# Diseño y simulación de una Infraestructura de Clave Pública basada en el estándar de certificados digitales X.509 a través de software libre para utilizarlos en la seguridad del correo electrónico en la red de datos interna del Cuerpo de Ingenieros del Ejército en la matriz Quito

Carlos A. Vásquez, David R. Valencia

***Resumen*—Este documento contiene información relacionada con el diseño de una Infraestructura de Clave Pública que emita y gestione certificados digitales X.509, para utilizarlos en la seguridad de la información transferida por el correo electrónico institucional, en el entorno de la red de datos interna del Cuerpo de Ingenieros del Ejército de Quito.**

**Esta solución, desarrollada en su totalidad bajo herramientas de software libre, provee un sistema de seguridad que complementa el nivel de protección garantizado por los actuales sistemas implementados en esta entidad. Es así que, se dispondrá de uno de los mecanismos de seguridad más fiables en la actualidad, cuya aplicación está enfocada en la protección del correo institucional, pero posteriormente es posible emplearlo para securizar información generada o manipulada por diversas aplicaciones y servicios de red, tratando de implantar la seguridad en profundidad basada en niveles de defensa.**

***Términos Indexados*—*Infraestructura de Clave Pública; certificado digital; autoridad certificadora; autoridad de registro; lista de revocación de certificados; clave públca; clave privada; cifrado; agente de trandferencia de correo; agente de entrega de correo; agente de correo de usuario.***

## I. INTRODUCCIÓN

El progresivo desarrollo tecnológico experimentado en el campo de las tecnologías de la información, ha generado diversas tendencias de comunicación telemática que han mejorado notablemente las condiciones de vida de las personas. Sin embargo, de manera simultánea a este suceso, también han evolucionado técnicas delictivas ejecutadas remotamente empleando redes de comunicación de por medio, que intentan robar o manipular información y producir daños o pérdidas de cualquier tipo.

Documento recibido el 11 de diciembre de 2014. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.

C.A. Vásquez, trabaja en la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador.

D.R. Valencia, egresado de la Carrera de Ingeniería Electrónica y Redes de Comunicación.

Por ello, para aprovechar favorablemente este aporte, es necesario determinar que la identidad de las personas que intervienen en una comunicación telemática sea genuina, o que la información en trayecto sea manipulada únicamente por destinatarios legítimos; más aún considerando que desde tiempos remotos ha existido la necesidad de proteger la información, hoy en día esto es trascendental.

Mediante la implementación de la Infraestructura de Clave Pública es posible constituir un servicio de red que emite certificados digitales, y admite también su gestión, controlando las actividades de sus titulares; de esta forma, se establecerá una plataforma de correo electrónico institucional seguro, que garantiza confidencialidad, integridad, autenticación y no repudio, en cada uno de los mensajes transferidos por este medio, mediante la aplicación de dichos certificados, y técnicas criptográficas de cifrado y firma digital.

## II. COCEPTOS BÁSICOS

### *A. Firma Digital*

Es una secuencia binaria que viaja por la red adjunta a un mensaje de datos o documento, para garantizar su integridad y verificar la identidad de quien provino, proporcionando de esta manera, un mecanismo de seguridad en las comunicaciones.

Técnicamente es la combinación de dos mecanismos de seguridad, el cifrado asimétrico y las funciones hash, debido a que aplicarla directamente sobre documentos completos, demandaría de muchos recursos computacionales, es más eficiente emplear un resumen de menor tamaño para ello. [1]

#### *Criptografía*

Es la ciencia que trata sobre técnicas de cifrado que permiten ocultar información para preservar su confidencialidad. Estas técnicas modifican los mensajes de datos utilizando un algoritmo de cifrado y una clave o llave, de manera que puedan descifrarlos e interpretarlos únicamente quienes dispongan de la clave apropiada.

Mediante el uso de la criptografía es posible garantizar ciertos servicios de seguridad de la información, como la confidencialidad (transformándolos en datos ilegibles), la integridad (utilizando funciones hash, el destinatario identifica si los mensajes sufrieron alguna modificación) y el no repudio

(la única manera de descifrar el mensaje es con la llave apropiada, con ello se autentica el origen de dónde provino el mensaje, e implícitamente impide que niegue haberlo enviado). [1]

*Funciones hash*

Las funciones resumen o hash se utilizan para crear la huella (firma) digital de un documento, comprimiéndolo hasta transformarlo en una secuencia de bits infalsificable; a diferencia de las funciones de compresión usuales como ZIP, deben ser irreversibles, con el propósito de salvaguardar la integridad del documento.

Para generar un resumen se realizan distintas operaciones, dependiendo del algoritmo empleado (MD5, SHA1, entre otros), pero se distinguen dos tipos de funciones hash: las que operan directamente sobre el contenido de los mensajes de datos a ser transmitidos llamadas MDC (Modification Detection Codes) y las que utilizan una llave complementaria en sus operaciones, para autenticar a usuarios o dispositivos, ante algún sistema informático o recurso de red, denominadas MAC (Message Authentication Code). [2]

*Distribución y Administración de claves criptográficas*

La fortaleza de los criptosistemas radica en la privacidad de las claves criptográficas, por ello su administración y distribución depende de protocolos y técnicas de cifrado, para garantizar el establecimiento de comunicaciones con entidades remotas fiables.

En criptosistemas de clave privada los métodos de generación de las claves son sencillos, pero su distribución a través de canales inseguros involucra métodos complejos para protegerlas. Los criptosistemas asimétricos notoriamente solventaron el problema de difusión de la clave simétrica, utilizando un par clave; la privada es secreta, y la pública debe ser difundida abiertamente para que todos la conozcan, en bases de datos o directorios de acceso público; de esta forma, la identidad de un usuario remoto está ligada a esta clave.

La desventaja es que una clave pública contiene únicamente una secuencia de bits, que puede ser autogenerada por cualquier persona, utilizando medios informáticos; esto produce una gran vulnerabilidad, al no existir la posibilidad de comprobar que dicha clave es realmente de quien se espera. En base a esto, se ha desarrollado un método denominado Certificado Digital, que al ser emitido por una entidad imparcial (Autoridad de Certificación), vincula legítimamente la identidad de una persona con su clave pública. [1][2]

## *B. Infraestructura de Clave Pública*

La PKI es un sistema de seguridad formado por hardware, software, personas y políticas, que aseguran la emisión y gestión de certificados digitales basados en claves criptográficas, avalando la relación usuario – clave pública, para implantar mecanismos de cifrado y firma digital sobre un conjunto diverso de aplicaciones telemáticas.

