por defecto es RA-UTPL.

- *Role*: Presenta los diferentes tipos de rol que puede tomar el servidor, por ejemplo Web Server, CA Administrator, RA Operator, web mail.

- *Level of Assurance*: Al igual que para los certificados de usuario, los niveles pueden ser *Low, Medium, High y Very High*. Para los servidores, el nivel recomendado es ***high*** para los menos críticos y **very high**

- PIN: O clave de seguridad que es suministrada por el administrador del servidor. Debe ser una clave segura, difícil de descifrar pero fácil de recordar para el administrador.

- Repetir el PIN: La misma clave anterior para confirmación.

- Cédula: El numero de cedula del administrador del servidor.

- Nombre: El dominio del servidor o algún nombre que identifique al servidor.

- E-mail: La dirección de correo del administrador del servidor (la cuenta de correo de la UTPL).

- Departamento: El área en la cual está ubicado el servidor o en la cual presta servicios.

- Teléfono: Convencional o móvil del departamento en donde está ubicado el servidor, o del administrador.

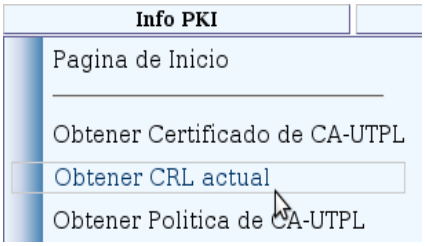
Luego de que la petición ha sido aprobada por la RA y posteriormente firmada y generada por la CA, puede ser descargada e instalada como en el caso del certificado de usuario.

4. Descarga de la Lista de Revocación de Certificado (CRL)

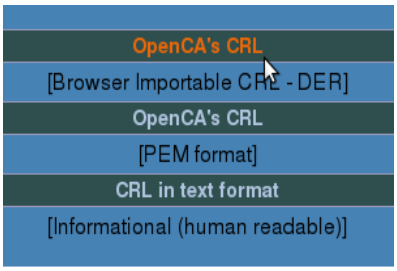
La CRL contiene información de los certificados que han sido revocados por CA-UTPL, es decir los certificados que ya no tienen validez.

La forma de hacer la descarga por parte del usuario es de la siguiente manera:

El usuario debe dirigirse a la página web de CA-UTPL, y en la pestaña *Info PKI*, escoger la opción *Obtener CRL actual.*



Posteriormente debe seleccionar la primera opción (Browser Importable CRL - DER).



Se muestra una ventana sobre el Estado de la Importación de CRL, la cual confirma la exitosa instalación de dicha CRL. Con ello queda instalada en el navegador la Lista de Revocación de Certificados actual.

5. Informes y Contacto

UTPL
Unidad de Proyectos y Sistemas Informáticos (UPSI).
Grupo de Telecomunicaciones.

1. Manual de Procedimientos

1.1. Proceso de petición de certificación por parte del usuario

1.1.1. Los usuarios (ya sean estudiantes, docentes, administrativos y autoridades), deberán llenar una solicitud de petición de certificado diseñada para el efecto, misma que reposa en la página web de la Autoridad Certificadora CA-UTPL, en la dirección ***https://repo.utpl.edu.ec/pub***.

1.1.2. El solicitante deberá escribir todos los datos requeridos en el formulario, sin faltar a la verdad, incluido el PIN que no es otra cosa que un número usado para la identificación del solicitante.

1.1.3. Una vez generada la solicitud de petición de certificado, el solicitante deberá presentarse junto con una copia de su cédula de identidad y su carnet (de estudiante, docente, administrativo) que lo acredite como miembro activo de la comunidad universitaria, ante el administrador de la Autoridad de Registro (RA), a fin de que éste pueda atender su petición.

1.2. Proceso de aprobación de la petición por parte del administrador

1.2.1. El administrador de la RA-UTPL comprobará que el solicitante mantiene relación contractual con la UTPL, En el caso de un alumno, comprobará que esté matriculado en el ciclo académico actual. Si se trata de un docente o personal administrativo, comprobará que se encuentre contratado en ese momento.

1.2.2. Esta comprobación se realizará mediante consultas a las bases de datos de la institución o en su defecto al personal encargado de proporcionar esa información, también puede hacerse mediante presentación de resguardo de matrícula en caso de alumno y/o contrato laboral en caso del personal. Posteriormente la Autoridad de Registro puede integrarse con el Sistema de Gestión Académica y con el de Recursos Humanos a fin de agilizar este procedimiento.

1.2.3. Una vez que el administrador de RA haya comprobado la validez de la información presentada por el solicitante, así como la identidad del mismo, ***aprobará*** la solicitud electrónica de certificado que el usuario previamente ha llenado en la página de la Autoridad Certificadora, y que se encuentra almacenada en el servidor de la RA. Esta solicitud quedará en poder del administrador de la RA, el cual es el encargado de hacerla llegar al administrador de la Autoridad de Certificación CA-UTPL, la cual cuenta con no más de diez días para ***firmar*** la petición.

