ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TÍTULO DEL PROYECTO

Prototipo para la generación y administración de certificados digitales para el sistema financiero del Ecuador y la superintendencia de bancos y segros

Previa a la obtención del Título de:

INGENIERO DE SISTEMAS E INFORMÁTICA

POR:
JUAN C. BENALCÁZAR Z.

Sangolquí, diciembre de 2010

CERTIFICACION

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. JUAN CARLOS BENALCÁZAR ZAPATA como requerimiento parcial a la obtención del título de INGENIERO DE SISTEMAS E INFORMÁTICA.

Sangolquí, 12 de abril de 2007

ING. Fernando Galarraga

DEDICATORIA

Dedico la presente tesis a los seres que más amo en este mundo: a mis padres por darme la vida y una carrera para mi futuro, a mis hermanos por ser mis mejores amigos y a quienes exaltó para que sigan adelante y a mi querida Alexita, por ser la fuente de mi inspiración y motivación para superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

Juan C. Benalcázar Z.

AGRADECIMIENTOS

Quiero extender un sincero agradecimiento de todo corazón a todos quienes de una u otra manera, han colaborado para la consecución de esta etapa en mi vida, doy gracias a mi Dios por permitirme tener la vida y la capacidad de alcanzar la culminación de mi carrera.

A mis padres que con su sacrificio, dedicación y amor han inculcado los valores de responsabilidad, sacrificio, solidaridad y superación, a mis hermanos que siempre han estado ahí cuando los he necesitado, quienes me han brindado sus palabras de aliento y cariño.

A mi Escuela Politécnica del Ejército por abrirme sus puertas y permitirme obtener la formación necesaria para contribuir al desarrollo de mi país, por brindarme la oportunidad de fortalecer mis valores patrióticos y representarlo dignamente en competiciones deportivas, a sus autoridades que supieron apoyarme en la realización de programas y eventos interuniversitarios.

A mis maestros, que han sido mis amigos y han guiado con certeza el camino que ahora nuevamente empieza, aquellos que me han enseñado que la única manera de cambiar el futuro de nuestro país, es siendo sincero con uno mismo, cultivando cada día la ética y el profesionalismo.

A las autoridades de la Superintendencia de Bancos y Seguros que confiaron en mis capacidades y me permitieron demostrar que con sacrificio y voluntad, se pueden alcanzar los proyectos por arduos e inalcanzables que parezcan.

A mi director de tesis Ing. Fernando Galárraga, codirector y profesor informante Ing. Héctor Revelo y a la Dra. Jacqueline Guerrero por su paciencia, consejos y apoyo durante la realización de este proyecto, a las autoridades de la Facultad que supieron canalizar positivamente mis solicitudes.

Finalmente, quiero agradecer de manera especial a esa persona que ha compartido de cerca mis angustias y gratificaciones, que siempre me ha brindado su apoyo incondicional, que ha sido un pilar fundamental en mi carrera y mi vida, y estoy totalmente convencido que nadie va a estar más feliz que tú, con todo mi amor para ti Ale.

Juan C. Benalcázar Z.

"Un hombre sin estudios es un ser incompleto. La instrucción es la felicidad de la vida; y el ignorante, que siempre está próximo a revolverse en el lodo de la corrupción, se precipita luego infaliblemente en las tinieblas de la servidumbre."

Libertador, Simón Bolívar

TABLA DE CONTENIDO

INDICE GENERAL

CERTIFICACION ii

DEDICATORIA iii

AGRADECIMIENTOS iv

RESUMEN 1

INTRODUCCIÓN 3

CAPITULO 1 5

PRINCIPIOS BÁSICOS DE LA CERTIFICACIÓN DIGITAL ---------- 5
1.1. INFRAESTRUCTURA DE CLAVE PÚBLICA ---------- 5
1.1.1. Definición ---------- 5
1.1.2. Misión ---------- 6
1.1.3. Servicios ---------- 6
1.2. MECANISMOS BÁSICOS DE SEGURIDAD ---------- 7
1.2.1. Criptografía ---------- 7
1.2.2. Firma Digital ---------- 14
1.2.3. Certificados Digitales ---------- 19
1.3. ELEMENTOS DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA ---------- 29
1.3.1. Autoridad Certificadora ---------- 29
1.3.2. Autoridad de Registro ---------- 32
1.3.3. Políticas de Certificación ---------- 34
1.3.4. Repositorio de Certificados o Directorios ---------- 35
1.3.5. Seguridades y Estándares Técnicos ---------- 38
1.4.1. Flexibilidad y Compatibilidad ---------- 41
1.4.2. Sencillez ---------- 42
1.4.3. Interoperabilidad ---------- 42
1.4.5. Confianza en la AC/AR ---------- 45

CAPITULO 2 46

MARCOS LEGALES NACIONALES E INTERNACIONALES SOBRE CERTIFICACIONES DIGITALES ------- 46
2.1. MARCO LEGAL INTERNACIONAL ---------- 46
2.2. MARCO LEGAL NACIONAL ---------- 51
2.2.1. Antecedentes en la Superintendencia de Bancos y Seguros ---------- 51
2.2.2. Legislación ---------- 53

CAPITULO 3 58

ESQUEMAS DE CERTIFICACIÓN ---------- 58
3.1. ARQUITECTURAS DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA ---------- 58
3.1.1. Jerárquica ---------- 58
3.1.2. Mesh (Malla) ---------- 59
3.1.3. Bridge (Puente) ---------- 60
3.2. COMO AUTORIDAD CERTIFICADORA (SBS AC) ---------- 62
a. Consideraciones Operativas ---------- 62
b. Consideraciones Legales ---------- 62
c. Consideraciones Técnicas ---------- 63
d. Arquitectura ---------- 63
3.3. COMO AUTORIDAD DE REGISTRO (SBS AR) ---------- 65
a. Consideraciones Operativas ---------- 65
b. Consideraciones Legales ---------- 65
c. Consideraciones Técnicas ---------- 65
d. Arquitectura ---------- 65
3.4. ESQUEMA SELECCIONADO POR LA INSTITUCIÓN ---------- 66

3.5. MODELO DE SEGURIDAD PARA LA AC ---- 67
3.6. ESTÁNDARES TECNOLÓGICOS UTILIZADOS ---- 69

CAPITULO 4 ..... **71**

DESCRIPCIÓN DE APLICACIONES COMERCIALES ---- 71
4.1. PRODUCTOS DE ENTRUST. ---- 71
a. Antecedentes de la empresa ---- *71*
b. Características del producto ---- *72*
4.2. PRODUCTOS VERISING. ---- 74
a. Antecedentes de la empresa ---- *74*
b. Características del producto ---- *75*
4.3. PRODUCTOS DE PGP CORPORATION. ---- 77
a. Antecedentes de la empresa ---- *77*
b. Características del producto ---- *78*
4.4. PRODUCTOS DE ADEXUS (RSA) ---- 79
a. Antecedentes de la empresa ---- *79*
b. Características del producto ---- *80*
4.5. ESTADO DEL ARTE EN ECUADOR ---- 82
a. Las Tecnologías de Información en Ecuador ---- *82*
b. Penetración de la Internet en Ecuador ---- *84*
c. Gobierno Electrónico ---- *85*

CAPITULO 5 ..... **88**

DESARROLLO DEL PROTOTIPO ---- 88
5.1. ANÁLISIS DE REQUERIMIENTOS ---- 88
a. Objetivo y Alcance de la SBS AC ---- *88*
b. Requerimientos de Diseño ---- *89*
c. Requerimientos del usuario ---- *91*
d. Requerimientos de Seguridad ---- *91*
5.2. SERVICIOS DISPONIBLES ---- 92
a. Servicios de manejo de llaves para firmas digitales ---- *93*
b. Servicio de manejo de certificados ---- *94*
c. Servicios de publicación y almacenaje de llaves, certificados y CRL ---- *98*
d. Servicios de interfaz con el cliente ---- *98*
5.3. DEFINICIÓN DE HERRAMIENTAS Y FUNCIONES PARA EL DESARROLLO DE LOS SERVICIOS ---- 99
a. Instalación del Lotus Domino Server 6.0.2 ---- *99*
b. Instalación de Lotus Notes, Lotus Domino Administrador y Lotus Domino Designer. ---- *100*
c. Configuración del Lotus Domino Server 6.0.2 ---- *100*
d. Configuración de Lotus Domino Certificate Authority ---- *100*
e. Definición de políticas de administración y usuarios. ---- *101*
5.4. PROTOCOLOS DE COMUNICACIÓN ---- 105
5.5. DESCRIPCIÓN DE ENTIDADES ---- 105

CAPITULO 6 ..... **107**

6.1. CONCLUSIONES ---- 107
6.2. RECOMENDACIONES ---- 108

REFERENCIAS BIBLIOGRÁFICAS **110**

LISTADO DE TABLAS

Tabla 1. Estándares tecnológicos. 69
Tabla 2. Estándares PKCS. 70

LISTADO DE CUADROS

Cuadro 1. Resumen de entidades financieras controladas por la SBS. 55
Cuadro 2. Penetración del Internet en el Ecuador. 85
Cuadro 3. Contenido de Certificados X.509 (versión 3) 96

Cuadro 4. Contenido de Certificados X.509 (versión 3) para certificación WEB. 96
Cuadro 5. Contenido de Certificados X.509 (versión 3) para usuarios finales. 97
Cuadro 6. Formulario para el solicitante del certificado. 97

LISTADO DE FIGURAS

Figura 1. Procesos de la Criptografía 8
Figura 2. Distribución de la llave pública 16
Figura 3. Uso de la Firma Digital para verificar la identidad 17
Figura 4. Certificado válido y emitido por la Autoridad Certificadora SBS AC de la Superintendencia de Bancos y Seguros 23
Figura 5. Mensaje de advertencia cuando un certificado ha caducado o aún no ha entrado en vigencia 26
Figura 6. Visión macro de una PKI 29
Figura 8. Esquema de una Infraestructura Jerárquica Subordinada 59
Figura 9. Esquema de una Infraestructura en Malla 59
Figura 10. Esquema de una Infraestructura en Puente 61
Figura 11. Esquema de certificación donde la SBS es reconocida por un nivel superior 64
Figura 12. Arquitectura Tipo Estrella 66
Figura 13. Diagrama de Comunicaciones 68
Figura 15. Estructura SBS AC 91

LISTADO DE ANEXOS

ANEXO A.- Metodología para el Diseño de una Infraestructura de Clave Pública 111
ANEXO B.- Instalación y Configuración del Prototipo en Lotus 118
ANEXO C.- Marco Legal Ecuatoriano 119

RESUMEN

Este documento, es un trabajo de investigación que tiene como propósito contribuir con el avance de la aplicación de nuevas tecnologías de información en el Ecuador, aquí se hace una recopilación de los conceptos básicos de certificación digital, elementos y mecanismos básicos de seguridad de una Infraestructura de Clave Pública (PKI), se describen también los marcos legales internacionales y nacionales donde se establecen los criterios jurídicos sobre la factibilidad de la implementación de este esquema en el ámbito de la supervisión y control financiero, así como también una reseña histórica de la evolución de las leyes dentro de la conocida **"Sociedad de la Información"** y las que fundamentaron la creación de la Ley de Comercio Electrónico en el Ecuador.