El funcionamiento de la PKI depende primordialmente de entidades denominadas autoridades de certificación, apoyadas en autoridades de registro y directorios, que operan bajo ciertos procedimientos de control establecidos por las políticas de seguridad, para gestionar los certificados digitales y enfocar su uso en la protección de información sensible. [3]

*Autoridad de Certificación (CA)*

Es una entidad imparcial en quien emisor y receptor confían mutuamente, aunque ellos no se conozcan con anterioridad (tercero de confianza), podría ser considerada como un notario electrónico que avala la comunicación entre entidades legítimas. Se encarga de verificar y acreditar la identidad de un usuario o dispositivo, a través de la emisión de un certificado digital que lo vincula con una clave pública, como también de su publicación en directorios, su renovación y la revocación o suspensión en caso de que haya expirado, se compruebe falsedad en los datos del registro o se vea comprometida su par clave privada.

La Fig. 1 muestra una arquitectura jerárquica de CAs en la que la fiabilidad radica en la autoridad raíz, que genera su propio certificado avalado por su firma digital (se auto-certifica), convirtiéndose en el respaldo en el que todos los usuarios de un entorno local, ciudad o país confían. Esta CA emite certificados firmados digitalmente a autoridades intermedias, habilitándolas para certificar a autoridades subordinadas, de menor jerarquía en la arquitectura, finalmente éstas últimas son las que certifican a usuarios y dispositivos finales tras un proceso de registro y verificación. [4][5]

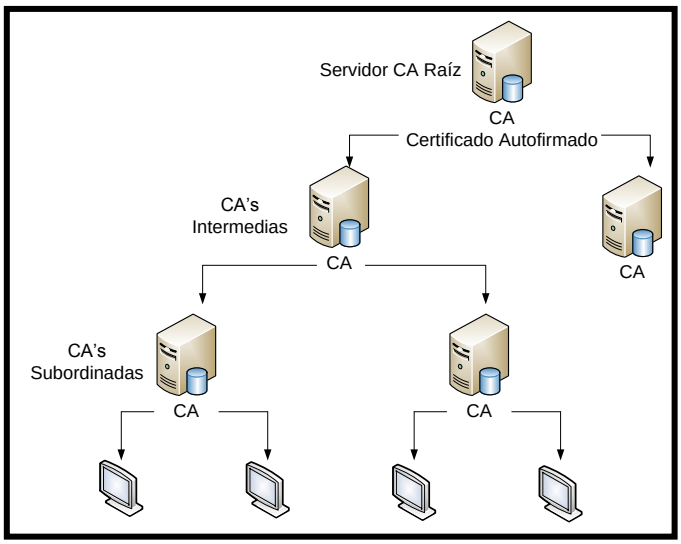


Fig. 1. Arquitectura Jerárquica de Certificación

*Autoridad de Registro (RA)*

Las CAs desempeñan diversas funciones para certificar a autoridades finales o intermedias, pero cuando la PKI cubre entornos con gran demanda de usuarios, o con dependencias geográficamente distantes, resulta complicado dar atención eficiente a todas las peticiones de certificación, incluso la CA podría colapsar por la sobrecarga de actividades.

Por tal motivo, existen ocasiones en las que esta entidad delega a una Autoridad de Registro el proceso de gestión de registro y autenticación de usuarios que soliciten certificación. La ventaja de utilizar esta autoridad adicional es garantizar escalabilidad en el servicio, al implementarse tantas como sean necesarias para dar atención a la mayoría de peticiones de certificación en distintos lugares, limitando a la CA a certificar únicamente a usuarios y dispositivos finales que han sido autenticados y autorizados previamente por la RA.

Es el vínculo entre el usuario final y la CA atendiendo solicitudes de registro, certificación, recuperación de claves o certificados, asociación entre la clave pública y el titular del certificado, y gestión del ciclo de vida de los certificados resaltando la revocación, expiración, renovación, reemisión del par clave criptográfico, o actualización de información del certificado. [4][5]

*Certificado Digital*

Es un documento que asocia la identidad de una persona o dispositivo informático con una clave pública, para demostrar ante los demás que es fiable, evitando potenciales suplantaciones sobre aplicaciones telemáticas de carácter confidencial. Para evidenciar la pertenencia a una entidad, persona o dispositivo informático, pueden contener diversa información, como datos personales de su titular, su clave pública, datos de la entidad que lo emitió, su firma digital y otras consideraciones adicionales; por ello, se ha desarrollado un estándar que especifica el formato de información que debe contener un certificado, la recomendación UIT-T X.509.

Los certificados digitales posibilitan la interacción sobre diversas aplicaciones telemáticas como acceso seguro a servidores web, intranets o redes privadas virtuales, correo electrónico seguro, etc., por tal motivo su emisión varía dependiendo de su propósito y hacia quién o que está destinado. La Fig. 2 muestra las clases que pueden existir.

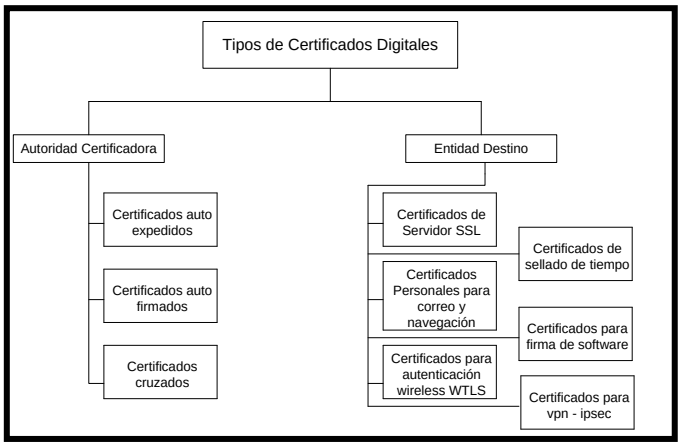


Fig. 2. Tipos de Certificados Digitales

*Directorio de Publicación de Certificados*

Son servicios empleados en entornos PKI para almacenar los certificados emitidos por la CA, manteniéndolos disponibles ante el acceso de usuarios que necesiten recuperarlos, para el establecimiento de comunicaciones seguras. Esto contribuye a su administración al posibilitar su distribución y control de estado de vigencia, mediante listas de revocación. [4]

*Listas de Revocación de Certificados (CRL)*

Los certificados digitales son emitidos para ser válidos durante un periodo de tiempo, pero existen diversas razones que pueden invalidarlos sin necesidad de haber expirado, por ejemplo si la clave privada del usuario se ve comprometida, o si sus datos en el certificado ya no corresponden a los actuales. Por ello la necesidad de que la CA publique una lista en la que consten aquellos certificados que por determinadas circunstancias han sido invalidados, de manera que cualquier entidad esté en capacidad de verificar su estado de vigencia; este directorio se denomina CRL.