1.2.4. Asimismo, paralelamente y a manera de respaldo, se creará un documento de solicitud (en papel), en el que se recojan los siguientes datos: Fecha de la solicitud, datos del solicitante (Nombre del Solicitante, cédula, Departamento al cual pertenece, Numero de Teléfono, extensión telefónica en caso de ser empleado de la Universidad), PIN cifrado. Estos datos

deberán quedar a cargo del administrador de la RA, quien está en la obligación de mantener la confidencialidad de esta información.

1.3. Proceso de Notificación por parte del administrador de RA al usuario.

1.3.1. Luego de que el administrador de la CA haya firmado y generado el certificado digital de usuario, debe retornarlo al administrador de la RA-UTPL, el cual enviará un correo electrónico de notificación al solicitante del certificado, informándole que puede descargar su certificado desde la URL de la página en donde realizó la petición.

1.4. Proceso de Certificación para servidores

1.4.1. El solicitante de un Certificado de Servidor será su responsable directo (es decir su administrador) y deberá disponer de una credencial de Identidad Personal emitida por CA-UTPL. Asimismo debe presentarse con una copia de su cedula de identidad.

1.4.2. Además de llenar los datos del servidor que se presentan en el formulario de petición alojado en la página web de CA-UTPL, el administrador deberá adjuntar el archivo con formato PKCS#10, que es el archivo de la petición del servidor, con el cual la CA-UTPL va a generar el certificado, generado por el propio administrador.

1.4.3. El administrador del servidor deberá presentarse ante el administrador de la Autoridad de Registro para que éste pueda confirmar la autenticidad y validez de las credenciales presentadas por el solicitante, una vez verificada, el administrador de RA aprobará la solicitud de petición.

1.4.4. Con la solicitud electrónica de certificado de servidor aprobada, la cual quedará en poder del administrador de la RA, este será el encargado de hacerla llegar al administrador de CA, el cual cuenta con un periodo de no más de diez días para generar el certificado.

1.4.5. Una vez emitido el certificado, el administrador de RA se encargará de comunicar al administrador correspondiente que su servidor ya posee un certificado digital.

1.5. Proceso de descarga del certificado (para usuarios y servidores)

1.5.1. Luego de que el usuario haya sido notificado de que su certificado digital ha sido emitido, debe dirigirse al sitio web de CA-UTPL para poder descargarlo.

1.5.2. Solo podrá hacerlo proporcionando la clave privada que ingresó al momento de formular la petición.

1.5.3. Existen dos formas de descargar el certificado del sitio web, las cuales están cubiertas en el manual de usuario, en el **anexo [3-14]**.

1.5.4. Luego de descargado el certificado, la mejor opción para el usuario seria almacenarlo en un token criptográfico, para que de esta forma gane en seguridad y portabilidad.

1.6. Proceso de revocación

1.6.1. A petición del usuario

1.6.1.1. Una vez que el poseedor de certificado haya justificado debidamente las razones por las cuales quiere revocar su certificado ante el administrador de RA, éste procede a revocarlo de la siguiente manera:

1.6.1.2. En todo certificado, al momento en que es generado, automáticamente se crea un CRIN o Pin de Revocación, el cual queda en poder del administrador de RA.

1.6.1.3. Con este CRIN, el administrador se dirige al sitio web de CA-UTPL, a la parte correspondiente a *Revocación de Certificados*. Ingresa el número de serie del certificado a revocar, proporciona el CRIN cuando se lo pida la aplicación; y de esta manera genera la solicitud de petición de revocación.

1.6.1.4. Luego accede a su interfaz, atiende la petición de revocación y la aprueba, posteriormente la envía al administrador de CA para que la firme y genera la nueva lista de revocación de certificados (CRL)

1.6.1.5. Luego de generada la revocación, el administrador de RA notifica al usuario que su petición ha sido atendida.

1.6.1.6. Además pone a disposición del resto de usuarios la nueva CRL con el o los nuevos certificados revocados, es decir no validos.

1.6.2. Por decisión de CA-UTPL

1.6.2.1. El administrador de RA podrá revocar unilateralmente un certificado digital de usuario si comprueba que la clave privada de dicho certificado ha sido divulgada de manera que ponga en riesgo la seguridad de la infraestructura; o compruebe que el estudiante, docente u otro usuario perteneciente a cualquier otro rol ya no forma parte de la universidad.

