IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) EN UNA RED DE PRUEBAS

Msc. Espinoza María Paula, Sánchez Ochoa Maritza Ximena,
Quizhpe Vacacela Martha Paulina

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Resumen— Hoy en día la conectividad es fundamental para muchas actividades, y es real a partir de la existencia de Internet, sin embargo, la problemática nace, de la necesidad de determinar cómo conducir las transacciones de misión crítica, ya sea sobre Internet o sobre las Intranet o Extranet de manera segura. El mecanismo adoptado por la Universidad Técnica Particular de Loja para suplir ésta necesidad, hoy por hoy, es el uso de Secure Socket Layer[1] (SSL) en las aplicaciones de Internet y el uso de redes privadas virtuales para la Intranet. Sin embargo, las necesidades son cada vez más exigentes, optando sin duda por el uso de algún mecanismo de seguridad más avanzado, como es una Infraestructura de Clave Pública - PKI.

Una PKI está considerada en la actualidad como el mecanismo de seguridad más completo, por lo cual éste artículo resume el resultado de un proyecto de tesis de ingeniería que tiene como objetivo realizar un estudio genera de PKI y su implementación en un entorno de prueba como plan piloto dentro de la Universidad que sea la base para el desarrollo de nuevos proyectos desarrollados mediante ésta tecnología.

I. INTRODUCCIÓN

Bajo las siglas PKI se engloba a una tecnología estándar, impulsada por la ISO, ITU, y el IETF, que pretende llevar a la práctica los conceptos teóricos de la Criptografía de Clave Pública.

La Criptografía de Clave Pública permite, entre otras cosas, implementar sistemas de firma digital y el cifrado de datos sin necesidad de compartición de secretos.

La firma digital garantiza la Integridad y el cifrado garantiza la Confidencialidad, pero indirectamente la criptografía de clave pública también permite garantizar la Autenticidad del receptor del mensaje cifrado o del emisor del mensaje firmado. Esto se consigue con el uso de *certificados digitales*, donde se asigna una identidad a una clave pública.

La utilización de claves (públicas y privadas) y certificados digitales para: firmar y cifrar correos electrónicos, autenticarse ante sitios Web, validar transacciones, solamente tienen éxito cuando existe transparencia entre las aplicaciones y los mecanismos que PKI utiliza para garantizar la seguridad [1].

II. INFRAESTRUCTURA DE CLAVE PÚBLICA

¿Utilizar una PKI es seguro? ¿Cómo funciona una PKI?

De un modo sencillo, una PKI, es el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales que pueden ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de la red de una empresa, Extranet o Internet.

La meta de una PKI, es asegurar que los datos sensibles sean protegidos mediante técnicas de encriptación[2].

Cada dispositivo de usuario final posee un software de encriptación y un par de claves: pública para distribuirla a otros usuarios y, otra privada, guardada y protegida por su

[1] Secure Socket Layer,

[2] ***Técnicas de encriptación***: son técnicas matemáticas avanzadas utilizadas en los procesos de ocultación y cifrado de la información. Los algoritmos más utilizados RSA, DSA, RC4, AES.

propietario. Por ejemplo, si un usuario quiere enviar un correo electrónico a otro usuario, el usuario emisor cifra el mensaje utilizando la clave pública del receptor; cuando el mensaje se recibe, el receptor lo descifra con su clave privada. Se pueden tener múltiples pares de claves para mantener comunicaciones distintas con grupos diferentes. Por tal motivo, dado el elevado número de claves que intervienen en las comunicaciones, resulta crucial contar con algún método para administrarlas y controlar su utilización. Aquí es donde una PKI entra en juego, permitiendo la creación, distribución, seguimiento y revocación centralizada de claves, siendo este el método de seguridad más completo que existe hoy en día.

A. Componentes PKI.

En la Figura 1, se presenta un diagrama de las interacciones de cada uno de los principales componentes que intervienen dentro de una PKI, según lo propuesto en el Grupo de Trabajo de PKI, denominado PKIX.

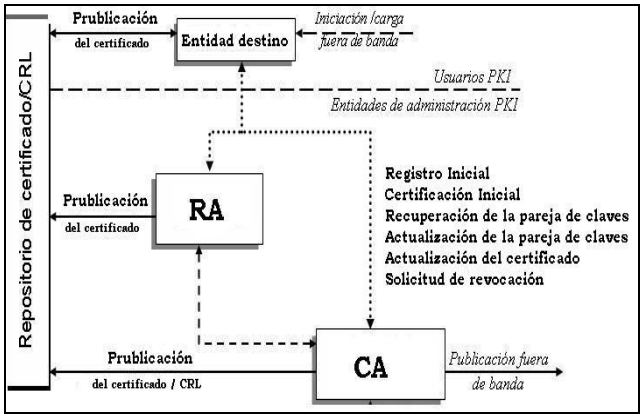


Figura. 1
Interacción de los Componentes PKI según PKIX

- **Entidad destino**

Usuario del certificado expedido por la autoridad de certificación.