Esta lista es de gran importancia en aplicaciones telemáticas, debido a que ninguna de ellas autenticará a una persona o dispositivo, o aceptará una firma digital, en la que se haya empleado un certificado que ya expiró, pero es muy probable que uno revocado siga siendo utilizado. [4]

*C. Correo Electrónico*

Es un servicio que permite la transferencia y recepción de mensajes a través de redes de comunicación, al emplear sistemas informáticos configurados como servidores de correo, que posibilitan su intercambio independientemente del tipo de redes intermedias para llegar a los destinatarios.

*Componentes y Funcionmiento*

Está estructurado de acuerdo a un modelo cliente - servidor, que se comunican entre sí a través de protocolos. El proceso inicia y termina en el extremo del cliente, cuando éste envía o recibe un mensaje empleando una aplicación cliente de correo denominada MUA (Mail User Agent), como Microsoft Outlook, Eudora o Mozilla Thunderbird.

Los servidores de correo están configurados para desempeñar dos procesos diferentes: de agente de transferencia de correo (MTA-Mail Transport Agent), que reenvía los mensajes hacia el MTA que administra el buzón del destinatario; y de agente de entrega de correo (MDA-Mail Delivery Agent), que almacena los mensajes en los buzones correspondientes a cada destinatario para su posterior entrega.

El MUA por parámetros de su configuración identifica a su servidor de correo MTA saliente, entonces para enviar un mensaje, se lo transfiere mediante el protocolo SMTP (Simple Mail Transfer Protocol). Luego el MTA saliente utiliza el dominio de la dirección del destinatario, e inicia una comunicación con el DNS (Domain Name System) al que está vinculado, para identificar al MTA que administra este dominio. Con ello, el MTA de origen establece una conexión TCP con puerto destino 25 hacia el servidor MTA destino, y le transfiere el mensaje original. Finalmente este servidor de destino verifica si tiene alojada la dirección del receptor, y opera como agente MDA para almacenar el mensaje en el buzón del destinatario correspondiente, para su próxima descarga o visualización. La Fig. 3 muestra este proceso.

*Seguridad en Correo Electrónico*

Una alternativa de seguridad es proteger la transferencia de correo empleando protocolos de transporte seguro como TLS. Esto implica que para garantizar fiabilidad en la comunicación extremo a extremo, será necesario en algunos casos asegurar enlaces establecidos entre MTAs intermedios. El problema con ello es que este servicio de red está diseñado para operar bajo un esquema almacenamiento-reenvío, de esta manera TLS protege a los datos en tránsito a través de las redes, pero durante su almacenamiento en nodos intermedios o finales (MDA) quedan totalmente vulnerables, pudiendo ser revisados o alterados antes de que lo haga el destinatario legítimo.

Esto ha generado el desarrollo de técnicas de seguridad que lo protejan durante todo el proceso de transferencia hacia el destinatario, sin necesidad de implantar adicionalmente mecanismos complejos de seguridad a nivel de capa transporte o red, o peor aún modificando la infraestructura de correo.

Actualmente la mayoría de plataformas de correo electrónico seguras emplean técnicas criptográficas en los agentes MUA, que generen correos auto-protegidos mediante cifrado y/o firma digital en capa aplicación, de modo que los MTA los transfieran de forma convencional a su destino.

Algunos de estos sistemas de seguridad usados comúnmente son PGP y S/MIME, el primero se basa en el manejo de par claves criptográficas (pública - privada), y el segundo mucho más seguro en base a certificados digitales; lo desventajoso es que no son compatibles. [6]

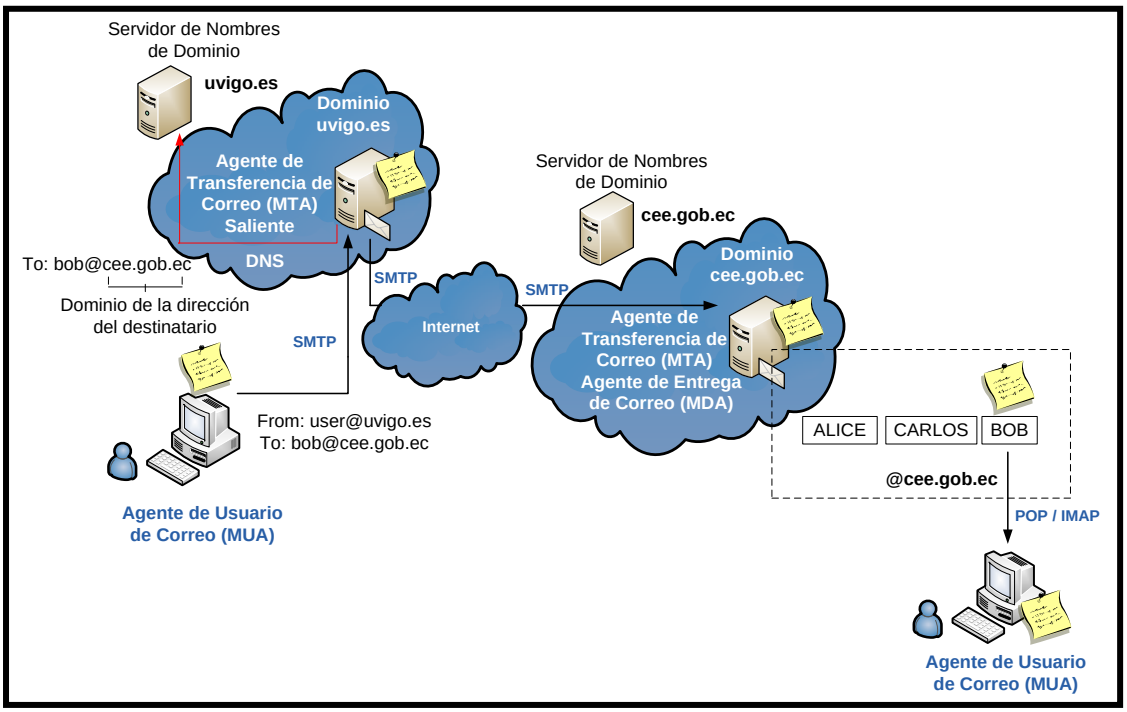


Fig. 3. Proceso de envío y recepción de un e-mail

## III. Diseño de la infraestructura PKI y de la plataforma de correo electrónico

### A. *Criterios de Diseño*

El propósito primordial de este proyecto es la certificación de los funcionarios y militares del Cuerpo de Ingenieros del Ejército (CEE) de Quito, mediante la emisión de certificados digitales que vinculen legítimamente su identidad con su clave pública generada, demostrando así que son entidades fiables.