1.6.2.2. El administrador de RA procederá de igual forma como en el caso de revocación a petición de un usuario.

Implementación de una Infraestructura de Clave Pública (PKI) en la Universidad Técnica Particular de Loja

Msc. Ma. Paula Espinoza, Bolívar León Ortega

Resumen- *El presente artículo es una síntesis del analisis, los procedimientos realizados, las herramientas utilizadas y una evaluación de alternativas disponibles, llevadas a cabo para lograr la implementación de una Infraestructura de Clave Pública (PKI [1]) en el entorno de la Universidad Técnica Particular de Loja, empleando el software OpenCA.*

I. INTRODUCCIÓN

En un proyecto desarrollado anteriormente **[1]** se ha evaluado e identificado ya la necesidad que tiene la Universidad Técnica Particular de Loja (UTPL) de implementar en sus sistemas ciertos mecanismos que tengan como objeto el aseguramiento de las transacciones y procedimientos que manejan dichos sistemas.

En dichos proyectos se han realizado estudios sobre la Infraestructura de Clave Pública (PKI), sus características, ventajas, desventajas y aplicabilidad en nuestra universidad. Todos estos estudios han determinado implementar la PKI en el entorno de la UTPL como el mecanismo para lograr los objetivos descritos en el párrafo anterior.

El rol principal de PKI es el de establecer identidades digitales en las que se pueda confiar, las cuales se pueden usar junto con mecanismos criptográficos para prestar servicios de seguridad como la autenticación, autorización o validación de una firma digital, garantizando así la confianza de los usuarios del servicio. Dichas identidades son plasmadas en los certificados digitales, emitidos por las llamadas Autoridades de Certificación, el centro de una PKI.

Una organización que emita identidades digitales de confianza, como pretende hacerlo la UTPL a través del establecimiento de una Autoridad de Certificación autofirmada propia (llamada en adelante CA-UTPL) debe tener el respaldo y la credibilidad de las personas que van a beneficiarse de sus servicios (personal docente, alumnado, personal administrativo) de tal forma que éstas puedan confiar plenamente en las prestaciones que van a recibir de dicha Autoridad de Certificación.

Para tal efecto, la PKI debe estar integrada con el sistema de seguridad interno y externo de la universidad, mediante la ubicación idónea dentro de la red de la universidad, para realmente brindar servicios de seguridad confiables.

II. INFRAESTRUCTURA DE CLAVE PÚBLICA

Una Infraestructura de Clave Pública es un conjunto de aplicaciones y de servicios que nos permite utilizar la criptografía de clave pública o asimétrica de una forma fácil y efectiva. Esta criptografía utiliza un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. **[2]**

La Criptografía de Clave Pública ofrece cuatro características que respaldan el aseguramiento de la información, estas características son la ***autenticación*** que asegura la identidad de un usuario, bien como firmante de documentos, ya que sólo él puede conocer su clave privada, evitando así la suplantación; el ***no repudio*** que impide que una vez firmado un documento el firmante del mismo se retracte o niegue haberlo redactado), la ***integridad*** de la información, que previene la modificación deliberada o accidental de los datos firmados, durante su transporte, almacenamiento o manipulación y el acuerdo de claves secretas para garantizar la ***confidencialidad*** de la información intercambiada.

---

[1] **P**ublic **K**ey **I**nfraestructure

A. Analisis de los requerimientos de los usuarios de la UTPL

Luego de revisar brevemente las características de PKI, se procede a realizar su implementación de acuerdo a las necesidades de la Universidad.

Como anteriormente se manifestó, se busca poner en marcha una Autoridad Certificadora propia de la UTPL, que se encargue de la administración de certificados digitales para dos grupos bien diferenciados: usuarios finales y los servidores de la universidad.

Dentro del primer grupo están comprendidos tanto estudiantes, docentes, personal administrativo como administradores de los servidores que funcionan en los predios universitarios.

Los servidores en sí constituyen el otro sector al cual irán enfocados los servicios de la Autoridad Certificadora.

Los niveles de seguridad empleados en la generación de certificados digitales para uno y otro grupo serán distintos, dando un mayor énfasis a los certificados generados para la autenticación de servidores, dada la importancia de éstos en el manejo de toda la información relacionada con la Universidad Técnica Particular de Loja.

Dentro del grupo de usuarios finales, la generación de certificados está orientada a lo que son las firmas digitales y el cifrado de datos, que proporcionan el aseguramiento de los mensajes de correo electrónico, los mismos que generalmente viajan en texto plano por la red, y en el caso de ser interceptados, son fáciles de leer por personas que no son el destinatario. La eficacia de estas técnicas mejora a través del uso de tokens criptográficos. Estos dispositivos, también llamados token USB proveen simplicidad, seguridad y facilidad de uso para soluciones PKI, generando claves de usuario y almacenándolas en el mismo token.

Para la generación de certificados digitales, ya sea para usuarios finales o para servidores, es necesario establecer primero la Autoridad de Certificación, conocida de aquí en más como CA, la cual se encargue del manejo del ciclo de vida de los certificados. Asimismo se debe elaborar la CP/CPS[2], la cual define las reglas y prácticas que toda CA debe seguir en el manejo de certificados.