Se establecen también los esquemas de certificación considerados como los más importantes según organismos especializados que tiene mayor experiencia en el tema, se analizaron y probaron herramientas informáticas desarrolladas específicamente para el negocio, las que permitieron establecer la complejidad en la administración y conceptualización del prototipo, dentro del aspecto técnico.

Finalmente, se desarrolla un prototipo para la Generación y Administración de Certificados Digitales para el intercambio de información entre las Entidades Financieras y la Superintendencia de Bancos y Seguros, usando la Certificación Digital como herramienta para aumentar los niveles de seguridad en las transacciones realizadas, se propone un esquema de certificación que se ajusta a las necesidades de la Institución así como también un marco jurídico y técnico que soporta las exigencias de la implementación de una Infraestructura de Clave Pública.

Es importante mencionar, que durante el desarrollo del proyecto existieron muchas dificultades al momento de consolidar la información en relación a los conceptos relacionados con la Infraestructu-

ra de Clave Pública, esquemas de certificación y el marco legal, la abundancia de información en muchos casos y la insuficiencia de experiencias en el medio se convirtieron en cuellos de botella, obviamente estos problemas se complicaron al momento de definir los objetivos, servicios, políticas y procedimientos de funcionamiento del prototipo, por lo que se desarrollo una metodología que facilitó la resolución de estos inconvenientes.

INTRODUCCIÓN

Para comprender mejor este trabajo de investigación es necesario conocer la misión y visión de la institución:

"La Superintendencia de Bancos y Seguros es un organismo técnico, con autonomía administrativa, económica y financiera, cuyo objetivo principal es vigilar y controlar con transparencia y eficacia a las instituciones del sistema financiero, de seguro privado y de seguridad social, a fin de que las actividades económicas y los servicios que presten se sujeten a la ley y atiendan al interés general. Asimismo busca contribuir a la profundización del mercado a través del acceso de los usuarios a los servicios financieros, como aporte al desarrollo económico y social del país. (Misión)

Ser un organismo técnico de reconocido prestigio nacional e internacional, independiente en su accionar, con recursos humanos competentes y suficiente apoyo tecnológico y financiero, que permitan regular y supervisar de manera transparente, eficaz y de acuerdo con las mejores prácticas internacionales, y de esta manera contribuir al desarrollo y consolidación de los mercados financiero, de seguro privado y de seguridad social. (Visión)"[1]

Para cumplir con estos lineamientos, se establece un marco de regulación, que se establece como un conjunto de reglas emanadas del órgano facultado por mandato legal, a ser aplicadas por las entidades sometidas a su control, que establecen las condiciones en las que desarrollarán sus actividades, en observancia de la regulación vigente.

De aquí se deriva la supervisión que se constituye en un conjunto de regulaciones (leyes, normas y demás disposiciones) y de mecanismos de verificación de su cumplimiento, que buscan preservar la solvencia y estabilidad de los sistemas controlados.

[1] *"**MISIÓN Y VISIÓN INSTITUCIONALES**", PLAN ESTRATÉGICO 2005-2008, Sección II, 2005.*

En conclusión, bajo cualquier orientación la supervisión de las entidades controladas, necesariamente deberá contar con disposiciones regulatorias y ciertas capacidades para poder vigilar que dichas leyes se cumplan.

El contenido de las regulaciones, su carácter preventivo o fiscalizador, su enfoque restrictivo o de apertura, entre otras particularidades, son las que definitiva, direccionarán la política supervisora que la SBS decidirá aplicar; y sobre ellas definir los mecanismos de control y supervisión de su cumplimiento.

En este contexto, lo que pretendo con esta investigación, es poner a disposición de la institución, una Infraestructura de Clave Pública (PKI) herramienta que permitirá brindar el marco legal y tecnológico apropiado para la realización de transacciones electrónicas en un entorno seguro, de modo de optimizar la recolección de información de las entidades controladas, la provisión de servicios en formato digital y el desarrollo de acciones de gobierno electrónico, asegurando la integridad, el no repudio, la confidencialidad, la auditabilidad y la autenticación de la información, de las entidades controladas y de la Superintendencia.

CAPITULO 1

PRINCIPIOS BÁSICOS DE LA CERTIFICACIÓN DIGITAL

1.1. Infraestructura de Clave Pública

Para entender los principios básicos relacionados con la certificación digital, es esencial conocer la estructura, servicios, elementos y demás características concernientes a una Infraestructura de Clave Pública, también conocida como Infraestructura de Firma Digital o PKI[2] por sus siglas en inglés.

El desarrollo tecnológico y el aumento en los servicios por Internet, han cambiado dramáticamente la forma en que las organizaciones y las personas se comunican y realizan transacciones de negocios tanto privados como públicos.

Una Infraestructura de Clave Pública le permite a una organización contar con un sistema de autenticación, controles de acceso, confidencialidad y no repudiabilidad para sus aplicaciones, usando tecnología avanzada, tales como firmas digitales, criptografía, certificados digitales, entre otros.

Este tipo de infraestructura se basa, en el cifrado RSA[3] o DSA[4] de llaves o claves públicas, siendo el algoritmo RSA el primero en patentarse por la empresa RSA Data Security Inc. y que junto a su filial certificadora Verisign, se constituyeron en una de las alianzas más importantes en el desarrollo e implementación de Infraestructuras de Claves Públicas, más adelante se profundizará en la situación actual y las características de los algoritmos asimétricos. (Diffie-Hellman[5], PGP[6])

1.1.1. Definición

Una Infraestructura de Clave Pública, puede definirse como *"un sistema de información compuesto de hardware, software, canales de comunicación, procedimientos y recursos humanos entrenados que provee un marco de seguridad y confianza a los documentos digitales y mensajes de datos*

---

[2] *PKI.- Public Key Infrastructure*
[3] *RSA Algoritmo de encriptación asimétricos de llaves públicas (Rivest, Shamir, Adleman), 1978*
[4] *DSA Digital Signature Algorithm – Algoritmo de Firmas Digitales*
[5] *Algoritmo de clave pública desarrollado por Diffie-Hellman 1976*
[6] *Pretty Good Privacy, algoritmo de clave pública desarrollado por OpenPGP, IETF RFC 2440*

mediante la realización de actividades vinculadas con la creación, administración, almacenamiento, distribución y revocación de certificados digitales de clave pública."[7]

Analizando esta definición se precisa que la adecuada combinación entre los productos de software, hardware, políticas, comunicaciones, procedimientos y recurso humano, determinará el nivel de seguridad con el que se podrán realizar las transacciones electrónicas a través de redes públicas o privadas; se menciona también a los certificados digitales, los cuales actúan como pasaportes electrónicos vinculando a un usuario de firma digital con su clave pública, los que se consideran como identificadores digitales.

Dentro de la cadena de seguridad que impone una *Infraestructura de Clave Pública* es substancial el papel de identificación de la persona, para ello, es necesario la creación de Autoridades Certificantes, que registren a las personas y emitan los así llamados Certificados (datos de identidad y clave pública de la persona, firmados digitalmente por la Autoridad Certificadora), garantizando la vinculación entre la persona real o institución y su clave pública.

La PKI también es considerada por algunos especialistas como una norma que trata de describir los procesos organizativos necesarios para la gestión de certificados digitales de claves públicas para el intercambio seguro de información, que permite firmar digitalmente un documento electrónico (un mail, el código de un programa, una transacción bancaria, unos análisis médicos, transacciones on-line, dinero digital, entre otros) o permite identificar a una persona o institución en Internet o permite acceder a un recinto virtual o servicio restringido o su vez todas ellas.

1.1.2. Misión

Su misión debe ser la de garantizar la acreditación, el no repudio, la integridad y la confidencialidad de los datos, así como también su auditabilidad.

1.1.3. Servicios

La implementación funcional de PKI permite como mínimo proporcionar los siguientes servicios:

[7] *Ley No.126-02 Sobre Comercio Electrónico, Documentos Y Firmas Digitales, Agenda Regulatoria del INDOTEL*

a. Servicios de Certificación .- Garantías de autenticidad, confidencialidad e integridad de los datos a través de una plataforma de certificación, gestión de usuarios, control de revocados, entre otros.
b. Servicios de certificación temporal y timbre o fechado digital[8].
c. Disponer de un conjunto heterogéneo y compatible de soluciones criptográficas.
d. Asesoramiento y apoyo en cuanto a soluciones disponibles ante problemas que surjan en la implementación de otros proyectos.

Estos servicios podrán variar según la naturaleza de la institución o empresa en la que se vaya a implementar, así como también de acuerdo a sus objetivos.

1.2. Mecanismos Básicos de Seguridad

1.2.1. Criptografía

Siempre se ha asociado a la Criptografía con algo secreto y misterioso utilizado por el espionaje en todas las guerras y, por otro lado, con una matemática indescifrable, compleja y no abordable para la mayoría de los mortales.

De hecho la Criptografía toma su denominación del griego y se puede traducir como "La manera de escribir raro" (Criptos, extraño; Graphos, escritura).

Las dos técnicas más básicas de cifrado en la criptografía clásica son la ***sustitución*** que supone el cambio de significado de los elementos básicos del mensaje las letras, los dígitos o los símbolos y la ***transposición*** que supone una reordenación de las mismas; la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas.

Si bien su origen tiene carácter militar, en la actualidad su interés ha desbordado ampliamente dicho campo, para introducirse en las áreas donde la información es valiosa, como la informática.

La criptografía comprende dos procesos bien definidos para la transformación de la información: (**Ver figura 1**)

[8] *Time-stamping .- servicio de fechado digital.*

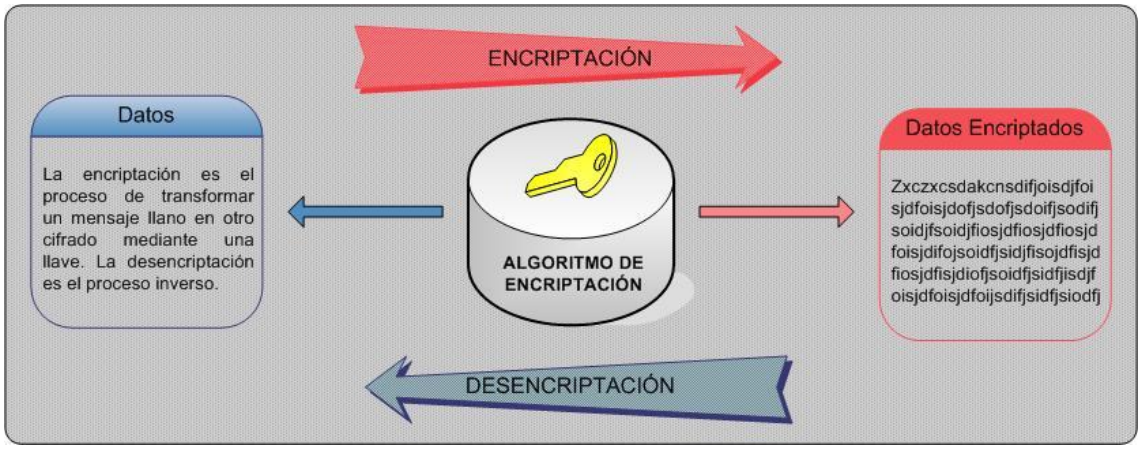

Figura 1. Procesos de la Criptografía
Elaborado por: el autor

1. Encriptación: Proceso mediante el cual un conjunto de datos se transforman en un conjunto cifrado de datos mediante una función de transformación y una llave de codificación. Transforma la información en una forma no legible asegurando la privacidad.
2. Desencriptación: Proceso inverso a la encriptación, en el cual el conjunto cifrado de datos se convierte en el texto original mediante una segunda función de transformación y una llave de desencriptación. La llave puede ser la misma para ambos procesos o distinta.