- **Autoridad de certificación (CA)**

Es responsable de crear y expedir certificados de la entidad destino, asociando la identidad de la entidad destino del sujeto. Además la CA es responsable de administrar todos los aspectos del ciclo de vida del certificado después de su expedición.
En términos PKIX [2] existe una "CA raíz" la misma que recibe directamente la confianza de un certificado digital.

- **Autoridad de Registro (RA)**

Entidad encargada de verificar los datos de las personas que solicitan el certificado para posteriormente aprobarlos y exportarlos a la CA para que sea firmado y emitido al usuario correspondiente, a demás, la RA se encarga de todos los procesos administrativos relacionados con los certificados

- **Repositorios de certificados**

Se lo utiliza para el almacenamiento público de certificados y lista de certificados revocados.

B. Certificado Digital

Un certificado digital incluye la clave pública, información acerca de la identidad del usuario, la clave privada, período de validez del certificado, y la firma digital de la CA.

La PKI trabaja exclusivamente con certificados digitales, misma que es responsable de emitir los certificados, asegurar la distribución de estos certificados a través de un directorio y validar los certificados.

El modelo de certificados digitales sigue la norma ISO X.509v3 adaptada a su uso por Internet por el grupo de trabajo PKIX del IETF en el RFC2459. También se han creado estándares para el cifrado y la firma de correo electrónico (S/MIME), para el cifrado de las comunicaciones (SSL), y en general para el formato de los datos firmados o cifrados (PKCS#7 o CMS).

- **Ciclo de vida de los certificados**

En la Figura 2, muestra el proceso por el cuál se valida el tiempo de duración de un certificado digital, por causa de caducidad, extravío, renovación del certificado y par de claves.

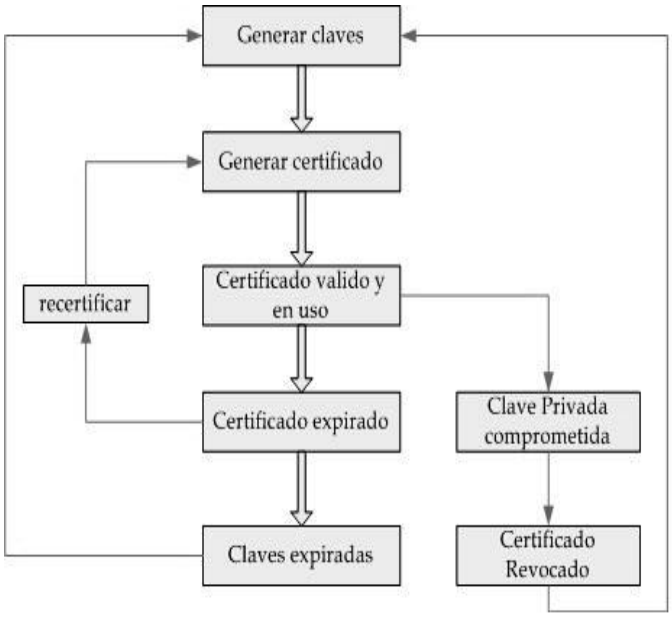


Figura 2
Ciclo de vida de los certificados

En la Tabla 1, muestra la descripción de los estados que un certificado puede alcanzar.

Tabla 1
Descripción de los diferentes estados de un certificado

Caducado	Cuando se ha superado la fecha de vigencia del certificado. El tiempo de validez que se da a los certificados digitales tanto para usuario, como para la CA, depende de lo estipulado en las políticas y procedimientos para la PKI.
Revocado	Cuando ha sido rechazado, bien por la CA que lo emite o por el propio usuario. El motivo de la revocación depende de lo estipulado en las políticas y procedimientos.
Suspendido	Cuando se ve afectado por una investigación, por lo que se procede a cancelar la validez del certificado digital durante un cierto período de tiempo, pudiendo volverse a levantar la suspensión dentro del período de validez del certificado.
Válido	Cuando no pertenece a ninguno de los estados anteriores, es decir, es un certificado digital que está válido o en uso.

III. MODELO Y ARQUITECTURA PKI

En una tesis desarrollada anteriormente [6], previa a la obtención de título de Ingeniero en Informática, se propone un modelo previo a sus respectivas observaciones.

A. Modelo Planteado

En la Figura 3, se muestra el modelo y la descripción obtenida de la tesis antes mencionada.

Descripción del modelo

- La Autoridad Certificadora denominada CA-UTPL, va a almacenar toda la información sensible como son las **claves privadas de los**

certificados emitidos a los usuarios, en un servidor que no va a estar disponible para los usuarios del sistema PKI.