El nombre de la CA de la UTPL es el de CA-UTPL.

Para comenzar la estructuración de la CA, es de gran importancia determinar la herramienta apropiada para llevar a cabo tal fin.

De entre las variadas alternativas disponibles, se seleccionó OpenCA.[3]

B. Modelo de confianza de la PKI

El modelo de confianza escogido para la implementación de PKI en la UTPL es el *modelo jerárquico*, el cual consta de una sola CA que es la CA raíz, bajo la cual se subordinan una o varias RA[4]. Inicialmente existe una sola RA que atenderá las peticiones de certificación de los usuarios, pudiéndose extender en el futuro a mas RA's.

Este modelo se muestra en la figura 1.

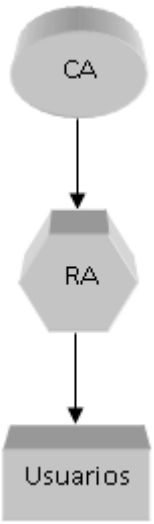


Figura 1. Modelo jerárquico de la PKI

---

[2] **CP/CPS: C**ertificate **P**olicy and **C**ertification **P**ractice **S**tatement.

[3] Información disponible en www.openca.org

[4] **RA:** Autoridad de Registro.

- **Descripción del Modelo**

La descripción del modelo de detalla a continuación:

La CA almacena toda la información sensible de la PKI, como son las claves privadas tanto de la propia CA como la de los usuarios a los cuales genere los certificados digitales.

Asimismo se encarga de la generación de los certificados de usuario, una vez sus solicitudes de petición hayan sido aprobadas por la RA; y de la elaboración de las CRL's[5].

La RA es la encargada de atender todas las peticiones de certificación por parte de los usuarios de la PKI, revisarlas para verificar si efectivamente el solicitante forma parte de la comunidad universitaria, ya sea como estudiante, docente, administrativo o administrador de algún servidor, y posteriormente generar la CSR[6] que será tratada posteriormente por la CA.

El acceso a la CA está restringido para todos los usuarios de la PKI, solo podrá tener acceso a ella la interfaz RA, y exclusivamente para funciones de intercambio, es decir, enviar las peticiones aprobadas por la RA hacia la CA, y recoger los certificados generados por la CA para su publicación y distribución hacia los usuarios que lo solicitaron; así como también las CRL's que contienen información acerca de los certificados revocados.

Tanto la interfaz CA como la RA estarán bajo el manejo de un administrador por cada una de ellas, los cuales se encargarán de realizar las funciones descritas anteriormente.

Una vez generado el certificado de usuario, éste puede descargarlo de la interfaz de RA y almacenarlo en un dispositivo de seguridad como un token criptográfico, el cual internamente realiza funciones como firma digital, y además es portable para el usuario.

- **Implementación del Modelo**

De acuerdo al modelo antes descrito, se realizó la implementación del mismo según el siguiente esquema (figura 2).

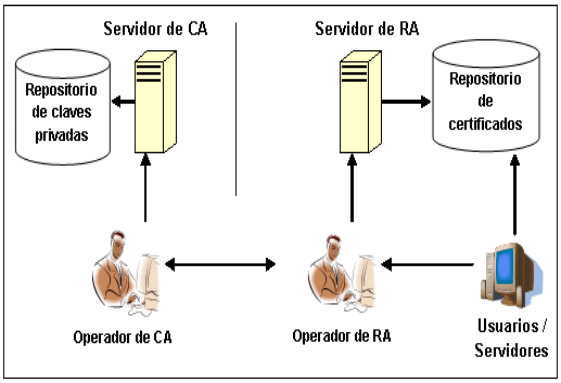


Figura 2. Implementación de la PKI

Se requieren dos servidores para este objetivo:

El primero de ellos se encarga de alojar la interfaz de CA, la cual, como se manifestó anteriormente, debe estar en contacto únicamente con la interfaz de RA, por tal motivo no tiene contacto alguno con red lógica alguna, menos aun con el internet.

El repositorio de claves privadas mantiene almacenadas ese tipo de claves tanto de los usuarios como de la propia autoridad certificadora.

El segundo servidor alberga la interfaz RA con todas las funciones que ella realiza. Como atiende las peticiones de certificación de los usuarios, debe necesariamente ser accesible por los mismos.

Todos los certificados y las Listas de revocación de certificados generados por la CA y que son enviados a la interfaz RA, son almacenados en el repositorio de certificados en donde están a disposición de los usuarios que los han solicitado.

III. Implementación de PKI

A. Requerimientos software

---

[5] **CRL: C**ertificate **R**evocate **L**ist (Lista de revocación de certificados)

[6] **CSR: C**ertificate **S**igned **R**equest (Petición de firma de certificado)

De acuerdo al analisis efectuado en **[1]**, de entre las diversas alternativas evaluadas, se escogió trabajar con OpenCA, debido entre otras cosas al hecho de que es una herramienta open-source, y actualmente la UTPL se encuentra fomentando el estudio y la investigación de proyectos de software libre.