Todas estas tecnologías usan técnicas matemáticas sofisticadas. Por ejemplo, para mantener la seguridad dentro del Sistema de Nombres de Dominio (DNS dinámico)[9] se consideró la autentificación de usuarios por medio de un nombre (login) y contraseña (password). Los usuarios inicialmente se conectarían al servidor (DNS dinámico) y si el usuario teclea una combinación válida, podrían llevarse modificaciones dentro del servidor; de lo contrario, no se tendría acceso al mismo.

Esta forma de autentificación es una seguridad "débil" por las siguientes razones:

1. Privacidad: El nombre y contraseña del cliente pueden ser capturados por un intruso y leídos sin mayor problema.
2. Verificación: No hay ninguna garantía que el nombre y contraseña del cliente no hayan sido enviados por un impostor (hacerse pasar por un cliente).

[9] *DNS.- Base de datos jerárquica y distribuida que contiene asignaciones de nombres de dominio para varios tipos de datos, como direcciones IP.*

El principal problema con un simple nombre y contraseña de un cliente es el hecho de que no pueden ser verificados; por lo tanto, es necesario aplicar un mecanismo para identificar a todos los clientes que intenten conectarse al servidor (DNS dinámico) así como verificar que los clientes son realmente los que dicen ser y no sean impostores.

Se han implementado dos algoritmos criptográficos para llevar a cabo el mecanismo antes mencionado:

a. Llave simétrica o secreta.- Utiliza una misma llave para encriptar y desencriptar la información enviada a través de la red; pero el problema que se presenta es que tanto quien envía como quien recibe la información deben tener la misma llave asegurándose que nadie más pueda obtenerla porque si intercepta la información pudiera desencriptarla y leerla fácilmente. Supongamos que necesitamos enviar un mensaje entre dos lugares muy separados, y que éste es confidencial o secreto, por lo que se requiere que nadie lo lea. Para esto se deberá "encriptar o cifrar" el mensaje mediante un procedimiento matemático (algoritmo), que hará que el texto se deforme para que no sea descifrable por un tercero desconocido o no autorizado.

   Estos algoritmos necesitan una "contraseña" o "clave" para la encriptación, por lo que, si se ha encriptado el texto original con una clave, el destinatario necesitará la misma clave y el mismo algoritmo para que el mensaje pueda descifrarse y ser leído. Este proceso se llama encriptación simétrica.

   Ahora bien, el problema se suscita en la transferencia de esta contraseña o clave al destinatario del mensaje, por lo que se necesita un canal seguro, protegido contra la intercepción, sin lo cual la clave podría ser conocida por un tercero ajeno al proceso. Pero surge la paradoja que si ya se posee un canal seguro para comunicarse con el destinatario del mensaje, no se necesitaría la criptografía para comunicarse en forma segura.

La realidad es que existen pocos canales seguros ya que los servicios de información mundiales, las escuchas telefónicas y otros métodos de interceptación son moneda corriente en nuestros días y por lo cual habría que encontrarse personalmente, supuesto imposible si ambas partes se hallan a una distancia considerable y sobre todo si para cada comunicación segura en Internet habría que repetir estos encuentros.

Este tipo de algoritmo es aun muy utilizado debido a su rapidez.

La fortaleza de los algoritmos de llaves simétricas depende de los siguientes factores:

- Confidencialidad de la llave.
- Dificultad de adivinar la llave.
- Dificultad de forzar el algoritmo de encriptación.
- Ausencia de puertas traseras, es decir huecos de seguridad que permitan desencriptar el mensaje sin tener la llave.
- La posibilidad de desencriptar un mensaje si se conoce una parte de él (ataque de piedra roseta).

Lamentablemente es muy difícil probar la fortaleza criptográfica. Generalmente se prueba la debilidad de un algoritmo que a veces ya se encontraba difundido como seguro. La verdadera seguridad criptográfica está en publicar el algoritmo y esperar a que no se le encuentren errores Los ataques más comunes que reciben este tipo de sistemas son algunos de los siguientes:

- Ataque de búsqueda de llaves (fuerza bruta): Si el violador de códigos tiene la capacidad de reconocer el resultado de utilizar la llave correcta, entonces el método más simple de violar la encriptación es probar todas las llaves posibles. Casi todas fallarán pero al final alguna tendrá éxito.. La forma de protegernos contra este tipo de ataques es que el universo de llaves posibles sea suficientemente grande para evitar que se prueben todas. Por ejemplo. En Internet se utilizan, generalmente lla-

ves de 128 bits. Esto permite 2128 (3.4 x 1038) llaves posibles, un número suficientemente grande como para evitar que alguien se ponga probar de a una. Hasta con ayuda de procesadores que intenten violar el código se tomaría varios miles de años hasta descifrar el código.

- Criptoanálisis: La mayoría de los algoritmos de encriptación pueden ser vencidos mediante la combinación de matemáticas y poder de cómputo. Por lo que casi nunca es necesario, para violar un código, el intentar el método de la fuerza bruta. Un criptoanalista (persona que rompe códigos) puede descifrar el texto encriptado sin necesidad de tener la llave y sin saber el código de encriptación. Un tipo de criptoanálisis es el ataque de piedra roseta en el que el violador tiene parte del mensaje desencriptado y la misma parte encriptada; con este tipo de ataque el violador obtendrá primero el algoritmo de encriptación, el que luego puede utilizar para intentar inferir el algoritmo de desencriptación para así descifrar el mensaje.
- Ataques basados en el sistema: Esta forma de ataque se basa en buscar debilidades en el sistema que utiliza el algoritmo criptográfico sin atacar al algoritmo en sí. Un ejemplo es el caso de una violación en la seguridad de Netscape que utiliza una llave aleatoria14. Pero el generador de números aleatorios de Netscape no era un buen generador por lo que se podía alterar la semilla del generador y predecir el número aleatorio generado, pudiendo así adivinar la llave.

b. Llave asimétrica o pública.- La solución para resolver el problema presentado por la llave simétrica, surgió en un trabajo publicado en noviembre de 1976, bajo el título "Nuevas Direcciones en Criptografía" de los entonces jóvenes investigadores de la Universidad de Stanford, Whitfield Diffie y Martin Hellman, quienes desarrollaron una metodología de encriptación llamada encriptación asimétrica o pública.

Es un método de transmisión de información en donde el que recibe la información puede estar seguro de la identidad de quien la envió. La idea básica de este método es el uso de un par de llaves:

- Llave privada: Solamente su dueño la conoce y se usa para desencriptar la información enviada por otras personas.
- Llave pública: Esta se publica y se usa por cualquier persona para encriptar la información antes de enviarla a su destino (dueño).

El par de llaves se generan simultáneamente, usando algoritmos especiales en donde los mensajes que se encriptan con la llave pública de una persona puedan ser desencriptados solamente con la llave privada de esa misma persona y viceversa. Por lo tanto, para establecer una comunicación segura ya no es necesario compartir primeramente una llave privada.

Esta transmisión es segura en el sentido de que nadie más que reciba la información podrá leerla porque no sabe el valor de la llave privada.

Con la utilización del par de llaves los sujetos que desean intercambiar mensajes pueden intercambiarse la llave pública encriptadora de forma no segura y conservar la llave desencriptadora. Este principio es el mismo que se usa en las firmas digitales. El problema más grave de este sistema es que es muy lento, entre "*diez y cien veces más que el sistema de llaves simétricas"*[10].

Ha habido mucho menos desarrollo de algoritmos de llave pública que de llave simétrica ya que para crear un algoritmo de llave simétrica sólo hace falta idear una forma de hacer la revoltura de datos, de forma confiable y suficientemente intrincada como para que no sea fácil deducir el algoritmo de desencriptación.

---

[10] ***"TECNICAS DE PROTECCIÓN CONTRA PIRATERÍA EN DISCOS COMPACTOS",*** *Ing. Ana Azucena Evangelsta, Tesis de Maestría en Ciencias, Telemática, página 31*

En cambio, los algoritmos de llave pública se basan en la teoría numérica por lo que el desarrollo de un algoritmo nuevo implica encontrar un paradigma matemático de características especiales.

Los ataques más comunes que reciben este tipo de sistemas son los siguientes:

- Ataques de factorización: Intentan derivar la llave secreta a partir de la llave pública, de la que el atacante tiene una copia. Este ataque necesita resolver problemas matemáticos de alta dificultad como la factorización de números grandes.
- Ataques algorítmicos: Este tipo de ataque consiste en encontrar una falla o debilidad fundamental en el algoritmo en que se basa el problema matemático.

El problema con este tipo de algoritmos es que un defecto en los mismos no necesariamente tiene que ser publicado, lo cual no significa que no exista o no se conozca.

Existe un problema que reside en el hecho de que la llave pública no puede ser verificada. Cómo se que la llave pública realmente es suya y no una llave pública generada por algún impostor que desee interceptar sus mensajes. Este problema es más serio cuando es usado para verificar automáticamente la comunicación entre dos "hosts", tales como un cliente ("browser") y un servidor (DNS dinámico). Aquí es donde intervienen los certificados.

c. Criptosistemas híbridos público / privado: Este sistema se basa en una llave de sesión, que es una llave pública aleatoria que se utiliza para crear un sistema de llaves simétricas. Cada vez que se inicie un intercambio de datos, la llave aleatoria habrá cambiado y se generará una nueva llave simétrica. Este sistema es uno de los más utilizados ya que combina las ventajas de ambos sistemas.

d. Funciones de compendio de mensaje: Este tipo de encriptación genera un patrón de bits único para cada entrada específica. Son como huellas digitales para archivos.