De esta forma, el requerimiento es configurar una Autoridad Certificadora Raíz que auto-genere su certificado, convirtiéndose desde este momento en una entidad legítimamente autorizada para prestar servicios de certificación, en el entorno del CEE. Sin embargo, esta entidad no solo estará destinada a emitir certificados, también deberá gestionarlos, integrándose con componentes adicionales para implantar una Infraestructura de Clave Pública. La Tabla I muestra estos componentes.

TABLA I
COMPONENTES ESTRUCTURALES

| COMPONENTE | DESCRIPCIÓN |
|---|---|
| **Autoridad de Registro (RA)** | Destinada a atender solicitudes de registro, recuperación de claves o certificados, gestión del ciclo de vida de los certificados, actualización de información de usuario, entre otras. |
| **Directorio de Publicación de Certificados** | Almacenará los certificados de usuario emitidos, para que los obtengan y utilicen en la protección de correo. |
| **Listas de Revocación de Certificados** | Es un documento que publicará y actualizará permanentemente la CA, para dar a conocer los certificados que han sido revocados (invalidados). |

Dentro de las consideraciones de diseño de una PKI, los aspectos referentes a su funcionamiento están muy ligados a la (s) vía (s) de entrega de los certificados que se tenga planificado; esto debido a que la CA puede ser configurada para entregarlos a sus propietarios empleando medios tanto de hardware como de software.

Los tokens criptográficos usb son dispositivos de hardware comúnmente empleados para almacenar de forma segura certificados digitales y claves privadas. En cuanto a las herramientas de software, una de las alternativas más usuales es emitirlos en un formato p12 o pfx para que sean almacenados en los ordenadores de usuario final.

En tal virtud, en el entorno PKI del CEE los certificados de usuario serán distribuidos empleando el formato p12, posteriormente cuando los funcionarios y autoridades de esta entidad estén más relacionados con este sistema, se podría implementar la distribución en tokens usb.

La segunda parte del proyecto es diseñar una plataforma de correo electrónico basada en herramientas de software libre, que provea las funcionalidades de la actual desarrollada sobre Exchange, aportando de esta manera con la migración hacia nuevos sistemas que proporcionan servicios similares a los privativos, pero que requieren de menor inversión para implementarlos, o en el mejor de los casos no tienen costo.

La alternativa más habitual para proteger este servicio es utilizar el protocolo de capa transporte TLS; sin embargo, para garantizar una comunicación segura extremo a extremo sería necesario cifrar todos los enlaces intermedios que puedan intervenir durante la transferencia.

La solución más idónea es generar correos auto-protegidos mediante cifrado y/o firma digital, en capa aplicación, de manera que los MTA los transfieran de forma convencional a su destino, con ello se garantiza la protección durante todo el proceso de transferencia, incluso mientras están alojados en el buzón de los destinatarios.

Es así que, la seguridad del correo electrónico institucional del CEE, a diseñarse, será implementada utilizando en primera instancia el protocolo TLS para securizar los enlaces de

comunicación establecidos entre cliente/servidor, pero el mecanismo prioritario de protección será la implementación de S/MIME para generar correos auto-protegidos.

*B. Modo de Operación*

Se ha considerado como medida de seguridad, que el usuario final (funcionario público o militar del CEE) no debe formar parte del proceso de solicitud e instalación de certificados en el entorno de la institución, ellos únicamente estarán destinados y serán capacitados para utilizar este mecanismo de seguridad, en la protección de información transferida por el correo electrónico institucional; será el administrador de red conjuntamente con un grupo capacitado quienes lleven a cabo estas actividades.

En base a esto, las actividades que tendrá que desempeñar el Administrador de red en el proceso de certificación son las que se muestran en la Fig. 4, considerando la interacción de los componentes que integrarán la PKI del CEE.

Esto permitirá que cada usuario de esta institución disponga de un certificado legítimo instalado en su ordenador personal. Complementariamente el administrador configurará el agente de correo (MUA) de cada usuario para integrar este certificado, y activará las técnicas S/MIME para proteger los e-mails transferidos con mecanismos de cifrado y firma digital.

En este punto del desarrollo del proyecto, la interacción de los ordenadores de los usuarios al enviar un mensaje firmado digitalmente, es mostrada en la Fig. 5.

1. El emisor a través del agente de correo de usuario Outlook, genera un mensaje con estructura S/MIME, al cual lo firmará con su clave criptográfica privada.
2. Este mensaje auto-protegido será transferido de manera habitual, empleando el protocolo de transporte SMTP, y TLS para cifrar el canal de comunicación, almacenándose finalmente en el servidor de correo de forma convencional.
3. El destinatario accederá a su buzón y descargará su mensajería pendiente utilizando el protocolo POP3, con seguridad SSL para cifrar la conexión.
4. Obtendrá el mensaje S/MIME.
5. El agente MUA detectará su estructura y obtendrá el certificado digital X.509 del emisor, que contiene este mensaje, para verificar su validez, empleando las listas de revocación de certificados (CRLs) que la PKI del CEE publicará constantemente, luego verificará su vigencia, y finalmente la firma digital que contiene, generada por la CA.
6. Si el certificado es legítimo verificará la firma digital del mensaje para determinar si no ha presentado ningún tipo de alteración desde que fue creado, e implícitamente la autenticidad del emisor. Además el receptor debe agregar a sus contactos de Outlook al emisor, almacenándolo conjuntamente con su certificado digital, que será utilizado desde ese momento para enviarle mensajes cifrados, y garantizar que sólo él pueda revisarlos.

En el caso del envío de mensajes cifrados es el mismo proceso de transferencia, pero difieren las operaciones criptográficas. La Fig. 6 muestra este proceso de verificación.