Además pone a disposición todo el código fuente, lo cual permite a la comunidad interesada brindar sus aportes para mejorar el software.

Por último cabe resaltar la ventaja que significa el costo en su implementación, el cual esta supeditado a la capacitación y el conocimiento en sí de la herramienta.

OpenCA a su vez se fundamenta en otras aplicaciones open-source para su correcto funcionamiento, como OpenLDAP, OpenSSL, Apache y Apache mod_ssl.

Es un proyecto surgido en 1998, el cual ha ido evolucionando basado siempre en principios como:

- Adhesión a los estándares IETF[7].
- Evolución en base al feedback dado por los usuarios y desarrolladores.
- Interoperabilidad para adherirse a los estándares como para ajustarse a distintas plataformas y ambientes (inclusión de Applets de JAVA para soportar Microsoft Internet Explorer).
- Uso de lenguajes de programación simples en la medida de lo posible **[3]**.

Antes de proceder a la instalación de OpenCA, se requiere que el sistema cuente con software libre preinstalado para soporte web, de base de datos y ciertos módulos Perl[8] utilizados para lograr una completa compatibilidad con la herramienta openca. Dicho software así como las versiones empleadas se muestran en la figura 3.

	Software	Versión
Sistema Operativo	Debian (interfaz CA) Ubuntu (interfaz RA)	8.04
Base de Datos	MySQL	5.0.45-7.el5
Servidor Web	Apache OpenSSL (interfaz RA)	2.2.6 0.9.8b
Módulos Perl	Perl	5.8.8-15.el5

Figura 3. Requerimientos software para la instalación de OpenCA

Para implementar la PKI, se ha utilizado el paquete ***openca-base 1.0.2.tar.gz*** que al momento es la más reciente en ser liberada. Además del paquete complementario ***openca-tools 1.0.0***.

B. Requerimientos hardware

De acuerdo a lo descrito en la implementación del modelo de la PKI, se destinaron dos servidores para cumplir con los requerimientos de implementación de la Infraestructura de Clave Pública.

Las características físicas de cada uno de los servidores se muestran en la figura 4, presentada a continuación:

	Servidor CA	Servidor RA
Sistema Operativo	Debian Etch	Ubuntu
Procesador	(1) 2,33 Ghz	(3) 2,4 Ghz
Memoria	2 Gb	2 Gb
Espacio en disco	70 Gb	290 Gb

Figura 4. Características de los servidores CA y RA

Los dos servidores fueron ubicados en el sitio más seguro de la red lógica de la universidad, con el fin de ser monitoreados y controlados permanentemente, de manera que el acceso a ellos sea reservado exclusivamente a sus administradores. Especialmente el servidor de CA que como se manifestó, es el más crítico por toda la información que en él se almacena.

Esta ubicación lógica es mostrada en forma gráfica en la figura 5.

---

[7] **IETF**: **I**nternet **E**ngineering **T**ask **F**orce [http://www.ietf.org]

[8] **Perl:** Lenguaje de Programación, toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp, etc.

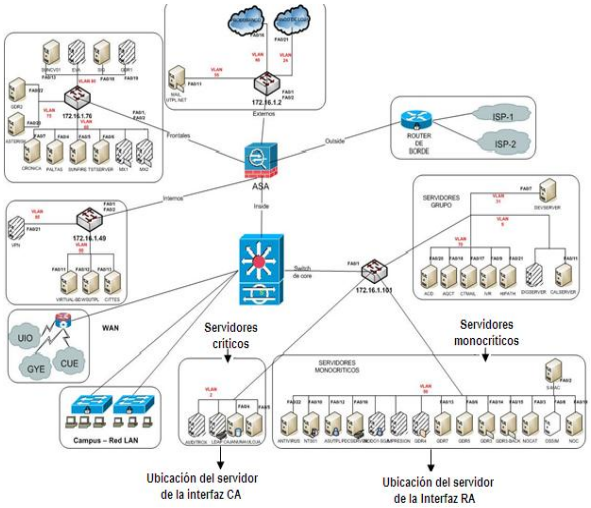


Figura 5. Ubicación de los servidores dentro de la red de la UTPL

C. Instalación de OpenCA

El software OpenCA esta constituido entre otras por las siguientes interfaces básicas, según lo describe **[4]**:

- CA, que contiene todas las funciones necesarias para crear certificados y listas de revocación de certificados.
- RA, que está capacitada para manejar funciones como la edición, aprobación o eliminación de requerimientos, ceración de claves privadas y notificación a usuarios.
- PUB, o Interfaz Pública, encargada de la interacción entre los usuarios y la RA, es decir permite a los usuarios solicitar, descargar o revocar certificados, descargar la CRL actualizada o buscar certificados de otros usuarios de CA-UTPL, por medio de una interfaz web.
- NODE, administra la base de datos y las funciones de exportación e importación entre CA y RA.