1.2.2. Firma Digital

Con la invención de la criptografía de llaves públicas, Es posible otro proceso conocido como firma digital. Una firma digital es equivalente a una firma manual, la cual proporciona la prueba que el que firma es el autor original del mensaje (Autenticación). Si se desea firmar el mensaje que será enviado a un destinatario, el mensaje se cambia por medio de una función matemática (conocida como función hash) para lo cual hace un resumen del mensaje (código hash). Este resumen es único para cada mensaje y es equivalente a una huella digital. Luego este resumen o código hash se encripta con la llave privada y se adjunta la final de mensaje. Este código adjunto es conocido como firma digital. El destinatario puede verificar luego que el mensaje fue enviado por una persona que tiene una firma digital haciendo uso de la llave pública a través de una función hash similar. Si los dos códigos hash son similares entonces el que envió el correo firmado fue la persona correcta (no repudio) y no fue alterado (integridad). Todo esto suena complicado pero en la práctica todo lo que se tiene que hacer es dar un clic en un icono que hace referencia a la firma digital, en la pantalla del computador.

Función HASH

Junto a la criptografía asimétrica se utilizan en la firma digital las llamadas funciones hash o funciones resumen. Los mensajes que se intercambian pueden tener un gran tamaño, hecho éste que dificulta el proceso de cifrado. Por ello, no se cifra el mensaje entero sino un resumen del mismo obtenido aplicando al mensaje una función hash.

Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Para ello, el mensaje originario se divide en varias partes cada una de las cuales tendrá ese tamaño de 160 bits, y una vez dividido se combinan elementos tomados de cada una de las partes resultantes de la división para formar el mensaje-resumen o hash, que también tendrá una dimensión fija y

constante de 160 bits. Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

La firma digital funciona en documentos electrónicos como una firma manuscrita en un documento impreso. La firma es una parte de la información infalsificable que identifica a la persona que lo envió y puede demostrar que está de acuerdo con el documento en el que puso su firma. Actualmente, la firma digital brinda un más alto grado de seguridad que la firma manuscrita. El receptor del mensaje digital puede verificar que el mensaje ha sido originado por la persona cuya firma se encuentra añadida y que el mensaje no ha sido alterado (de forma maliciosa o accidental) desde que fuera firmado. Es por esto que las firmas digitales seguras no pueden repudiarse. El firmante del documento no puede alegar que la firma era falsa. En otras palabras, las firmas digitales permiten la autenticación de los mensajes, asegurándole al receptor la identidad del emisor y la integridad del mensaje.

Para una mejor comprensión de la utilización de una firma digital se plantearan algunos ejemplos:

Supongamos que un sujeto A, distribuye una llave pública a prueba de alteración. Como esta llave sólo sirve para comprobar si la llave privada que el sujeto A conserva es realmente la llave privada del sujeto A, sí alguien intercepta la llave pública no le serviría de nada, por lo tanto el sujeto A podría distribuir la llave pública por cualquier medio. (**Ver Figura 2**)

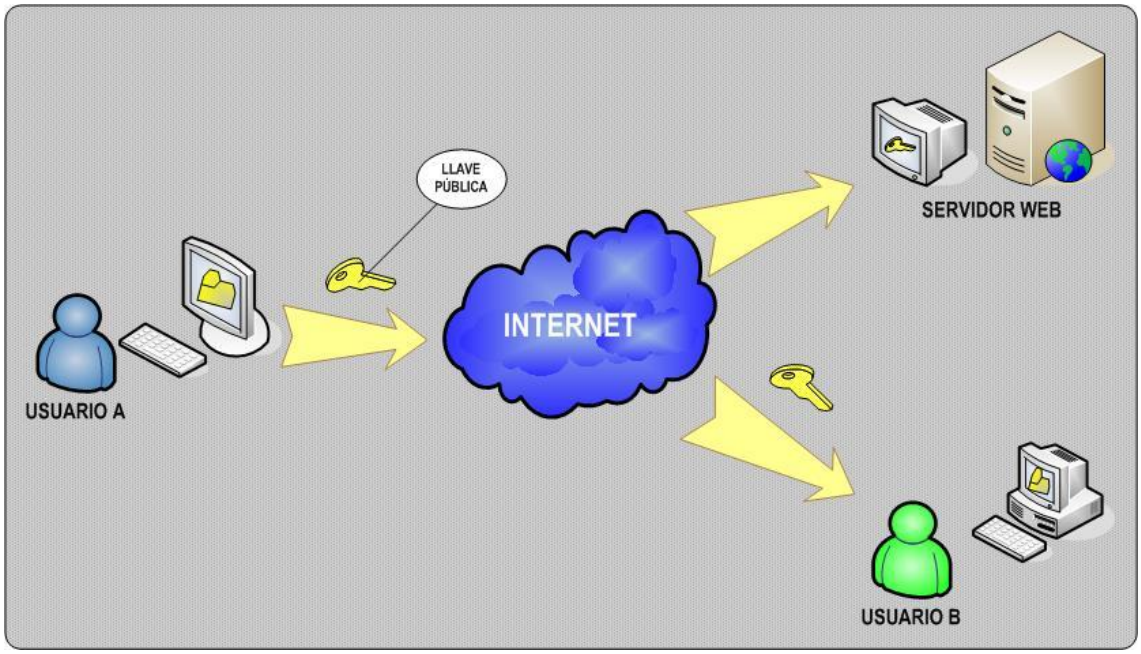

Figura 2. Distribución de la llave pública
Elaborado por: el autor

Supongamos ahora que un sujeto B, necesita corroborar que el sujeto A ha leído un documento X, para esto envía el documento X por mail al sujeto A, el sujeto A recibe el documento X lo lee y anexa su firma generada con la llave secreta. El sujeto A reenvía el documento firmado al sujeto B que mediante la llave pública corrobora la legitimidad de la firma. (**Ver Figura 3**)

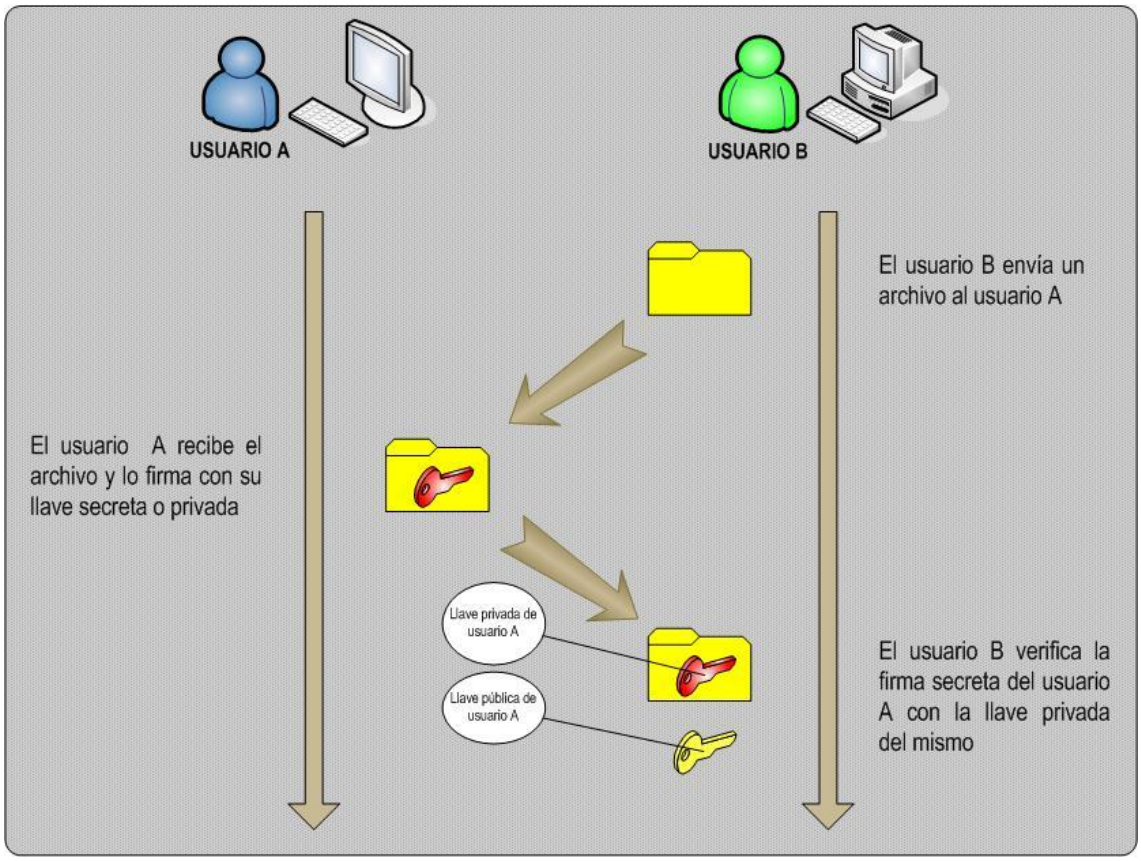

Figura 3. Uso de la Firma Digital para verificar la identidad
Elaborado por: el autor

Los siguientes son los medios físicos en los que soportan la tecnología de llave digital para realizar firmas.

- Llave encriptada almacenadas en disco duro: esta es la forma más sencilla de almacenar la llave, aunque vulnerable a usuarios de la computadora y a programas hostiles.
- Llave encriptada en medio removible: es un poco más seguro guardar la llave privada en un disquete, disco compacto u otro medio removible. Pero para utilizar la llave privada la computadora debe desencriptarla y copiar la memoria, por lo que aún sigue siendo vulnerable a programas hostiles.
- Llave almacenada en un dispositivo inteligente: estos dispositivos son una tarjeta con un microprocesador que almacena la llave privada transfiriéndola directamente sin cargarla en

memoria por lo que es inmune a un programa hostil que intente capturarlo. La desventaja de este tipo de dispositivo es su fragilidad y la posibilidad de ser robadas o extraviadas.

A continuación mencionaremos algunas desventajas que presenta utilizar una infraestructura de llaves públicas.

1. La mayor parte de las transacciones de comercio en Internet se basan en las tarjetas de crédito, sin utilizar la tecnología de firmas digitales.
2. Las firmas digitales facilitan la prueba de identidad pero no la aseguran, todo lo que comprueban es que una persona tiene acceso a una llave privada específica que complemente a una llave pública específica que está firmada por una autoridad certificadora específica.
3. Al no existir estándares que regulen a las autoridades certificadoras no es posible evaluar la confiabilidad de las mismas, no es posible saber si la autoridad certificadora quebranta sus propias reglas emitiendo documentos fraudulentos. También es difícil comparar una autoridad certificadora con otra y más difícil aún hacerlo de forma automática.
4. El certificado no posee los datos suficientes como para identificar de forma legal a su poseedor.
5. La tecnología de firma digital no permite la divulgación selectiva de datos

Generalmente, una clave expira tras un período de tiempo de aproximadamente un año. Un documento firmado con una firma caducada no debe ser aceptado. No obstante, existen varios supuestos en los que un documento firmado es considerado legalmente válido por un período superior a dos años; por ejemplo los alquileres a largo plazo y los contratos. Al realizar un contrato con el servico de "sello de tiempo digital", la firma tiene validez incluso después del vencimiento de la clave. Si todas las partes que intervinieron en el contrato guardan una copia de el sello de tiempo, pueden verificar que el contrato se firmó con claves válidas. De ahí que el sello de tiempo pueda garantizar

la validez de la operación posteriormente el periodo de validez de la clave. Todo documento firmado digitalmente puede tener sello de tiempo.