- Los usuarios del sistema PKI solamente tendrán acceso al servidor CRL, y todos los certificados válidos, revocados o caducos y además al certificado de la CA. La única que tendrá acceso al servidor de la CA, es la RA, quien brinda la comunicación entre la CA y los usuarios.

- Si un estudiante, personal administrativo o un docente, realiza la petición de un Certificado Digital, es atendido por la Autoridad de Registro RA, quien es responsable del registro y la autenticación de los usuarios a quienes se les expide un certificado después de que les ha sido aprobado la solicitud presentada y una vez validada toda la información.

- Una persona puede encargarse de las responsabilidades de una RA. Todo el proceso de validación de la identidad se puede desarrollar como un conjunto de procedimientos manuales.

- La CA entregará el certificado digital al usuario que lo solicite, a través de la RA, otorgando los privilegios que requiera dicho usuario.

- En el repositorio, se almacenan los certificados y las claves públicas correspondientes, que se necesiten para que puedan entrar en funcionamiento. Estos repositorios generalmente son directorios tipo LDAP.

- Los usuarios necesitan validar los certificados que reciben.

- La clave privada (PKI) de un usuario puede ser almacenada en un Smart Card donde internamente todas las funciones criptográficas se realizan, incluyendo firma digital, y descripción de las claves de sesión.

- Otra opción para almacenar la clave privada pudieran ser los *Smart Tokens* Estos, usan una tecnología idéntica a las Smart Cards, con la diferencia de su forma y su interfaz.

- La información podrá ser almacenada de una manera estructurada en bases de datos centralizadas, para posteriormente ser migradas a bases de datos especializadas conforme los volúmenes de información que se generen y las definiciones de seguridad de la información que se establezcan.

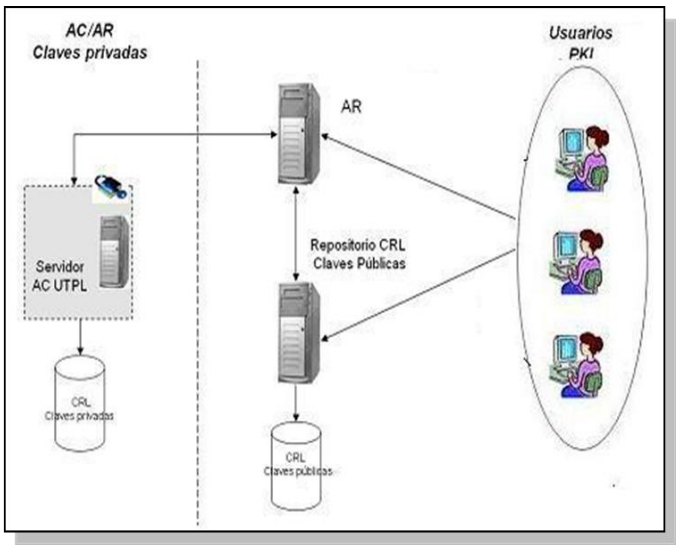


Figura 3
Modelo PKI propuesto

B. Evaluación del modelo planteado

Para realizar la evaluación se toma en cuenta los siguientes criterios, de acuerdo a la información adquirida en documento de estudio de maestría [3]:

- Arquitectura
- Manejo de certificados y claves
- Escalabilidad

Para más información acerca de criterios de evaluación, ver Anexo 1.

Dado que no existe un plan de pruebas del modelo planteado, no se pueden tomar datos numéricos para su evaluación, sin embargo, se lo realiza de forma descriptiva.

- **Arquitectura**

  La validación de certificados y el establecimiento de confianza entre dos partes que necesitan comunicarse son los puntos más importantes en la creación de una PKI, es decir, la interoperabilidad. En el modelo planteado, se utiliza únicamente una CA raíz que se encarga de firmar a sus usuarios, siendo ella, su única tercera parte de confianza. Por tal motivo, la arquitectura define un modelo básico interoperable. Sin embargo, la CA no guarda las claves privadas de los certificados emitidos, las tareas fundamentales de una autoridad certificadora son: emitir certificados y resguardar su clave privada. Además, los usuarios no tienen relación alguna con el servidor de la RA UTPL sino con el servidor público de certificados, y con la persona encargada de la Autoridad de Registro, que se lo denomina Operador de la RA.

- **Manejo de certificados y claves**

  El modelo lo describe utilizando, para el almacenamiento de claves, los dispositivos criptográficos y para la administración de certificados, mediante los repositorios de certificados, utilizando el LDAP, entre otros existentes. Estos mecanismos de administración de claves y certificados hace que el modelo sea seguro en cuanto a las claves privadas y fácil la administración en cuanto a los certificados, porque los usuarios pueden validar fácilmente en el repositorio de certificados, el estado de un certificado. La CA se encarga de resguardar su clave privada, pero el modelo expone que, a demás, resguarda las claves privadas de todos los usuarios, siendo ésta responsabilidad única del usuario del certificado.