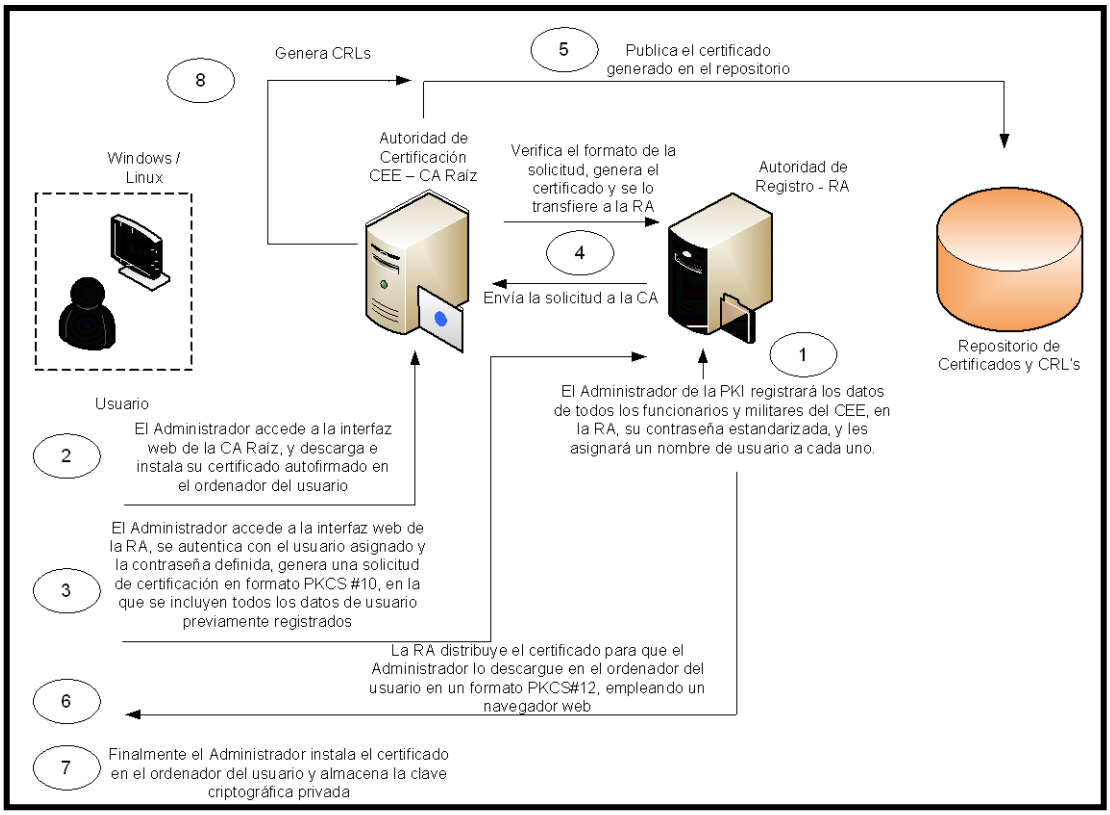


Fig. 4. Proceso de certificación en el entorno PKI

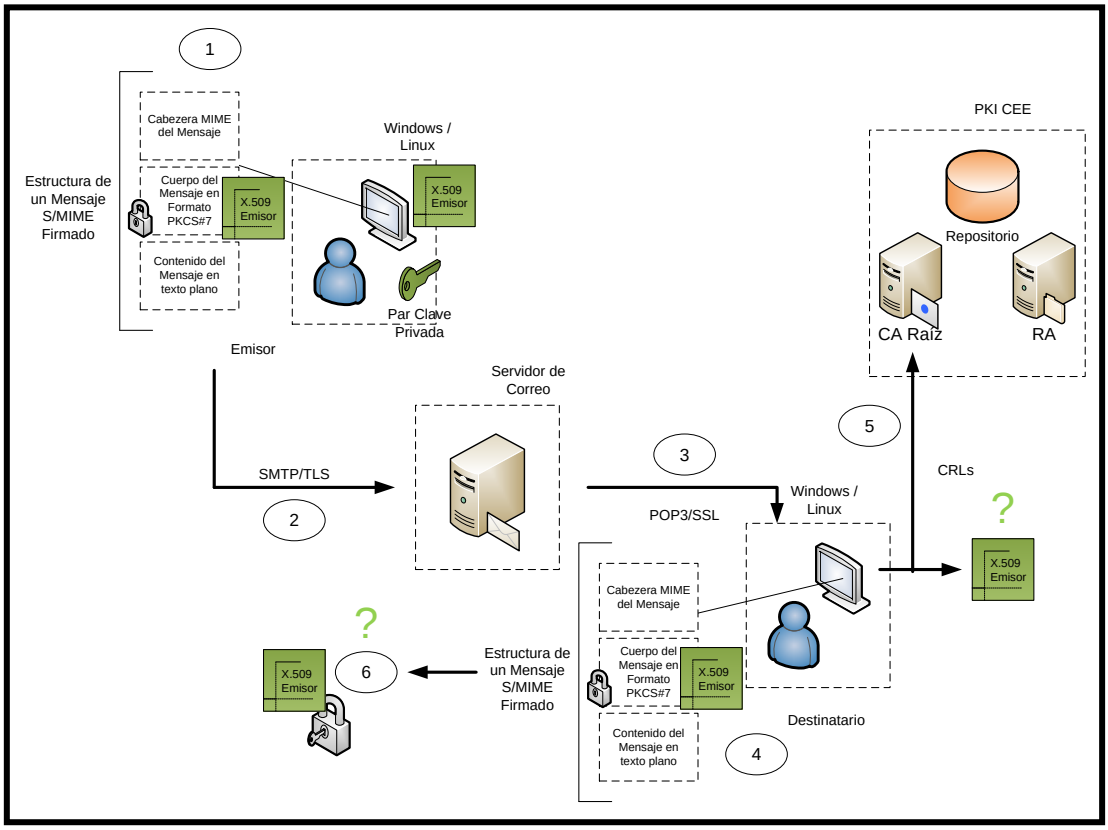


Fig. 5. Interacción del usuario, la PKI y el sistema de correo en el entorno del CEE – Mensaje Firmado