1.2.3. Certificados Digitales

Un certificado digital es un equivalente electrónico del pasaporte. Este contiene información que puede ser usada para verificar la identidad del dueño. Una parte principal del contenido de la información del certificado digital es la llave pública del usuario. Una llave pública puede ser usada para poder realizar una comunicación encriptada entre dos usuarios que tengan certificados digitales.

Los Certificados electrónicos son documentos digitales que sirven para asegurar la veracidad de la Clave Pública perteneciente al propietario del certificado ó de la entidad, con la que se firman digitalmente documentos que puedan proporcionar la más absoluta garantía de seguridad respecto a cuatro elementos fundamentales:

- La autentificación del usuario/entidad (es quien asegura ser).
- La confidencialidad del mensaje (que sólo lo podrá leer el destinatario).
- La integridad del documento (nadie los ha modificado).
- El no repudio (el mensaje una vez aceptado, no puede ser rechazado por el emisor).

Es, por tanto, muy importante estar realmente seguros de que la Clave Pública que manejamos para verificar una firma o cifrar un texto, pertenece realmente a quien creemos que pertenece.

Sería nefasto cifrar un texto confidencial con una Clave Pública de alguien, que no es nuestro intencionado receptor. Si lo hiciéramos la persona a quién pertenece la clave pública con la que lo hemos cifrado, podría conocer perfectamente el contenido de este, si tuviera acceso al texto cifrado. De la misma forma, si manejáramos una clave pública de alguien que se hace pasar por otro, sin poderlo detectar, podríamos tomar una firma fraudulenta por válida y creer que ha sido realizada por alguien que realmente no es quien dice ser.

Otro dato a tener en cuenta, es que un certificado no puede falsificarse ya que van firmados por la Autoridad de Certificación. Si algún dato se modificase la firma no correspondería con el resumen (hash) que se obtendría de los datos modificados.

Por tanto al utilizarlo, el software que los gestiona daría un menaje de invalidez. Un certificado electrónico contiene una clave pública, y una firma digital. Para su correcto funcionamiento, los certificados contienen además la siguiente información:

- Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.
- Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.
- Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.
- Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.
- Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.

Los navegadores actuales gestionan y almacenan las Claves Públicas de los certificados que permiten al emisor de mensajes firmarlos y encriptarlos utilizando las claves públicas de los destinatarios. Para estar complementar la seguridad en cualquier transacción es necesario utilizar, otro tipo de herramientas y protocolos.

Además de servir como mecanismo confiable y seguro de identificación en la red, su certificado de identidad digital le permite disfrutar de otra serie de beneficios: puede enviar y recibir información confidencial, asegurándose que sólo el remitente pueda leer el mensaje enviado; puede acceder a

sitios Web de manera segura con su identidad digital, sin tener que usar el peligroso mecanismo de passwords; puede firmar digitalmente documentos, garantizando la integridad del
contenido y autoría del documento; y todas aquellas aplicaciones en que se necesiten mecanismos seguros para garantizar la identidad de las partes y confidencialidad e integridad de la información intercambiada, como comercio electrónico, declaración de impuestos, pagos provisionales, uso en la banca, etc.

La utilización de los Certificados Digitales conjuntamente con los sistemas de encriptación, así como también estrictos procedimientos de verificación de identidades, proporciona una eficaz alternativa de solución en cuanto a la seguridad, por cuanto es posible asegurar que todas las partes involucradas en una transacción son quienes dicen ser y que la información se transmite con integridad, es importante mencionar y considerar que ninguna herramienta o infraestructura asegura el 100% de confiabilidad y seguridad.

Las tiendas virtuales, la banca electrónica y otros servicios electrónicos se están convirtiendo en lugares de encuentro que ofrecen al cliente un servicio flexible y personalizado 24 horas al día, directamente en su casa. No obstante, la preocupación acerca de la privacidad y la seguridad puede limitar el aprovechamiento de estas nuevas formas de intercambio. Por sí sólo, el sistema de encriptación no es suficiente, porque no ofrece prueba alguna sobre la identidad del remitente que envió la información encriptada. Sin ninguna garantía especial, se arriesga a que un tercero se haga pasar por usted en línea. Los Certificados Digitales solucionan este problema, ofreciendo un medio electrónico para verificar la identidad de una persona. Al utilizar los Certificados Digitales en conjunto con el sistema de encriptación, se proporciona una solución más completa para la seguridad, asegurando la identidad de todas las partes involucradas en una transacción.

Igualmente, un servidor seguro debe tener un Certificado Digital para asegurar que el servidor está administrado por la organización que dice poseerlo y para asegurar que el contenido que ofrece es auténtico.

Cuando usted recibe mensajes firmados digitalmente puede verificar que el firmante del mensaje es quien dice ser y que no se está produciendo una suplantación, siempre y cuando en la practica, durante el proceso de asignación de los certificados se haya constato y verificado la identidad del individuo, así como también, información que permita disminuir el riesgo de suplantación. Los navegadores de Internet reconocen a muchas de estas autoridades certificadoras automáticamente y permiten agregar manualmente a las que no reconocen.

El "ciclo de vida" de un certificado comprende la emisión, renovación y revocación, siendo esta última ocasionada si la llave privada del tenedor ha sido violada, si la persona ha dado datos incorrectos o si hay copias falsas de ésa llave, entonces el certificado puede ser revocado. Las llaves revocadas que aún no están vencidas son colocadas en una Lista de Revocación de Certificados (CRL), estas listas tienden a crecer con rapidez pero su actualización es lenta.

A continuación, se muestra dos certificados uno emitido por VeriSing una Autoridad Certificadora reconocida a nivel internacional y un certificado emitido por la Superintendencia de Bancos y Seguros. (**Ver Figura 4**)

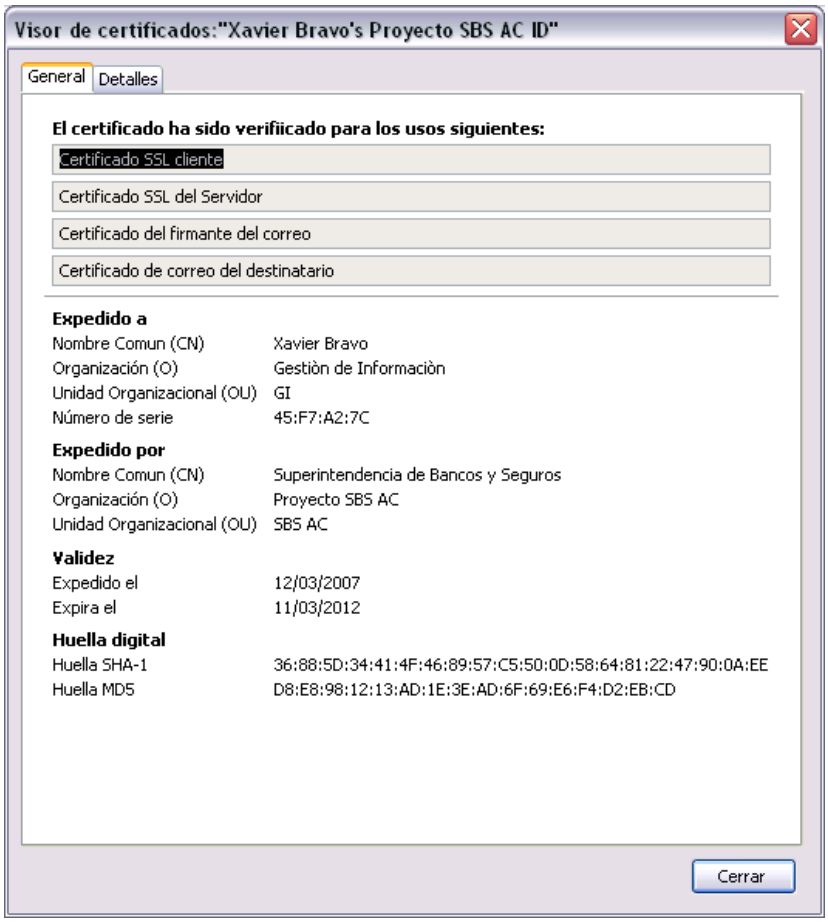

Figura 4. Certificado válido y emitido por la Autoridad Certificadora SBS AC de la Superintendencia de Bancos y Seguros
Elaborado por: el autor

Tipos de certificados

A continuación veremos los distintos tipos de certificados disponibles hoy en día, dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras han dividido los certificados en varios tipos. Del tipo de certificado a emitir van a depender las medidas de comprobación de los datos y el precio del mismo.

Los certificados, según las comprobaciones de los datos que se realizan, se dividen en cuatro clases:

- Certificados de Clase 1: corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.
- Certificados de Clase 2: en los que la Autoridad Certificadora comprueba además el DNI o permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento.
- Certificados de Clase 3: en la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante un servicio del tipo Equifax o Duns&Bradstreet.
- Certificados de Clase 4: que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

Desde el punto de vista de la finalidad, los certificados electrónicos se dividen en:

1. Certificados SSL para cliente: usados para identificar y autentificar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.
2. Certificados SSL para servidor: usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.
3. Certificados S/MIME: usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autentificación, Integridad y No Repudio. También se puede cifrar el mensaje con la clave pública del destinatario, lo que proporciona Confidencialidad al envío.

4. Certificados para la firma de código: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc). Cuando un código de éste tipo puede resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.
5. Certificados para AC: que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.

Toda persona o entidad que desee obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor), más costará el certificado. La vigencia de cada uno de ellos será determinada por la Autoridad Certificadora emisora, que deberá considerar las necesidades del negocio.

A continuación se presentan ejemplos de certificados digitales:

- Certificado digital clase 3 caducado (no válido) emitido por VeriSing (**Ver Figura 5**).