- **Escalabilidad:**

  La escalabilidad debe ser estudiada teniendo en cuenta varios criterios, los cuales deben evaluarse en conjunto y no separadamente, como ser, flexibilidad, el TCO (Total cost of ownership, el costo total por puesto), facilidad de uso, desempeño, etc. Sin embargo, estos criterios no pueden ser tenidos en cuenta siempre, porque los escenarios son diferentes. [3]

  El modelo planteado es ajustable a las necesidades futuras, por el hecho de ser un modelo básico PKIX, sin embargo, el costo de inversión depende del cambio al cuál será expuesto, existen distintas alternativas mediante las cuales la universidad puede crear relación de intercambio confiables, cuya complejidad es directamente proporcional a la cantidad de la CA's a relacionar. Si la necesidad es, intercambiar datos entre CA's distintas, se debería emitir certificados cruzados entre CA's, o, si la necesidad es, crear una nueva CA, el modelo a acoplar será jerárquico, creando adicionalmente una CA raíz la cual firmará a las sub-CA's.

C. Modelo a Implementar

- El modelo anteriormente evaluado se acopla en gran medida a las necesidades iniciales de implementación de una PKI, el cual se lo ha tomado como referencias para implementarlo pero realizando algunas modificaciones. El modelo a implementar se presenta en la Figura 4.

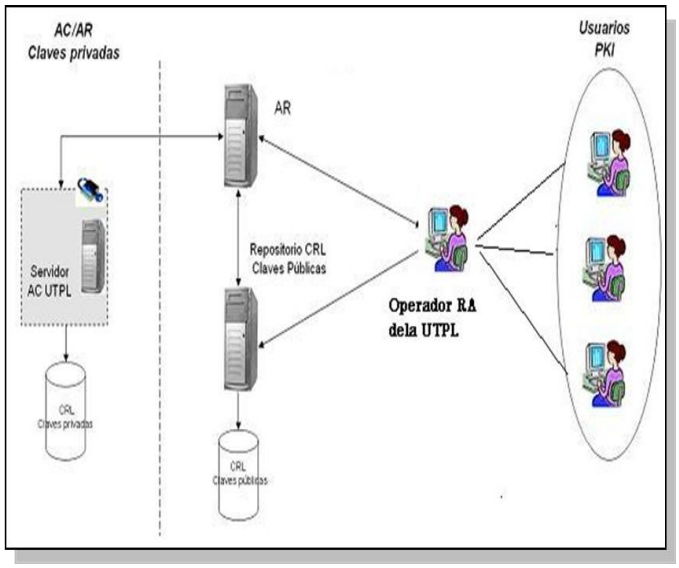


Figura 4
Modelo PKI seleccionado para la UTPL

Al modelo planteado se ha agregado un operador RA, quien será el encargado de receptar y validar todas las peticiones de certificados, ya que los usuarios no tienen relación alguna con el servidor de la RA.

Es necesario además definir hacia qué usuario van dirigidos los servicios de PKI. Para la Universidad inicialmente se consideraría a los servidores y administradores. En una primera fase docentes y estudiantes no estarían considerados.

V. ANÁLISIS DE HERRAMIENTAS SOFTWARE Y HARDWARE

A. Selección de Alternativas Software

Para la selección de las diferentes alternativas software se evaluaron dos soluciones: Software Libre u Open Source y el Software Propietario, validando cada una de ellas y eligiendo como la mejor opción el software Libre/OpenSource dentro del cual se eligió trabajar con la herramienta OpenCA[3], por las siguientes razones:

- Hoy en día, las universidades se encuentran promoviendo e impulsando proyectos de Software Libre u Open Source.

- Por ser una de las alternativas que permite trabajar en comunidad, y tener a disposición todo el código fuente.

- OpenCA es una de las herramientas PKI disponibles en el medio, ofreciendo ventajas significativas para los requerimientos estipulados en este proyecto, uno de ellos es sin duda, el costo, ya que, el gasto como cualquier software Open Source, es poco significativo en la adquisición del software como tal, sin embargo, no hay que despreciar el costo que involucra la administración y capacitación requeridas. Más adelante se estipula los costos y beneficios que implica esta implementación.

Tabla 2
Descripción de requerimientos Software para la Implementación de una PKI en una red de pruebas.

Aplicaciones	Software
Sistema Operativo	Linux Debian Sarge 3.1
DNS	Bind 9.2.4-1
Base de Datos	MySQL
Servidor Web	Apache 1.3.33-6.deb Openssl 0.9.7e.deb
PKI	OpenCA 0.9.3-rc1
PKI	Openca-tools-1.0.0
Módulos Perl	Perl 5.8.4-8

B. Selección de Alternativas Hardware

Luego de realizar un estudio del software se procede a evaluar las opciones de hardware, las

[3] OpenCA, www.openca.org

mismas que dependen del modelo y arquitectura PKI definidas anteriormente.