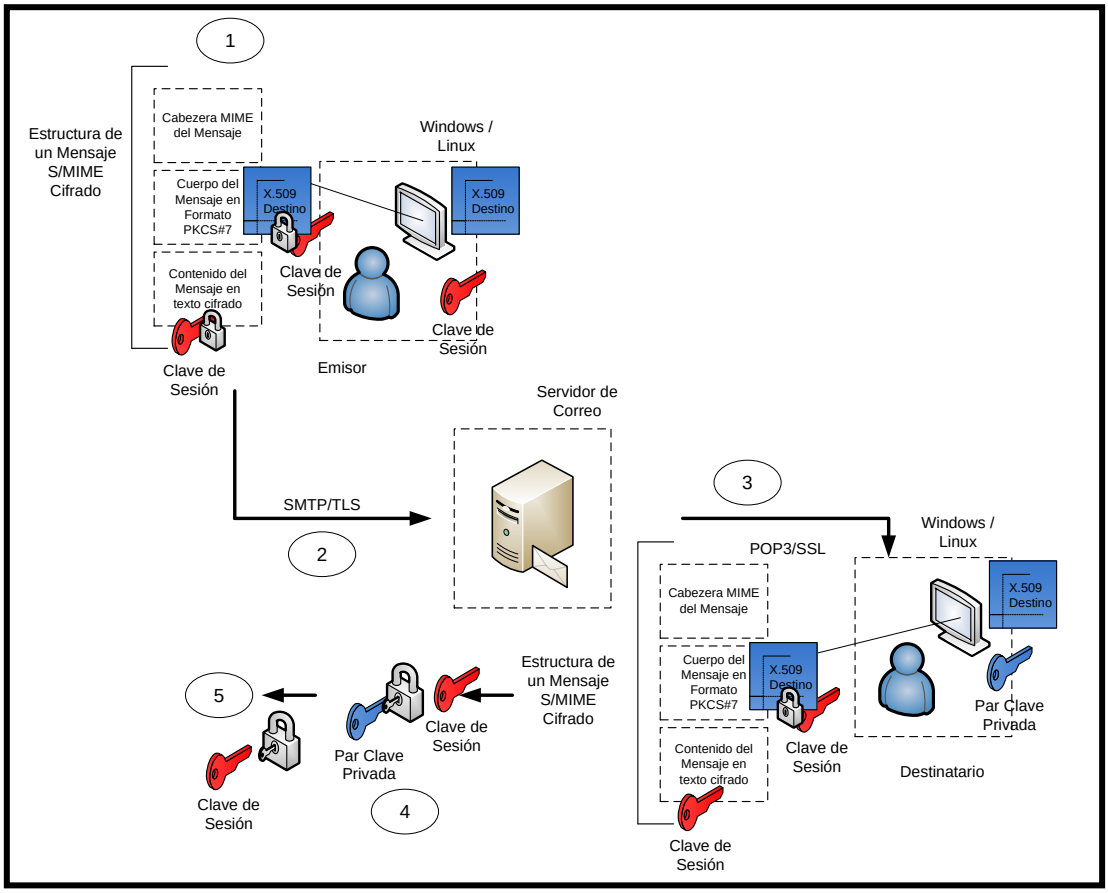


Fig. 6. Interacción del usuario, la PKI y el sistema de correo en el entorno del CEE – Mensaje Cifrado

- El ordenador del emisor generará una clave de sesión que será cifrada utilizando el certificado del destinatario, garantizando de esta forma que sólo él pueda descifrarla con su clave privada. El contenido del mensaje será cifrado con la clave de sesión.
- El destinatario con su par clave privada descifra la clave de sesión, y finalmente el mensaje para revelar su contenido.

Finalmente uno de los requerimientos primordiales de este proyecto es migrar la información de los buzones creados en servidor de correo actual (mensajería, contactos, calendario), desarrollado sobre Microsoft Exchange, hacia la nueva plataforma sobre software libre, para garantizar que durante la transición los usuarios conservarán toda su información.

### C. *Principales Herramientas empleadas*

- **EJBCA.-** Es un software que permite implementar una PKI construida en base a J2EE (Java 2 Platform, Enterprise Edition) con la capacidad de desempeñar todas las funciones de una CA (Autoridad Certificadora, de Registro y emisión de CRLs), sin necesidad de emplear herramientas adicionales que la complementen; esto es debido a que está estructurada por componentes que cumplen cada uno con su función designada. [7]

- **JBOSS AS.-** Es un servidor de aplicaciones diseñado para soportar el despliegue de aplicaciones empresariales de alto rendimiento sobre J2EE, que al operar bajo una licencia de código abierto, posibilita su descarga, instalación, ejecución y libre distribución sin ningún tipo de restricciones, este es el motivo por el cual es una de las plataformas más usuales en aplicaciones reales de producción. Su principal función consiste en gestionar la mayor parte de la lógica de las aplicaciones desarrolladas y el acceso a sus datos; con la ventaja de que para su desarrollo no es necesario programarlas, sino más bien ensamblarlas a partir de módulos provistos por este servidor.

- **ZIMBRA COLLABORATION SUITE (ZCS).-** Es un proyecto de colaboración que ha desarrollado un software completo de mensajería de código abierto, que ofrece un servicio de correo electrónico fiable y de alto rendimiento, con funcionalidades complementarias como libretas de direcciones, agendas y diversas tareas adicionales. El núcleo de este proyecto es el servidor zimbra, que ha sido desarrollado en base a JAVA, utilizando Jetty como servidor de aplicaciones. Está integrado por varios sistemas: el MTA basado en Postfix, almacenes de datos para información de usuarios en base a OpenLDAP y MySQL, soporte para protocolos de cifrado SSL/TLS, incorpora mecanismos de seguridad como antivirus y antispam, y un potente motor de búsqueda de mensajes basado en Lucene.

- **MICROSOFT EXCHANGE 2010.-** Es el software sobre el que se ha desplegado el sistema de correo actual del CEE de Quito.

### D. *Dimensionamiento de Hardware*

Generalmente, los parámetros de hardware relevantes que deben considerarse al implementar un servidor son: el procesador, la memoria RAM y la capacidad de almacenamiento. Para dimensionar estos parámetros, en este proyecto se han considerado los requerimientos mínimos de las principales aplicaciones implícitas en su desarrollo, como EJBCA, JBoss, MySQL, Zimbra Collaboration Suite y también el sistema operativo anfitrión para cada servicio; garantizando de esta forma su operatividad.

La capacidad de procesamiento es determinada mediante el análisis del comportamiento de un usuario común frente al servicio de red, e involucra conocer las operaciones que ejecuta, el tiempo que demanda hacerlo y la frecuencia con que las realiza. La Tabla II resume las características de hardware recomendadas para implantar estos servicios de red.