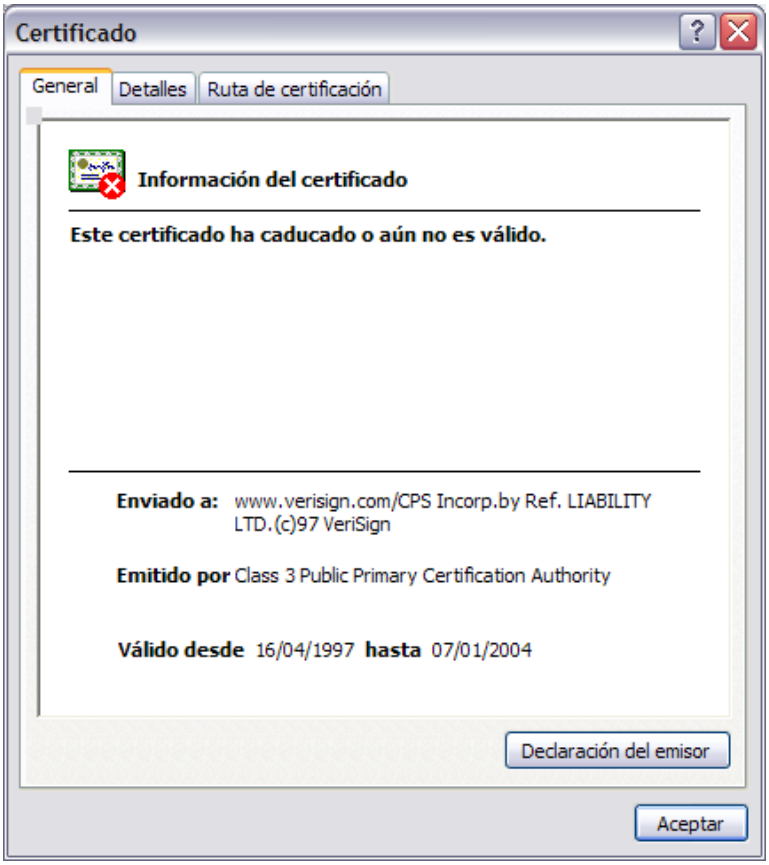

Figura 5. Mensaje de advertencia cuando un certificado ha caducado o aún no ha entrado en vigencia
Elaborado por: el autor

1.2.3.1. Certificación cruzada

También conocido como subordinación cualificada, la Certificación Cruzada permite colocar restricciones en las autoridades de certificación (CAs) subordinadas y en los certificados expedidos por éstas y crea confianza entre las CAs de distintas jerarquías. El soporte de Certificación Cruzada mejora la eficiencia de la administración de la clave de infraestructura pública. La certificación cruzada es el acto de compartir niveles de confianza entre dos o mas organizaciones o autoridades de certificación. Esto quiere decir que 2 o mas CAs intercambian información de llaves criptográficas para la confianza entre sus respectivas llaves, esto permite definir relaciones de confianza entre dominios gestionados por diferentes Autoridades de Certificación. Estas relaciones de confianza pueden ser jerárquicas, de modo que una CA puede permitir CAs subordinadas que expandan la infraestructura, o también pueden establecerse relaciones entre CAs raíces, que son totalmente independientes; estas relaciones de confianza se denominan certificación cruzada “peer-to-peer”.

1.2.3.2. Time stamping

El servicio de Sello de Tiempo Digital (DTS, Digital Time-Stamping) emite fechas ciertas relacionando una fecha y hora con un documento digital en un sistema criptográfico robusto. El sello de tiempo digital puede utilizarse posteriormente para verificar que el documento electrónico fue creado o modificado el día que figura en el sello de tiempo. Por ejemplo, un físico puede escribir una brillante idea en un procesador de texto y sellar con sello de tiempo dicho documento. Ambos, conjuntamente, pueden probar con posteridad que el científico se merece el Premio Nobel, aún cuando un investigador rival lo haya publicado antes.

Supongamos que Alicia desea firmar un documento con sello de tiempo. Alicia utiliza una función numérica segura para procesar el documento y enviarlo al DTS, que le devuelve un sello de tiempo digital, es decir el mensaje numérico y una fecha y una hora. Como el mensaje numérico no revela ninguna información sobre el contenido del documento, el servicio de sello de tiempo digital (DTS) no puede indagar en el documento. Por eso Alicia puede presentar el documento y el sello de tiempo en forma conjunta para probar la fecha en que se realizó el documento. Un verificador procesa el mensaje numérico del documento, se asegura que coincida con el sello de tiempo y luego verifica la firma del servicio de sello de tiempo digital (DTS) sobre el sello de tiempo. Para ser creíble, el sello de tiempo debe ser infalsificable. Considere los requisitos que debe cumplir el servicio de sello de tiempo digital:

1. El servicio de sello de tiempo digital (DTS) debe tener una clave larga para que el sello de tiempo sea fiable durante décadas.
2. La clave privada del DTS debe guardarse con total seguridad, en un hardware cerrado a posibles modificaciones.

3. La fecha y hora deben provenir de un reloj, dentro de un hardware a prueba de modificaciones, que no puede ser reseteado y que guardará la fecha exacta durante años e incluso décadas.
4. Debe ser imposible crear un sello de tiempo sin utilizar el reloj que se encuentra dentro del hardware a prueba de modificaciones.

El servicio de sello de tiempo digital (DTS) combina esencialmente los valores numéricos de los documentos en una estructura de datos denominada árboles binarios, cuyos valores de "raíz" se publican periódicamente. El sello de tiempo consiste en un par de valores numéricos que permiten a un verificador procesar nuevamente la raíz del árbol. Como las funciones numéricas poseen un solo sentido, no puede falsificarse la validación de los valores numéricos. La fecha relacionada con el documento por el sello de tiempo, es la fecha de publicación de dicho documento.

El uso del servicio de sello de tiempo digital (DTS) es extremadamente importante o esencial, para mantener la validez del documento durante años. Pongamos por caso un contrato de alquiler por tiempo de 20 años. Las claves públicas que se utilizaron para firmar el contrato de alquiler expiran poco después de la firma. Una solución consistiría en firmar el acuerdo cada dos años con nuevas claves, pero esto requeriría que la sociedad dure varios años tras la firma original. En caso que una de las partes no esté satisfecha con el contrato, puede rechazar la sociedad. La solución es registrar el contrato de alquiler con los servicios de sello de tiempo digital (DTS) en la fecha de la firma original. Luego, ambas partes recibirán una copia del sello de tiempo, que puede ser utilizada varios años después para exigir el cumplimiento del contrato original.

En el futuro, el servicio de sello de tiempo digital (DTS) será utilizado para multitud de actividades, desde los contratos cuya vigencia alcance un largo periodo de tiempo hasta diarios personales y cartas. Actualmente, si un historiador descubre una carta perdida de Cervantes, su autenticación se realiza a través de medios físicos. Pero un descubrimiento parecido puede ocurrir dentro de 100

años en los archivos informáticos de un autor actual; y el sello de tiempo puede ser la única manera de dar validez al descubrimiento.

1.3. Elementos de una Infraestructura de Clave Pública

La siguiente figura, se muestra en forma macro los elementos mínimos requeridos en una Infraestructura de Clave Pública y que serán estudiados en este documento. (**Ver Figura 6**)

Figura 6. Visión macro de una PKI
Elaborado por: el autor

Para poder realizar un adecuado estudio, es preciso identificar claramente los conceptos y estándares utilizados en la implementación de una PKI, su uso e importancia.

1.3.1. Autoridad Certificadora

También llamadas Autoridades Certificadoras (AC) son entidades de confianza quienes tienen la responsabilidad principal de certificar la autenticidad de los usuarios.

Una autoridad certificadora es aquella que presta servicios de emisión, revocación u otros servicios inherentes a la certificación digital, pudiendo también asumir las funciones de una autoridad de Registro (AR) o verificación.

Es decir una AC es la tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actúa como una especie de notario electrónico que extiende un certificado de cla-

ves el cual esta firmado con su propia clave, para así garantizar la autenticidad de dicha información.

La AC, es quien firma digitalmente los certificados, asegurando su integridad y certificando la relación existente entre la Clave Pública contenida y la identidad del propietario. La firma de la AC es la que garantiza la validez de los certificados.

La confianza de los usuarios la Autoridad de Certificación es fundamental para el buen funcionamiento del servicio. El entorno de seguridad (control de acceso, cifrado, etc.) de la AC ha de ser muy fuerte, en particular en lo que respecta a la protección de la Clave Privada que utiliza para firmar sus emisiones. Si este secreto se viera comprometido, toda la infraestructura de Clave Pública (PKI) se vendría abajo.

Las autoridades de certificación realizan las siguientes tareas:

- Emisión de los certificados de usuarios registrados y validados por la Autoridad de Registro (AR).
- Revocación de los certificados que ya no sean válidos (CRL[11]). Un certificado puede ser revocado por que los datos han dejado de ser válidos, la clave privada ha sido comprometida o el certificado ha dejado de tener validez dentro del contexto para el que había sido emitido.
- Renovación de certificados.
- Publicar certificados en el directorio repositorio de certificados.
- Definir tipos de certificados y su aplicación según su jerarquía.
- Definir Políticas y Procedimientos necesarios para la Certificación.
- Definir las funciones de la o las autoridades de registro si las hubiera.

La emisión de certificados y la creación de claves privadas para firmas digitales acostumbran a depender de una pluralidad de entidades que están jerarquizadas de una manera que las de nivel

[11] *CRL .- Lista de certificados revocados* o, *en inglés, Certificate Revocation List*

inferior obtienen su capacidad de certificación de otras entidades de nivel superior. Finalmente, en la cúspide de la pirámide suele hallarse una autoridad certificadora, que puede pertenecer al Estado. (**Ver figura 7)**

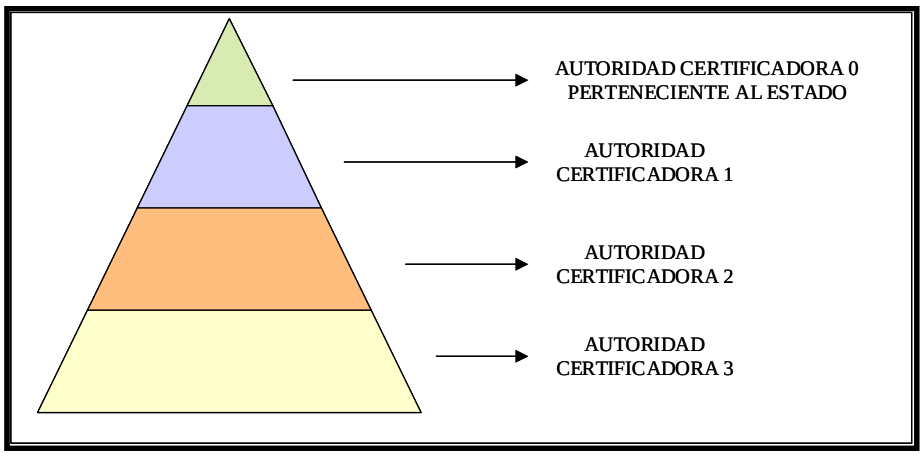

Figura 7. Autoridades Certificadoras que certifiquen a otras.
Elaborado por: el autor

Los certificados indican la autoridad certificadora que lo ha emitido, identifican al firmante del mensaje o transacción, contienen la clave pública del firmante, y contienen a su vez la firma digital de la autoridad certificadora que lo ha emitido.

De esta manera, las partes que intervienen en una transacción aportan como credencial los certificados de su correspondiente entidad certificadora. Para llegar a ser una entidad certificadora deberá mediar una solicitud a una autoridad certificadora de nivel superior, que podrá denegar la licencia si el solicitante no ofrece la fiabilidad o los conocimientos necesarios, ni cumple los requisitos establecidos en la ley.