Tomando como referencias a las experiencias adquiridas a nivel mundial acerca de este tema [4], se ha clasificado los diferentes componentes hardware por niveles, definiendo los requerimientos mínimos para la implementación de la PKI, el cual se describe en el Anexo 2.

En la Tabla 3, se muestra los requerimientos hardware mínimos recomendados:

Tabla 3
Descripción de los requerimientos Hardware para la Implementación de una PKI.

	Memoria	Procesador
CA	1 GB	3.4 GHz
RA	2048 MB	3.4 GHz
Servidor de Copias de Seguridad	2048 MB	3.4 GHz
PC aislado	1 GB	3 GHz

C. Costo y Beneficios

Los aspectos más destacados en cuanto a costos se muestran en Anexo 3:

En la Tabla 4, se describen los costos mínimos requeridos para la implementación de una PKI en la UTPL.

Tabla 4
Costos mínimos de inversión en una PKI
.

	Tiempo de trabajo (meses)	Horas diarias	costo (hora)	Número de personas	Costo Total
Costos estratégicos	4	4	3,75	1	600
Desarrollo e implementación	6	8	3,75	2	2400
Capacitación	5 dias	4	10	1	200
La inversión en el establecimiento y operación	12	8	3,75	1	7200
Total					**10400**

Tabla 5
Costos mínimos de inversión en una PKI

	Costo Dispositivo	Unidades	Costo Total
Requerimientos Hardware	5500	2	11000
Requerimientos Software			0
Total			**11000**

Tabla 6
Costos mínimos de inversión en una PKI

Costo total de inversión	**21400**

VI. DESARROLLO E IMPLEMENTACIÓN

Para el proceso de implementación de un plan piloto de PK, se requiere montar la red de pruebas, requiriendo como recursos hardware, dos computadores, que actuarán como servidores, tanto de CA y RA. La RA tiene acceso al Internet, mientras que la CA se encuentra conectada a la RA sin acceso a la red pública.

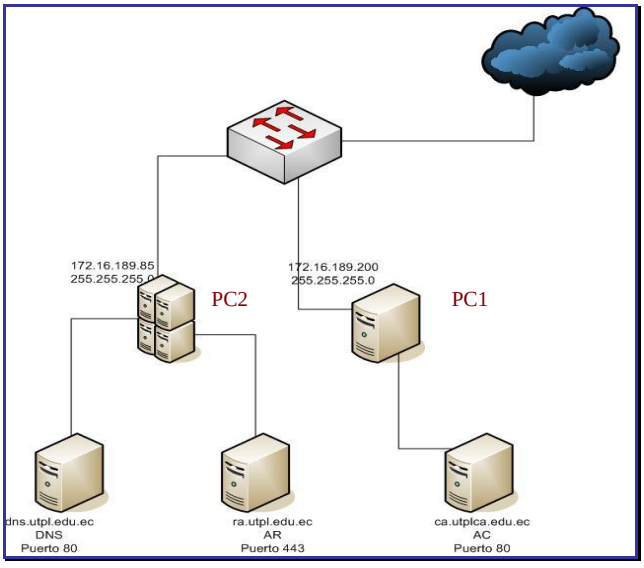


Figura 5
Topología de la red PKI

La topología de la red de prueba, opera con dos computadores conectados al Switch, donde cada computador simulará las funciones de una PKI. Estos dos PC se integran y forman la implementación total de la PKI, distinguidas por diferentes dominios, como se muestra en la Figura 7. Sin embargo, para un entorno en producción deberá evaluarse el esquema de seguridad de la red y ubicar los servidores en las distintas DMZ´s dependiendo del nivel de seguridad requerido, que para el caso de la CA debe ser la red más segura.

Tabla 7
Dominios para la red de pruebas PKI

utplonline.edu.ec	Para la Autoridad Certificadora CA y el Servidor de Nodo, donde tendrán acceso solo el personal autorizado de la PKI, por razones de seguridad.
utpl.edu.ec	Bajo este dominio estarán tres módulos muy importantes la Autoridad de Registro AR, el Administrador del Nodo y el módulo del servidor público de certificados PKI, destinado a los usuarios.

OpenCA, software utilizado en este proyecto, está diseñado para ser una infraestructura distribuida, puede construir toda una jerarquía de tres o más niveles. La idea básica de cada X.509 PKI es una fuerte organización jerárquica. Esto se traduce en un árbol de las bases de datos si se trata de crear una arquitectura distribuida PKI. [5].

Al haber instalado la red física de pruebas, se define el esquema lógico.

El intercambio de los datos entre las bases de datos de las jerarquías describen una red lógica, pues estos pueden ser aislados de manera automática si se utiliza un sistema de base de datos distribuido en el sentido de OpenCA, tal sistema de base de datos distribuido se identifica como una base de datos en el árbol. Si realmente se tiene una base de datos aislada (por ejemplo: nodo offline y nodo online), entonces se tiene la tecnología para el intercambio de datos y la gestión completa del nodo en la jerarquía. Esta gestión de la funcionalidad que se incluye en una interfaz llamada nodo o también denominada, nodo de gestión.