Se instaló la interfaz CA en un servidor independiente, el cual funciona de forma ***offline*** para garantizar que quede aislada de la red; la manera de hacer esto es emplear el parámetro ***make install offline*** al momento de la instalación. El servidor CA tiene como sistema operativo una distribución GNU/Linux denominada Debian.

Las interfaces RA y Pub en cambio fueron agrupadas en el segundo servidor, el cual corre bajo otra distribución GNU/Linux como es Ubuntu y está conectado a la red, para atender las peticiones de los usuarios vía web.

Una vez instaladas las interfaces en los distintos servidores, en cada uno de ellos se generan directorios en los cuales se crean ***templates***, que son archivos modificables y que hacen referencia al archivo principal denominado ***config.xml***, el cual contiene los parámetros de configuración principales, necesarios para la inicialización de openca; generalmente se encuentra ubicado bajo el directorio ***/PREFIX[9]/etc/openca/*** .

Luego de que se hayan realizado las modificaciones necesarias tanto a los templates como al archivo config.xml, se ejecuta el script ***configure_etc.sh***, el cual carga los nuevos parámetros que se hayan configurado últimamente en estos archivos.

Finalmente al ejecutar ***openca_start***, se levanta el servicio openca, y el software comienza a funcionar.

D. Configuración de OpenCA

Las secciones del software openca que debieron ser revisadas y/o modificadas son:

- **Control de Acceso:** OpenCA basa la configuración del control de acceso a las diferentes interfaces mediante XML. Se empleó el método **passwd** con autenticación soportada en una base de datos interna, que permite que uno o más usuarios puedan ser habilitados ingresando un login y un password, a este password se le aplica una función *hash*[10] ya sea por cualesquiera de los siguientes algoritmos: SHA1, MD5 o Crypt, con lo cual se garantiza la autenticidad de la contraseña ingresada por el usuario.

---

[9] **/PREFIX:** Directorio raíz de instalación de openca

[10] **HASH:** Comprimen un texto en un bloque de longitud fija, se utilizan en autenticación y firma digital.

Los archivos de control de acceso se agrupan en ***/PREFIX/etc/openca/access_control***, tanto en el servidor RA como en CA. No está por demás indicar que el/los usuario(s) autorizado(s) a acceder a las interfaces CA y RA deben proporcionar passwords seguros, fáciles de recordar, y renovarlos periódicamente.

- **Requerimientos de Certificación:** La Autoridad Certificadora CA-UTPL genera certificados tanto para usuarios como para servidores que pertenezcan a sus instalaciones. OpenCA para ello proporciona dos archivos configurables para cada tipo de petición:

Para el caso de los usuarios como estudiantes, docentes o personal administrativo, las peticiones serán realizadas de la misma forma, independientemente del navegador que estén empleando, puesto que la herramienta proporciona soporte tanto para Mozilla, Firefox, Konqueror, Opera e IE6 y 7. El archivo que administra todos los parámetros de petición de certificado para usuarios, como los perfiles de los mismos, el nivel de seguridad en la generación de sus certificados, los modos de generación de clave (a través de navegador o de servidor), los tipos de clave permitido (entre RSA[11], DSA[12] o ECDSA[13]) y el tamaño que puedan tener estas claves de acuerdo a las capacidades del navegador y al tipo de petición es ***browser_request.xml***.

Para el caso de petición de certificados para servidor, el archivo que maneja todos los parámetros de petición se denomina ***server_request.xml***. Ambos archivos se encuentran en el directorio ***/PREFIX/etc/openca***.

- **Niveles de Seguridad:** o LOA[14] son aplicados de acuerdo al tipo de usuario que solicita un certificado digital. Los niveles de seguridad que la aplicación son: *Low, Medium, High, Very High y Test* (este último únicamente para propósitos de testeo). El nivel de seguridad que adopte cada usuario está determinado por las políticas de certificación que CA-UTPL determine.

La ubicación del archivo que maneja las distintas LOA's para los diferentes tipos de usuario es ***PREFIX/etc/openca/loa.xml***.

- **Interfaz de Usuario:** La interfaz de usuario es el único módulo de OpenCA al cual no se le aplican modificaciones en lo relacionado al control de acceso, puesto que es el que se encarga de atender las peticiones de todos los usuarios en general, así que debe estar disponible para cualesquiera que solicite su certificado de usuario, siempre que pertenezca al quehacer universitario.

Se adaptó la configuración de la interfaz de acuerdo a las necesidades de los usuarios, modificando scripts como el ubicado en ***/PREFIX/etc/openca/menus/***, el cual esta desarrollado en Perl.