Existen varias Autoridades Certificadoras, que tengan la facultad de certificar o verificar la identidad de otra Autoridad Certificadora y así sucesivamente; pero habrá un punto en que una Autoridad no tendrá quién la certifique, en este caso, el certificado es firmado por uno mismo ("self-signed"'), por lo tanto, la Autoridad Certificadora es verificada o confiada por ella misma (Generalmente la última Autoridad Certificadora es el Estado por medio de alguna Institución).

Las Autoridades Certificadoras (o notarios electrónicos) deben ser entes fiables y ampliamente reconocidos que firman las claves públicas de las personas, certificando con su propia firma la identidad del usuario. Por lo tanto, si se desea establecer una Autoridad Certificadora, éstas deben tomar extremadas precauciones para evitar que sus claves caigan en manos de intrusos, lo cual comprometería todo el sistema. Para ello tendrá que utilizar claves largas y dispositivos especiales para su almacenamiento. Además, cuando emiten un certificado, deben estar seguros de que lo hacen a la persona adecuada. No podemos olvidar que la Autoridad Certificadora es la responsable, en última instancia, de todo el proceso, con una serie de responsabilidades legales y que basa su "negocio" en la credibilidad que inspire en sus potenciales clientes. Una Autoridad Certificadora con autentificaciones erróneas no tendrá más remedio que cerrar ya que los usuarios no considerarán sus certificados de la suficiente "calidad".

Varias compañías se han establecido como Autoridades Certificadoras. Entre las cuales destacan:

- VeriSign, Inc. [http://www.verisign.com]
- Thawte Certification. [http://www.thawte.com]
- Xcert Sentry CA. [http://www.xcert.com]
- Entrust. [http://www.entrust.net]
- Cybertrust. [http://www.baltimore.com]

1.3.2. Autoridad de Registro

La Autoridad de Registro (AR) es la entidad encargada de identificar de manera inequívoca a los usuarios que solicitan un certificado a la Autoridad de Certificación (AC), así como de gestionar los certificados.

Las autoridades de registro realizan las siguientes tareas:

- Validar solicitudes de certificado en base a determinados procedimientos de identificación, apropiados a los niveles de seguridad que ofrece cada categoría de certificado (políticas de seguridad).
- Mandar las peticiones de generación de certificados a la Autoridad de Certificación (CA), para que esta los firme con su clave privada.
- Recibir los certificados solicitados a la Autoridad de Certificación (CA).
- Entregar físicamente los certificados a los solicitantes, por cualquier medio (e-mail, disquete)
- Informar a los usuarios de la necesidad de la renovación de su certificado.
- Petición de revocación de un certificado (también puede solicitarlo el propio usuario).

En toda PKI deben establecerse los mecanismos para que los usuarios soliciten su propio certificado, de tal forma que se asegure la identidad de dicho usuario. A este procedimiento se le denomina "Proceso de Registro" y se realiza a través de la denominada "Autoridad de Registro".

Existen dos tipos principales de registro:

- Registro Clásico.- El solicitante acude en persona a una "Oficina de Registro", donde, tras acreditar su identidad, se le proporciona de forma segura su clave privada y su certificado.
- Registro Remoto.- El usuario, a través de Internet, realiza una solicitud de certificado. Para esto empleará un software (p.e. un navegador, Lotus/Notes) que generará el par de claves y enviará su clave pública a la Autoridad de Registro para que sea firmada por la Autoridad Certificadora y le sea devuelto su certificado.

La validez de la Firma Digital estará condicionada por la calidad del proceso de registro, siendo obligatorio para asegurar la validez legal de la firma, algún tipo de registro "Cara a Cara", ya que es el único que asegura la identidad del solicitante. Por otra parte, la validez de la firma digital también estará condicionada a la firma manuscrita de un "contrato" por el que el solicitante acepta su certificado y las condiciones de uso del mismo.

La Autoridad de Registro se compondrá de una serie de elementos tecnológicos (hardware y software específico) y unos medios humanos (los Operadores de Registro). Es el punto de comunicación entre los usuarios de la PKI y la Autoridad Certificadora.

1.3.3. Políticas de Certificación

Deben diseñarse una serie de políticas y procedimientos operativos, que rigen el funcionamiento de la PKI y establecen los compromisos entre la Autoridad Certificadora y los Usuarios Finales.

Estos documentos tendrán un carácter tanto técnico como legal. Dentro de una PKI, las Autoridades de Certificación y Registro tienen mucha importancia y por ello, la seguridad toma un cariz de máxima importancia. Si por cualquier motivo, se compromete la clave privada de alguno de estos sistemas, la PKI utilizada no tendrá ninguna garantía de validez.

Por ello, una solución PKI debe garantizar:

- El secreto de las claves privadas de la Autoridad de Certificación (AC) y la Autoridad de Registro (AR), que se almacenarán cada una en un módulo de seguridad a prueba de manipulaciones.
- El acceso a la AR y a la AC debe realizarse previa autenticación tanto de usuarios como de administradores, utilizando cualquier mecanismo seguro como pueden ser las tarjetas inteligentes.
- La existencia de un operador o administrador de AR que apruebe las distintas peticiones de certificación destinadas a la AC.
- La integridad y confidencialidad de todas las peticiones de certificación que se cursen dentro del sistema, para evitar la generación de posibles "peticiones intrusas" de terceras entidades.

Las políticas de certificación establecen y definen la dirección que debería seguir la organización respecto de la seguridad de su información considerando también los procesos y principios establecidos para el uso de medios criptográficos. También incluye documentos de cómo la organización

deberá manejar sus claves a fin de establecer el nivel de control deseado de acuerdo a los riesgos existentes. Típicamente, todos estos aspectos son agrupados en lo que es conocido como Certification Practice Statements – CPS – Este documento es donde se detallan los procedimientos operacionales, como son el funcionamiento de la autoridad certificadora, las actividades de administración de los certificados, las características de los certificados, etc.

La finalidad de este documento es detallar las políticas y prácticas de emisión y gestión de certificados digitales por parte de una Autoridad Certificadora (AC), además, se incluyen las políticas y prácticas de las Autoridades de Registro acreditadas por esta AC.

Para conformar este sistema se requiere de una serie de componentes que procedemos a detallar a continuación:

En el contenido de este manual se debe considerar los siguientes puntos importantes:

- Usuarios Informados,
- Ambiente de Operación Seguro,
- Responsabilidad bien definida,
- Operaciones bien efectuadas,
- Autenticación correcta de identidad.

1.3.4. Repositorio de Certificados o Directorios

Los repositorios de Certificados o Directorios son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados.

En una lista de revocación de certificados se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecido dentro del mismo certificado, más con-

cretamente se almacenan los números de serie de los certificados que han sido revocados o que ya no son válidos y en los que no debe confiar ningún sistema de usuario, este generalmente es un archivo de texto encriptado que se encuentra dentro de las carpetas de configuración del CA.

Cuando una autoridad de certificación emite un certificado digital, lo hace con un periodo máximo de validez que oscila entre tres y cinco años. El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Disminuyendo el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital. Cabe anotar que entre más corto sea este periodo de validez más seguro será el certificado, pero la carga operativa aumentará.

Sin embargo, existen otras situaciones que pueden invalidar el certificado digital aún cuando no ha caducado, de manera inesperada:

- El usuario del certificado cree que su clave privada ha sido robada.
- Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica.
- El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.
- Una orden judicial, etc.

He aquí la importancia de que las herramientas cuenten con algún mecanismo para comprobar la validez de un certificado antes de su caducidad. Las CRL son uno de estos mecanismos.

Profundizando un poco más en el tema, una CRL es una lista de números de serie de certificados digitales revocados por una autoridad de certificación concreta. Dicha lista está firmada digitalmente por la propia autoridad de certificación.

Cuando un tercero desea comprobar la validez de un certificado debe descargar una CRL actualizada desde los servidores de la misma autoridad de certificación que emitió el certificado en cuestión. A continuación comprueba la autenticidad de la lista gracias a la firma digital de la autoridad de certi-

ficación. Después debe comprobar que el número de serie del certificado cuestionado está en la lista. En caso afirmativo, no se debe aceptar el certificado como válido.

Estrictamente hablando, no es necesario descargar una CRL cada vez que se verifica un certificado. Solamente es necesario cuando no se dispone de la CRL de una entidad de certificación concreta, y cuando dicha lista tiene una cierta antigüedad que aconseja su renovación.

La única ventaja de las CRL es que se pueden consultar sin necesidad de una conexión de datos permanente con cada autoridad de certificación. Basta establecer dicha conexión con cierta periodicidad para descargar las CRL actualizadas.

Sin embargo, las desventajas de las CRL son varias:

- Existe el peligro de que un certificado haya sido revocado, pero no aparezca en la CRL del tercero que comprueba su validez. Esto se debe a que la CRL utilizada podría no estar actualizada.
- Si existe responsabilidad legal por el uso de un certificado revocado, no hay forma de demostrar quién es el culpable: el tercero por no comprobar la validez, o la autoridad de certificación por no incluirlo en la CRL a tiempo.
- Las CRL solamente crecen en tamaño, resultando ineficientes para su tratamiento directo.

Además es muy importante realizar un análisis profundo y exhaustivo de las implicaciones que pueden producirse según los esquemas o arquitecturas utilizadas en los casos prácticos.

Generalmente, las aplicaciones comerciales proveen de un software que permite la verificación de las CRL's, otras en cambio utilizan dispositivos de hardware previamente configurados para realizar una verificación evitando la participación del usuario, cualquiera de las dos formas anotadas anteriormente tendrían sus desventajas en cuanto a la disponibilidad de la información (actualización) ya que lo ideal sería que estás verificaciones se las realicen en línea.

El protocolo usado con mayor frecuencia para publicar los CRL's es el Protocolo de Acceso Ligero a Directorio, mejor conocido como LDAP, está basado en el estándar X.500, pero significativamente

más simple y adecuado de mejor manera para satisfacer las necesidades del usuario. A diferencia de X.500 LDAP soporta TCP/IP, que es necesario para el acceso a Internet.

1.3.5. Seguridades y Estándares Técnicos

A continución se presentan una serie de estándares definidos por algunas de las siguientes organizaciones:

1. Estándares internacionales dictados por la Internet Engineering Task Force (IETF)
2. Unión Internacional de Telecomunicaciones (UIT)
3. Las Request For Comments (RFC) que son un conjunto de notas técnicas y organizativas donde se describen los estándares o recomendaciones de Internet

- **Seguridad Criptográfica**
  - Requerimientos de seguridad para módulos criptográficos, para la publicación de estándares del procesamiento de información de las entidades públicas (tomando como referencia el FIPS 140-1 del gobierno de los Estados Unidos).
  - Realizar una evaluación para la garantía criptográfica y los respectivos programas de evaluación.
- **Estándares de Algoritmos Criptográficos**

Algoritmos Simétricos:

- **DES** (Data encryption Standar), 64 bits, fue aprobado como estándar federal en noviembre de 1976, y publicado el 15 de enero de 1977 como FIPS PUB 46, autorizado para el uso no clasificado de datos. Fue posteriormente confirmado como estándar en 1983, 1988 (revisado como FIPS-46-1), 1993 (FIPS-46-2), y de nuevo en 1998 (FIPS-46-3), El 26 de mayo de 2002, DES fue finalmente reemplazado por AES (Advanced Encryption Standard), tras una competición pública[12]. DES continúa siendo ampliamente utilizado.