Por lo tanto, para la implementación en la red de pruebas, se utiliza bases de datos aisladas, de acuerdo al diseño que propone OpenCA, mismo que se describe a continuación en la Figura 6.

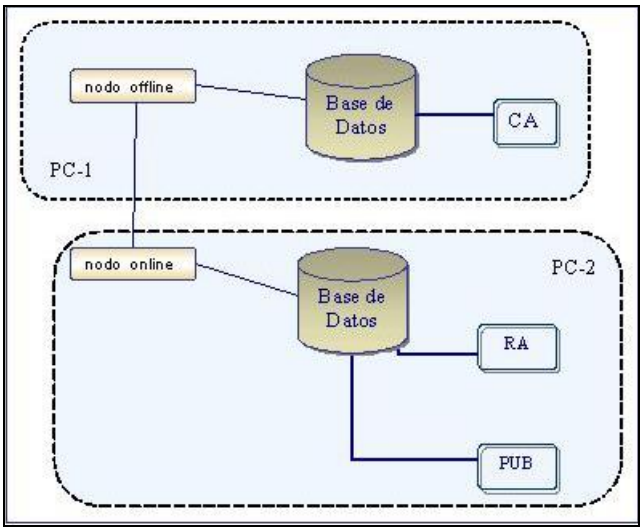


Figura 6
Diseño Lógico para la red de pruebas

La descripción para cada uno de los PC's se muestra a continuación:

a) PC1:

- *Servidor de CA*: Este servidor debe estar físicamente en un lugar seguro y apropiado, el servidor no debe tener acceso a la red de Internet, de tal forma que se garantice la seguridad de su clave privada, de lo contrario la PKI y todos los certificados vinculados con esta clave privada no tendría razón de ser.

- *Base de Datos de CA* (local de cada máquina - localhost): Se almacenan información de la PKI como certificados, peticiones, etc.

b) PC2:

- *Servidor de RA*: tiene como función principal verificar la identidad del usurario que está realizando la petición, validado los datos del usuario se envía la petición aprobada por la Autoridad de Registro RA a la Autoridad Certificadora CA, para que sea esta la que firme y emita el certificado. El intercambio de datos entre las dos partes CA y RA se la denomina operaciones de exportación e importación, su explicación se la dará mas adelante.

- *Base de Datos de RA* (local de cada máquina - localhost): Se almacenan los mismos registros que la base de datos del PC-1.

- *Servidor Público de la PKI*, destinado a los usuarios, para acceder y realizar las solicitudes de certificado y las solicitudes de revocación de certificado, descargar el certificado de la CA y tener acceso a los CRLs.

A. Requerimientos Preliminares

Apache

- Implementación de canal de seguridad, mediante la utilización del protocolo SSL tanto para la CA como para la RA.

Base de datos MySQL

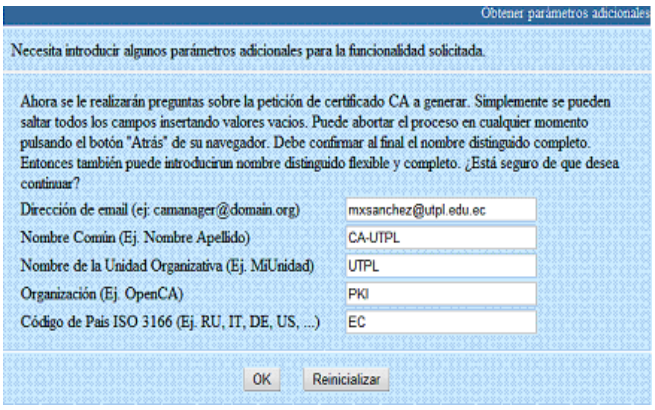
- Creación de base de datos para PC-1 y PC-2, donde se almacena todos los registros donde reposará la información de certificados, peticiones, listas de revocación de certificados.

B. Implementación de los componentes de la PKI

a. CA

Después de la instalación de OpenCA, se procede a generar la clave privada y el certificado para la CA, firmada por sí misma como tercera persona confiable, considerando las políticas y procedimientos establecidos.

Figura 7
Petición de certificado CA raíz



En la Fig. 6 se muestra la solicitud de certificado para la Autoridad Certificadora de la UTPL, llamada CA.

Las características de la CA, son:

- El algoritmo para el cifrado de la clave es el 3DES, con un mínimo de 10 caracteres.

- La longitud de la clave es de 2048 bits.

- El algoritmo utilizado para la generación de las claves, es RSA.

- El tiempo de validez para el certificado de la CA es de dos años, por ser una CA de pruebas.