TABLA II
CARACTERÍSTICAS DE HARDWARE

| PARÁMETRO | REQUERIMIENTO MÍNIMO |
|---|---|
| **INFRAESTRUCTURA DE CLAVE PÚBLICA** | |
| **Memoria RAM** | 4 GB |
| **Procesador (CPU)** | 2 núcleo que operen a 3 Ghz |
| **Disco Duro** | 160 GB |
| **SERVIDOR DE CORREO** | |
| **Memoria RAM** | 4 GB |
| **Procesador (CPU)** | 2 núcleo que operen a 3 Ghz |
| **Disco Duro** | 160 GB |

## IV. PRUEBAS DE FUNCIONAMIENTO

Su ejecución implica que cada ordenador personal de usuario tenga instalado el certificado digital respectivo, y configurado el agente de correo Outlook para implantar técnicas S/MIME de protección.

### A. *Escenarios de Prueba*

Se realizará la captura y el análisis de paquetes para intentar vulnerar la confidencialidad de los mensajes transferidos. La Fig. 7 expone el correo en cuestión.

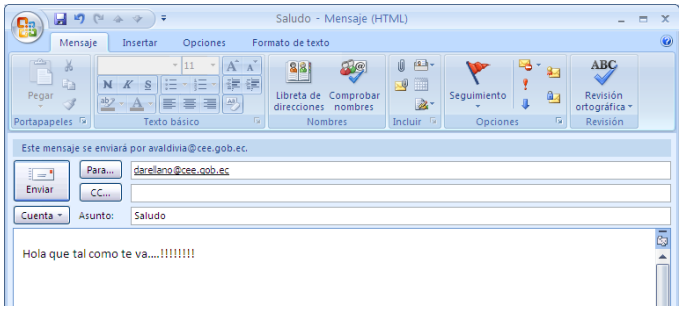


Fig. 7. Correo a analizarse

Esto se ha realizado empleando el analizador de tráfico de uso generalizado (Wireshark), sobre varios tipos de mensajes.

*Mensaje en texto plano*

En el analizador se aplica un filtro sólo para capturar paquetes del protocolo SMTP que es lo que interesa; cuando inicia la captura sobre cualquier paquete hacer click derecho y elegir la opción Follow TCP stream, esto permite visualizar la conversación tal como ocurrió. La Fig. 8 muestra el resultado esta operación.

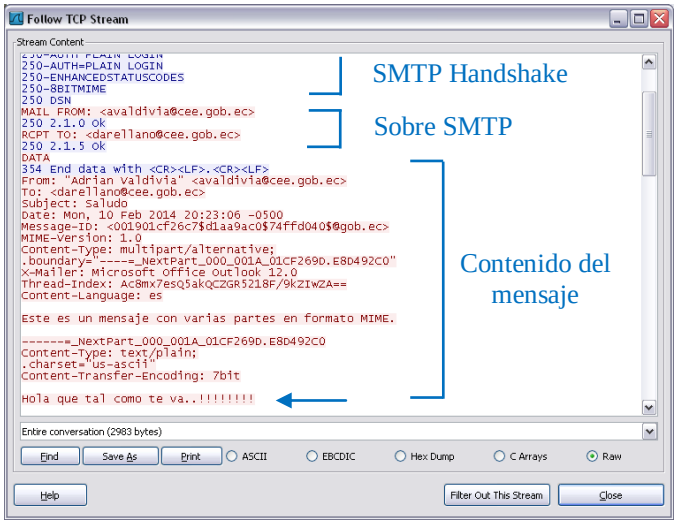


Fig. 8. Captura SMTP con Wireshark

En esta captura se ha podido revelar las direcciones de correo electrónico del emisor y receptor, y además es posible visualizar el mensaje en sí; por lo que se concluye que este tipo de mensajes convencionales no imponen ningún tipo de oposición ante técnicas que intenten vulnerarlos.

*Mensaje cifrado*

Se efectuó el mismo procedimiento, y los resultados los muestra la Fig. 9.

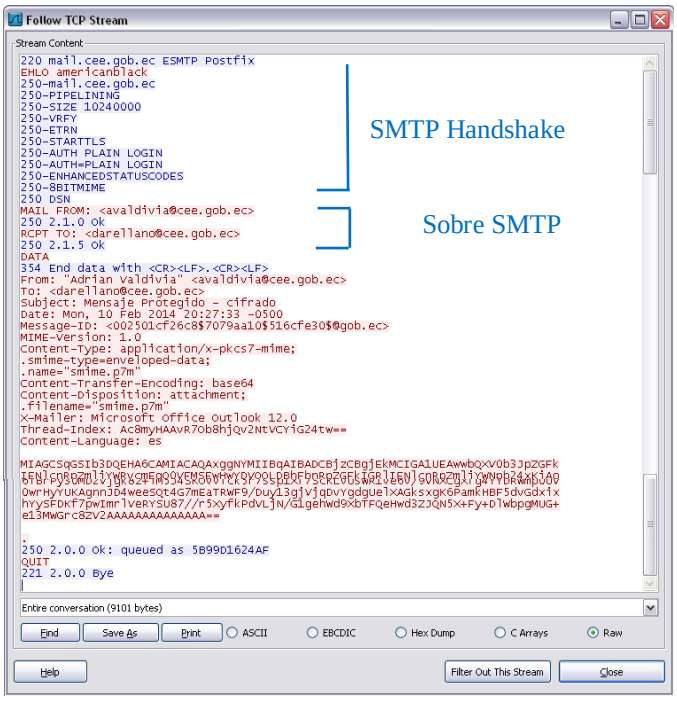


Fig. 9. Captura SMTP con Wireshark

En esta captura se puede apreciar que los dos primeros campos estructurales del mensaje no han variado, pero el contenido del mensaje ha sido transformado a un formato ilegible, generando de esta forma mensajes auto-protegidos que pueden ser transferidos convencionalmente por el servidor de correo, y que van a ser almacenados de ésta forma en este servidor.

*Mensaje cifrado transferido empleando TLS*

La operación es la misma pero adicionalmente se ha activado en el cliente de correo Outlook este protocolo de protección en capa transporte. La Fig. 10 muestra los resultados.