- **Intercambio de Datos:** Puesto que es necesaria la transferencia de datos (peticiones de certificados, certificados aprobados, listas de revocación de certificados) entre las interfaces CA y RA; y debido a que se encuentran en servidores separados, se debía establecer la manera en que dichos datos lleguen seguros a su destino sin poner en riesgo la seguridad en el acceso al servidor de la CA, dada su criticidad.

La manera en que OpenCA lleva a cabo este intercambio se muestra en la figura 6. En ella se puede observar que las interfaces NODE (ubicadas en cada servidor) son las que extraen la información almacenada en las bases de datos de cada servidor; y posteriormente establecen la conexión entre ellas para iniciar el intercambio.

---

[11] **RSA: S**ign **A**lgorithm
[12] **DSA: D**igital **S**ign **A**lgorithm
[13] **ECDSA: E**liptic **C**urve **D**igital **S**ign **A**lgorithm
[14] **LOA: L**evel **O**f **A**ssurance

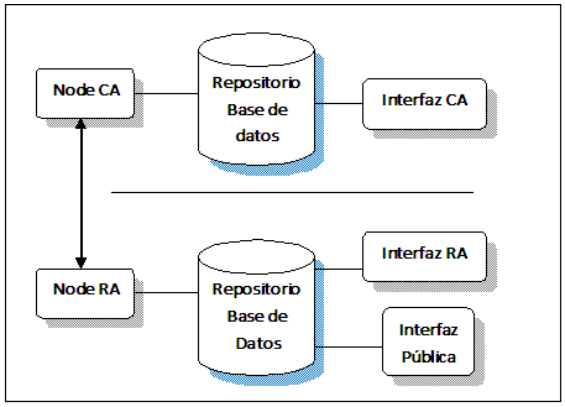


Figura 6. Intercambio de datos CA-RA

Luego de finalizada la trasferencia, la información es ubicada en su respectiva base de datos.

OpenCA dispone de algunas alternativas para efectuar tal tarea, como son: el uso de dispositivos de almacenamiento como disquetes, cd o memorias USB; y la utilización del protocolo SSH[15] para la transferencia de información entre los dos servidores.

Debido a la poca practicidad de la primera opción, se eligió la transferencia mediante la implementación de ssh, el cual permite el aseguramiento de la información intercambiada y la automatización de este proceso.

El sitio donde se efectuaron las configuraciones respectivas es en el directorio **etc/openca/servers/,** en el archivo **node.conf.template.**

También se tomaron otras medidas adicionales de seguridad, como la implementación de reglas de firewall y ACL's[16] para verificar que únicamente el servidor de RA tenga acceso al servidor de CA y viceversa.

Los anteriores fueron los aspectos más destacados en cuanto a la configuración de openca que se realizaron para cumplir los requerimientos de certificación de los usuarios de la UTPL. Luego de poner en funcionamiento la infraestructura, dichos usuarios, al acceder a la dirección **https://repo.utpl.edu.ec/pub**, entrarán en contacto con la Autoridad Certificadora CA-UTPL para realizar sus respectivas peticiones de certificación.

IV. Costos de la Implementación

La puesta en producción de la PKI en la Universidad Técnica Particular de Loja conlleva costos de hardware (adquisición de servidores, dispositivos token criptográficos para asegurar los certificados generados); de software en lo relacionado a administración, mantenimiento de los servidores por parte de sus administradores y capacitación y autoconocimiento de la herramienta utilizada (openca) para los mismos administradores y los usuarios en general que quieran acceder a dicha infraestructura.

Por ahora CA-UTPL se instalará como una Autoridad Certificadora autofirmada, con lo cual los certificados que emita tendrán validez dentro de la jurisdicción para la cual fueron diseñados, es decir, la comunidad de la UTPL. Pero en caso de que se requiera en lo posterior que la Autoridad Certificadora de la universidad se establezca como una autoridad reconocida a nivel nacional con potestad de brindar servicios de certificación a entidades ecuatorianas, deberá someterse a las disposiciones de las leyes de Ecuador, que, hasta la elaboración de este informe, establecían un costo aproximado de **$ USD 22000,00** para la Acreditación de una Entidad de Certificación de Información y Servicios Relacionados, previo a que se realice el registro respectivo.

El mismo hecho de ser una autoridad certificadora autofirmada ha llevado al analisis y posterior conclusión de que, para asegurar a los servidores considerados más críticos, es decir aquellos que manejen información vital para los intereses de la universidad, se deba recurrir a organizaciones reconocidas internacionalmente en el aseguramiento de la información y de mayor experiencia en el establecimiento de una PKI.

---

[15] **SSH: S**ecure **SH**ell, o intérprete de órdenes seguro, sirve para acceder a máquinas remotas a través de una red.

[16] **ACL: A**ccess **C**ontrol **L**ist.