El Certificado de la CA se instala en todos los navegadores de usuarios antes de solicitar un certificado.

b. **RA**

Encargada de la modificación, aprobación y eliminación de las peticiones de certificado realizadas por los usuarios. La RA, es la única entidad encargada de la validación de los datos recibidos por los usuarios que conforman la comunidad universitaria.

RA debe:

- Instalar en el navegador del Operador de la RA (Administrador de la RA) el certificado de la CA para iniciar y realizar las operaciones.
- Instalar el certificado del Operador RA emitido por la CA, para poder validar y firmar las peticiones.

RA es encargada de:

- Modificar la petición determinando el tiempo de vida y la fecha y hora de emisión y expiración que tendrá el certificado
- Aprobar la petición.
- Eliminar la petición.

c. **Interfaz Pública de los usuarios.**

El usuario debe:

- Descargar el certificado de la CA en su navegador Web.

El usuario puede:

- Realizar una petición de certificado (de acuerdo al navegador Web que esté utilizando).
- Realizar una petición de revocación de certificado.

El navegador Web y cliente de correo recomendados en este artículo, son: Mozilla Firefox 2.0 y Thunderbird, respectivamente.

VII. CONCLUSIONES

- El despliegue de una PKI y la utilización de certificados digitales, posee, desde el punto de vista administrativo, un beneficio a largo plazo, dado al elevado nivel de seguridad que otorga, justificando de esta forma la inversión.
- Liderar un proyecto de implementación de aplicaciones basadas en PKI, es una tarea laboriosa y de sumo cuidado, por cuanto se deben considerar los costos que implica en cuanto a la capacitación para la adopción de este nuevo estilo de trabajo, no solo por los cambios tecnológicos sino por los cambios culturales.
- La importancia de asegurar la clave privada de la CA, es por el hecho de que se vea expuesta a terceras personas mal intencionadas, resultando un problema de gran magnitud y pérdidas monetarias, ya que se verían involucrados todos los certificados emitidos por esta entidad pudiendo quedar vulnerables, perdiendo la confiabilidad adquirida por la organización.
- Para la implementación de la RA y CA se debe evaluar el esquema de seguridad de la red a fin de ubicarlas en un lugar estratégico que la aísle totalmente del acceso de personas no autorizadas conectadas a la red de Internet.
- En las pruebas realizadas a los usuarios finales, el 80% manifestó su complejidad al obtener un certificado digital, al instalarlo y al revocarlo, mientras que un 20% no tuvo inconvenientes, concluyendo de esta forma que el uso de ésta nueva tecnología requiere una capacitación previa en su utilización y el manejo de una interfaz con campos bien definidos.

- El proyecto piloto PKI en la red de pruebas, es la primera experiencia real de implementación PKI en la Universidad, quedando como una base para que en el futuro se lo mejore e implemente en producción.

VIII. GLOSARIO DE TÉRMINOS

PKI	Infraestructura de Clave Pública
ISO	Organización Internacional para la Estandarización.
ITU	Unión Internacional de telecomunicaciones.
IETF	Grupo de Tareas de Ingeniería de Internet.
CA	Autoridad Certificadora
RA	Autoridad de Registro

IX. REFERENCIAS

[1] **NASH Andrew, DUANE William, JOSEPH Celia, BRINK Derek.**
"Infraestructura de Claves Públicas PKI.". La mejor tecnología para implementar y administrar la seguridad electrónica de su negocio. Colombia: Editorial, impresos ejemplares 2002. 512pg.

[2] **Grupo de trabajos de Ingeniería de Internet IETF**
[Disponible en Internet]
http://www.ietf.org/html.charters/pkix-charter.html

[3] **Di Girolamo, Claudio** Titulo "Implementación y uso de PKI, Masterado en ciencias de la computación.
[Disponible en Internet]
http://www.itba.edu.ar/capis/rtis/articulosdeloscuadernosetapaprevia/digirolamo10.pdf

[4] **CATCERT, Agencia Catalana de Certificación**, creado el 17/07/2007
[Disponible en Internet]
http://www.catcert.net/descarrega_cas/Plec_tecnic_maquinari_CPD.pdf.

[5] **OpenCA**
[Disponible en Internet]
http://www.openca.org

[6] Caicedo, Maria Augusta, Tesis titulada "*La Infraestructura de Clave Pública y el diseño de un modelo para su implementación en la UTPL*", Previo a título de Ingeniero en Sistemas, 2008.

X. ANEXOS.

Anexo 1. Criterios de Evaluación

Arquitectura	Diseño de certificación entre las diferentes autoridades certificadoras que conforman la infraestructura basándose en los diferentes tipos existentes, como son: básico PKIX, jerárquica, malla y cruzadas.
Manejo de certificados y claves	Se refiere a la administración del par de claves y sus certificados.
Escalabilidad	Acoplamiento del modelo a las nuevas necesidades futuras de la universidad.