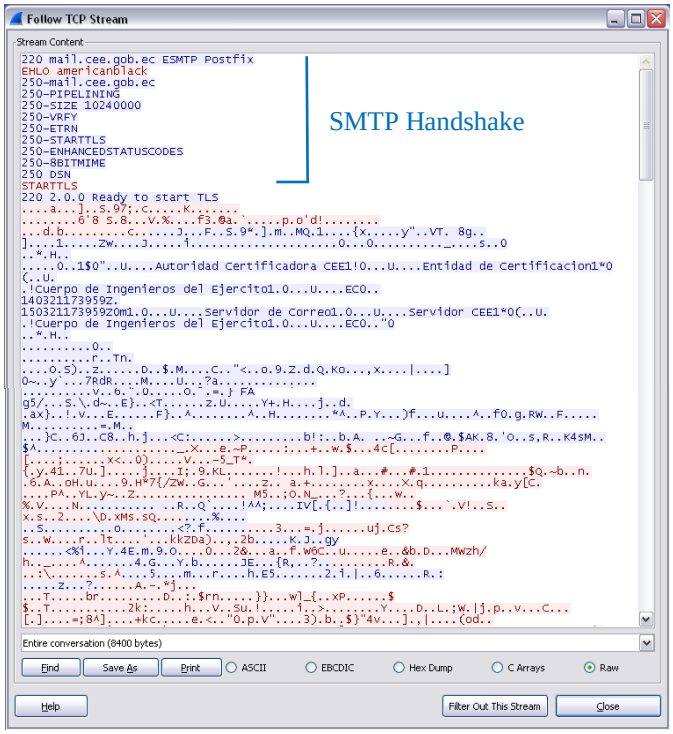


Fig. 10. Captura SMTP con Wireshark

Se puede observar que este mecanismo complementa la seguridad del sistema, ocultando el sobre SMTP que contiene las direcciones de correo origen y destino. Esto resulta útil porque en ocasiones a los hackers no les interesa revelar el contenido de mensajes al azar, sino determinar de quién provienen y hacia quién están dirigidos, para ejecutar seguimientos especiales sobre la información que manipula alguien en específico.

Con esto se concluye que las herramientas desarrolladas, y las configuraciones realizadas en este proyecto, cumplen con su propósito principal, la seguridad del correo electrónico institucional.

## V. CONCLUSIONES

La transferencia fiable de mensajes de correo electrónico es garantizada mediante la implementación de mecanismos criptográficos que los protegen usualmente mientras están en tránsito a través de las redes, en base al protocolo TLS; pero la alternativa más efectiva que además los protege durante su almacenamiento en los buzones avalando una comunicación segura extremo a extremo, son las extensiones S/MIME, que

operan en capa aplicación para generar mensajes auto-protegidos, y permiten implementar el mecanismo de firma digital.

Durante el diseño de la Infraestructura de Clave Pública es trascendental definir una ubicación estratégica para la CA Raíz, aislándola de la granja de servidores del CEE, para preservar la operatividad del sistema de certificación. El objetivo es restringir el acceso hacia este servidor, tratando en lo posible de proteger su clave criptográfica privada.

La Jerarquía de Certificación configurada para el Cuerpo de Ingenieros del Ejército, está basada en una arquitectura plana, siendo la CA Raíz quien certifica directamente a usuarios finales, con la posibilidad de complementarla con CAs subordinadas o intermedias, para ampliar eficientemente el servicio de certificación, hacia los grupos de trabajo remotos de esta institución.

La interfaz de administración de EJBCA provee funcionalidades de seguridad en base al número de serie de los certificados, para restringir el acceso de usuarios que intenten vulnerarla empleando un certificado digital fraudulento; esto significa que únicamente los administradores tendrán autorizado el acceso a los diversos recursos de la PKI, tras autenticarse con el certificado autorizado.

La Infraestructura de Clave Pública diseñada cumplió con los propósitos de emisión y gestión de certificados digitales X.509 efectuados durante la etapa de pruebas de funcionamiento, resaltando la compatibilidad que se logró con los agentes de usuario de correo MUA, para cifrar y firmar digitalmente los mensajes transferidos por este medio.

Con este trabajo de investigación se ha demostrado que es posible integrar un mecanismo de seguridad basado en certificados digitales personales, sobre una de las plataformas de comunicación más generalizadas en la actualidad, el correo electrónico, para proteger el flujo de información que circula a través de este medio.

Se pudo comprobar que en realidad los mensajes fueron protegidos durante todo el proceso de su transferencia, siendo únicamente los destinatarios legítimos quienes pudieron revertir los mensajes cifrados, verificar la integridad de la firma digital y la autenticidad del emisor.

## RECONOCIMIENTOS

Se manifiesta un reconocimiento especial al Departamento de Sistemas del Cuerpo de Ingenieros del Ejército de Quito, destacando al Ing. Freddy Chuquimarca, Administrador de Red de esta institución, y al Capitán Braulio Moreno, por la apertura, el apoyo y la colaboración prestada en beneficio del desarrollo de este proyecto.

## REFERENCIAS

[1] Stallings, W. (2006). Cryptography and Network Security Principles and Practice. Recuperado de http://evilzone.org/ebooks/cryptography-and-network-security-principles-(5th-edition)/.

[2] Lucena, M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de http://es.scribd.com/doc/39400098/Criptografia.

[3] Cuesta, J., & Puñales, M. (2002). Seguridad en Redes Telemáticas-Infraestructura de Clave Pública (PKI). Recuperado de http://es.scribd.com/doc/116154580/Infraestructura-de-clave-publica-PKI.

[4] INDRA Sistemas, S.A. (2005). Infraestructura de Clave Pública (PKI). Recuperado de http://www.inteco.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

[5] Osorio, J. M. (s.f.). Evaluación de la Herramienta EJBCA para un prestador de Servicios de Certificación. (Proyecto Final de Carrera). Universidad Politécnica de Cataluña, Barcelona, España.

[6] Perramon, X. (s.f.). Aplicaciones Seguras. Recuperado de http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01772.pdf

[7] Ayesha, I. G. & Asra, P. (2006). PKI Administration using EJBCA and OpenCA. Recuperado de http://teal.gmu.edu/courses/ECE646/project/reports_2006/IL-3-report.pdf.

**Director – Ing. Carlos A. Vásquez A.**

Nació en Quito, provincia de Pichincha, el 19 de Septiembre de 1981. Ingeniero en Electrónica y Telecomunicaciones (CUM LAUDE), Escuela Politécnica Nacional (EPN) en Quito-Ecuador 2008. Actualmente, es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador. Aprobó los cursos CCNA 1, 2, 3 y 4 en el período junio 2006 – marzo 2007 en la Escuela Politécnica Nacional, y cursa la Maestría en Redes de Comunicación, Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

**David R. Valencia T.**

Nació en Ibarra, Imbabura el 30 de Mayo de 1987. Segundo hijo de Nelson Valencia y Gladys de la Torre. La educación primaria la realizó en la Escuela Fiscal de Niños “28 de Septiembre”. En el año 2005 obtuvo su título de Bachiller en Ciencias con especialización Físico Matemático en el Colegio Nacional “Teodoro Gómez de la Torre”. Actualmente, es egresado de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.