Por tal motivo se han establecido contactos con Verisign, a través de su filial E-sign con sede en Santiago de Chile **[5]**, a fin de que nos proporcionen alternativas de solución a nuestras necesidades.

Con la colaboración de Verisign, se ha elaborado un informe que resume todos los aspectos analizados, parte de este informe se sintetiza en el cuadro mostrado en la figura 7.

Parametro	Número	Costo Unitario	Costo Total
Servidores	2 (para CA y RA respectivamente) Tipo BLADE	7000,00	14000,00
Tokens	30 (estimados inicialmente)	60,00	1800,00
Administradores	2 (gastos estimados por un año a Razón de $ USD 500,00)	6000,00	12000,00
Certificados Verisign MPKI SSL para servidores	30 (por un año, sin considerar renovación)	690,00	20700,00
TOTAL		48500,00	

Figura 7. Costo estimado de la implementación de PKI en la UTPL

V. Conclusiones

De la implementación de una PKI en la UTPL se ha llegado a las siguientes conclusiones:

- La implementación de una PKI dentro de la Universidad Técnica Particular de Loja, con el establecimiento de una Autoridad Certificadora y la emisión de certificados digitales que permitan a los usuarios funcionalidades como firma digital y cifrado de datos, constituye el inicio de una alternativa cuyos beneficios pueden incluir desde la simplificación de tareas administrativas (reducción en la cantidad de trámites en las matrículas, aprobación de solicitudes, presentación de informes), hasta la reducción de los gastos que estas mismas tareas generan en la actualidad (consumo de papel, impresora); a la vez que se contribuye con la conservación de los recursos naturales.

- Al ser PKI una plataforma compleja que involucra software, hardware y políticas de seguridad combinadas en el aseguramiento de la información de una organización, no todo debe estar basado en la herramienta OpenCA, sino que ésta debe constituir una parte de la infraestructura. Por tal motivo se ha elaborado una propuesta que incluye el apoyo de entidades más experimentadas en el campo de seguridad de datos (como es el caso de Verisign), a fin de abarcar no solo a usuarios, sino a los servidores que prestan funciones para la universidad. Asimismo se han establecido políticas de acceso a los equipos, requerimientos en cuanto a la capacidad de los mismos para una mayor agilidad en los procesos y soporte para escalabilidad de la infraestructura.

- El establecimiento de CA-UTPL como Autoridad de certificación avalada a nivel nacional mediante el cumplimiento de las disposiciones dictaminadas por el Conatel, permitirá que en poco tiempo CA-UTPL se convierta en proveedora de servicios de certificación, ya sea a entidades públicas como privadas a nivel local y nacional.

- La implementación de la PKI en la UTPL emplea un modelo de confianza jerárquico, lo que implica el establecimiento de una Autoridad Certificadora raíz (CA) con sus funciones de intercambio y de generación de certificados; y bajo la cual existe una Autoridad de Registro (RA) subordinada, encargada de la aprobación de las peticiones de certificación y de la interacción con los usuarios. Tanto CA como RA se encuentran en servidores separados.

- El empleo del protocolo ssh en el intercambio de información entre los servidores CA y RA establece una conexión cifrada y automatizada, garantizando la integridad de los datos transportados, una ventaja considerable sobre otros medios de intercambio de información como disquetes, cd roms o memorias flash.

- El campo de acción inicial de PKI está enfocado a miembros de la comunidad universitaria pertenecientes a modalidad presencial, debido a que es más fácil para el administrador de la RA verificar físicamente la identidad de un solicitante de certificado, así como su relación actual con la universidad. Queda entonces latente la posibilidad de ampliar el rango de aplicabilidad de la infraestructura mediante la integración con el Sistema de Gestión Académico, a fin de involucrar a todos los miembros de la comunidad universitaria.

VI. Referencias

[1] QUISHPE, M. y SANCHEZ, M. (2008): "Implementación de una Infraestructura de Clave Pública (PKI) para la Universidad Técnica Particular de Loja". Loja, UTPL. Escuela de Ciencias de la Computación.

[2] NASH, A., DUANE, W., JOSEPH, C., y BRINK, D. (2002): PKI La mejor tecnología para implementar y administrar la seguridad electrónica de su negocio. Colombia: Ed. McGraw-Hill.

[3] DIAZ, F., AMBROSI, V., LUENGO, M., MACIA, N., MOLINARI, L. y VENOSA, P. (2006): Adaptando OpenCA para implementar una PKI para e-ScienceCongreso Argentino en Ciencias de la Computación -CACiC 2006. Formato de archivo: PDF/Adobe Acrobat. Disponible en: www.linti.unlp.edu.ar/.../adaptando_openca_para_implementar_una_pki_para_e_science.pdf.

[4] OpenCA Guide for Versions 0.9.2+. Formato de archivo: PDF/Adobe Acrobat. http://www.openca.org/projects/openca/

[5] www.e-sign.cl