Anexo 2. Descripción de niveles para seleccionar los requerimientos hardware.

Niveles	Descripción
Nivel 1 Capa PKI	Esta capa procesará gran número de peticiones, puesto que es la interfaz con los clientes. En esta capa se requieren como mínimo 2 Servidores, el servidor 1 alojará la CA, mientras que el servidor 2 alojará a la RA y al Servidor público de certificados de la PKI, donde tendrán acceso todos los usuarios.
Nivel 2	

Capa de Base de Datos	Existe una base de datos por cada módulo, por lo tanto las Bases de Dato se alojará en los mismos servidores de CA y la RA. En el caso que sea necesario será conveniente utilizar servidores de alta disponibilidad, para el servidor de base de datos
Nivel 3 Sistemas de copias de seguridad	Se requiere de un servidor de copias de seguridad que permitan hacer Backups de los servidores tanto, CA, RA y la parte pública de la PKI.
Nivel 4 Seguridad de la PKI	Para esta capa, el equipo humano de PKI debe proveer las características que crea necesarios para garantizar la seguridad de la PKI, como lo es el Firewall, en que subred se encuentran.
Equipo Informático	El equipo informático corresponde a un PC estándar para la administración remota de todos los dispositivos de la plataforma. Este PC deberá estar aislado del exterior.

Anexo 3. Tipo de Costos

Tipo Costo	Descripción
Costos estratégicos	Aquellos costos que implica el tiempo invertido en el planeamiento de todo lo que tenga que ver con el diseño e implementación de una Infraestructura de Clave Pública.
Implementación	Incluye el costo del personal del área de Sistemas que asegura la compatibilidad de las aplicaciones internas con los sistemas.
Desarrollo	Adquisición de programas, desarrollo y programación de las interfaces de aplicación, mejoramiento del software de aplicación interno para aprovechar todas las ventajas de una PKI y las pruebas necesarias para la óptima implementación de la nueva Tecnología.
Requerimientos de software y Hardware	En cuanto a los requerimientos software se evalúa el tipo de software que puede ser propietario o software libre u Open Source y en cuanto al hardware se evalúa de acuerdo a los requerimientos de la universidad.
Capacitación	Este aspecto incluye tanto el entrenamiento del personal interno para definir y asumir nuevas responsabilidades en un ambiente de seguridad, como así también la educación de los usuarios externos que eventualmente queden implicados en una aplicación de ésta tecnología.
La inversión en el establecimiento y operación efectiva de la PKI	Depósitos de claves públicas y todos los servicios necesarios para el funcionamiento de estos procesos.

XI. Hoja de Vida de los Autores

Maritza Ximena Sánchez Ochoa (Tesista), nacida en Zamora-Ecuador, el 07 de Enero de 1982. En el año 1999 obtuvo el Título en Bachiller en Ciencias de la Educación especialidad Computación en el Instituto Tecnológico "12 de Febrero" de la ciudad de Zamora provincia Zamora Chinchipe. En Agosto del 2006 egresó de la carrera de Ingeniería en Sistemas Informáticos y Computación en la Universidad Técnica Particular de Loja. Entre Mayo del 2007 a Marzo del 2008 culminó los cuatro módulos CCNA de la Academia CISCO. Actualmente, ha culminado con el desarrollo de la tesis "Implementación de una Infraestructura de Clave Pública PKI en una red de pruebas para la UTPL" faltando la aprobación y su respectiva disertación. Correo electrónico mxsanchez@utpl.edu.ec

Martha Paulina Quizhpe Vacacela (Tesista), nacida en el año de 1983 Azuay-Cuenca, Título de Bachiller especialidad "Físico Matemático" en el año 2000 en el "Instituto Técnico Superior Saraguro". Cursó la academia Linux en el periodo Octubre 2003- Junio 2004. Egresada de la Universidad Técnica Particular de Loja en la carrera de "Ingeniería en Sistemas Informáticos y Computación" en Agosto 2006. Actualmente, ha culminado con el desarrollo de la tesis "Implementación de una Infraestructura de Clave Pública PKI en una red de pruebas para la UTPL" faltando la aprobación y su respectiva disertación. Correo electrónico: mpquizhpe@utpl.edu.ec

María Paula Espinosa Vélez (Directora Tesis), nacida en el año de 1979 Loja - Ecuador, Título de Bachiller especialidad "Físico Matemático" en el año 1996 en el "Colegio Santa Mariana de Jesús". Ingeniera en Sistemas Informáticos y Computación, Universidad Técnica Particular de Loja, año 2003. Master en Gestión de Telecomunicacines en la Empresa, Universidad Politécnica de Madrid, año 2006. Actualmente trabaja en el Grupo de Telecomunicaciones de la Unidad de Proyectos y Sistemas Informáticos de la UTPL, en la línea de Seguridad de la Información. Correo electrónico: mpespinoza@utpl.edu.ec