[12] *http://es.wikipedia.org/wiki/Data_Encryption_Standard*

- **3DES** (Triple Data encryption Estándar) se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES, fue desarrollado por IBM en 1978.
- Algunos de los algoritmos para sustituir a DES fueron: **CAST-256** de Entrust Technologies, Inc., **CRYPTON** de Future Systems, Inc., **DEAL** de Richard Outerbridge, Lars Knudsen, **DFC de CNRS** – Centre National pour la Recherche Scientifique – Ecole Normale Superieure, **E2 de NTT** – Nippon Telegraph and Telephone Corporation, **FROG** de TecApro International, S.A., **HPC** de Rich Schroeppel, **LOKI97** de Lawrie Brown, Josef Pieprzyk, Jennifer Seberry, **MAGENTA** de Deutsche Telekom AG, **MARS** de IBM, **RC6** de RSA Laboratories, **RIJNDAEL de John Daemen, Vincent Rijmen**[13], **SAFER+** de Cylink Corporation, **SERPENT** de Ross Anderson, Eli Biham, Lars Knudsen, **TWOFISH** de Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Algoritmos Asimétricos:

- El sistema criptográfico con clave pública 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.

Algoritmos de Resumen (HASH):

- MD5 es un de algoritmo de reducción criptográfico diseñado por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Masachusets).
- SHA-1 es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).

En la actualidad se conoce que, en ambos sistemas se han descubierto colisiones o han sido rotos por algunos investigadores.[14]

Algoritmos de firma digital:

---

[13] El algoritmo Rijndael ganó la competición pública para reemplazar al algoritmo DES y en Noviembre de 2001 se publicó FIPS 197 donde se asumía oficialmente.

[14] http://en.epochtimes.com/news/7-1-11/50336.html, http://www.schneier.com/blog/archives/2005/02/sha1_broken.html

- DSA (Digital Signature Algorithm, en español Algoritmo de Firma digital) Es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital(DSS), especificado en el FIPS 186 . DSA se hizo público el 30 de agosto de 1991, este algoritmo como su nombre lo indica, sirve para firmar y para cifrar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que RSA.

❖ **Protocolos de Comunicaciones y formatos de datos**

- RFC 1777 LDAP (Protocolo de acceso ligero a directorios)
- ISO/IEC 8824 y 8825
- Especificación de mensajes S/MIME : PKCS Servicios de seguridad para formatos MIME.
- PEM (Privacidad en el correo electrónico)
- MSP (protocolo de seguridad de mensajes)
- Unidad de protección independiente de los datos (IDUP)
- GSS API, RFC 1508
- Protocolo para verificación del estado de un certificado en línea (OCSP[15])
- SSH (Secure SHell) sirve para acceder a máquinas remotas a través de una red, permitiendo copiar datos de forma segura.
- HTTPS es la versión segura del protocolo HTTP[16] utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado.
- FTPS (FTP/SSL) es un nombre usado para abarcar un número de formas en las cuales el software FTP puede realizar transferencias de ficheros seguras. Cada forma conlleva el uso de una capa SSL/TLS debajo del protocolo estándar.

---

[15] Online Certificate Status Protocol, este protocolo se describe en RFC 2560

[16] HyperText Transfer Protocol, es el protocolo usado en cada transacción de la Web (WWW)

- SSL (Seguridad de la Capa de Transporte), protocolo criptográfico que proporciona comunicaciones seguras en Internet.
- SET Secure Electronic Transaction (Transacción electrónica segura) es un protocolo estándar para proporcionar seguridad a una transacción con tarjeta de crédito en redes de computadoras inseguras, en especial Internet.

❖ **Infraestructura para almacenamiento de certificados**

Servicios de directorio X.500, y soporte para otros directorios o repositorios que tengan interfase LDAP.

❖ **Infraestructura de llave pública**

- Certificados X.509 v3
- Especificaciones para interoperabilidad mínima para componentes
- Protocolo de intercambio seguro (SEP)
- Mecanismos simples de llaves publicas GSS-API, RFC 2078

1.4. Consideraciones para la implementación de la PKI

En resumen las consideraciones que se deberán tomar en cuenta para evaluar la futura implementación de la PKI:

1.4.1. Flexibilidad y Compatibilidad

Una parte importante en la optimización del uso de una PKI, es que todos sus componentes sean compatibles con los diversos estándares y RFCs que definen cada uno de ellos. De esta forma la PKI, debe ser compatible con LDAP y X.500 para la comunicación con servidores de directorios.

Por otra parte, debe ofrecer la posibilidad de realizar tanto un nuevo registro de usuario como peticiones (de certificación, de revocación o renovación de certificados) por distintas vías : correo electrónico, navegador web o cualquier otro dispositivo de comunicación en red.

Según la finalidad a la que se destine el PKI, puede ser muy interesante tratar las peticiones por lotes, debido a su gran número. De esta forma, se exigirá a la Infraestructura de Clave Pública un proceso automatizado en la comunicación entre AR y AC.

Aunque los principios con los que funciona un sistema de PKI pueden ser complicados, su gestión no debe serlo. La PKI debe permitir a personal no especializado, manejarla con confianza. Estos operadores no tienen por qué entender las complicaciones de los algoritmos criptográficos, claves y firmas.

Debe resultar tan fácil como pulsar iconos y dejar a la aplicación de software que se encargue del resto. El interfaz debe ser gráfico e intuitivo, ayudando a la tarea de gestión, en lugar de dificultarla con complejos registros de la base de datos.

1.4.2. Sencillez

Las características más importantes de un sistema PKI, serán la flexibilidad y la sencillez en el manejo del mismo. Ello conllevará ventajas apreciables en todos los aspectos concernientes a la formación, el mantenimiento, la configuración del sistema, la integración de los distintos componentes y la posibilidad de crecimiento en el número de usuarios.

Pero como todo, tiene el inconveniente del coste asociado a la optimización de estas dos características. Hay que llegar a un equilibrio razonable entre ambos aspectos: el funcional y el económico.

1.4.3. Interoperabilidad

El escenario ideal para que exista una interoperabilidad en una o varias PKIs debería ser, cuando las entidades emisoras emitan un conjunto de certificados de interoperabilidad plena, basándose en un protocolo estándar de solicitud de certificados, solo así las aplicaciones dependientes podrán ser

evaluados adecuadamente y no existiría ambigüedad, ni sintáctica, ni semántica en la interpretación durante la duración del proceso.

Como es natural en el desarrollo de nuevas herramientas tecnológicas, es difícil conseguir el grado de interoperabilidad mencionado anteriormente, pero como es lógico a medida que se da un mayor número de aplicaciones que utiliza la tecnología basada en claves públicas, es más factible alcanzar una interoperabilidad sin problemas, esto es atribuible a la relativa madurez de esta tecnología.

Es importante tener muy claro que los estándares de Internet no aseguran la interoperabilidad, aunque resulten de una gran ayuda, como ocurre frecuentemente en los mercados de desarrollo tecnológico la falta de colaboración de las empresas hace que la estandarización sea mucho más complicado, y la tecnología de llaves públicas y certificados digitales no puede ser la excepción; actualmente la IETF tiene múltiples grupos de trabajo desarrollando activamente los estándares propuestos para la tecnología basada en claves públicas. Sin embargo, muchas de las posibles aplicaciones beneficiarias de estos estándares están ya integradas en productos comerciales. Además, ningún estándar puede anticipar todos los requisitos y dependencias de las aplicaciones. Incluso los estándares más completos no se aprovechan al máximo al implementarse. La interoperabilidad, entonces, es el resultado de los estándares atenuados por la realidad del mercado. El grupo de trabajo IETF encargado de la definición de bases para lograr la interoperabilidad de PKI es PKIX (X.509). Después de casi tres años de trabajo, la arquitectura básica está establecida y la especificación, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile, Part 1"[17] sigue el proceso de convertirse en estándar.

En IETF se están haciendo muchos esfuerzos que pueden tener impacto significativo en la compatibilidad de la PKI. Éstos se deben a las necesidades de las aplicaciones basadas en claves públicas, especialmente TLS, S/MIME e IPSec. En cada caso, estas aplicaciones se han visto en la necesidad de definir un subconjunto de PKIX que satisfaga sus necesidades o a menudo sustituyen la

[17] *http://www.ietf.org/ids.by.wg/pkix.html*

funcionalidad PKIX definida. Aunque podría parecer que esto trunca el proceso, en realidad crea un ciclo de sugerencias para los diseñadores de PKI.

También hay una "obligación moral" inminente para conseguir la interoperabilidad de la PKI. El National Institute of Standards (NIST) ha creado un grupo de trabajo acerca de interoperabilidad compuesto por AT&T, CertCo, Certicom, Cylink, Digital Signature Trust, Dynacorp, Entrust, Frontier Technologies, GTE, ID Certify, MasterCard, Microsoft, Motorola, Spyrus, VeriSign y Visa. El objetivo de este proyecto es asegurar la interoperabilidad mínima entre las implementaciones de los miembros de PKIX parte 1. NIST piensa que este grupo resolverá todas las ambigüedades y errores del nuevo estándar de PKIX.

Otro factor en la definición de los estándares de la PKI está completamente fuera de IETF.

Hay un conjunto de estándares[18] de hecho de mensajes cifrados ("PKCS"), desarrollados y mantenidos por RSA Laboratories, que se distribuyen ampliamente con los productos. Los estándares PKCS, publicados por primera vez en 1990, incluyen la sintaxis para los mensajes cifrados. Los estándares más relevantes para la PKI son PKCS-7, "Estándar de sintaxis de mensajes cifrados" y PKCS-10, "Estándar de sintaxis de solicitud de certificados". La importancia de estos estándares RSA radica en que proporcionan un marco básico, aunque bien definido, para la interoperabilidad. De hecho, cuando el grupo de trabajo PKIX propuso otro estándar para administración de certificados, el grupo S/MIME creó una propuesta propia basada en PKCS. Esta respuesta es típica de las prácticas de IETF y refleja su conocimiento del mercado. Los estándares de hecho son, a menudo, la mejor alternativa para maximizar así la interoperabilidad.

Es razonable esperar que los estándares se completen, aunque a fin de cuentas sólo un subconjunto de ellos se integra en los productos que crean los fabricantes para proporcionar soluciones interoperables. Un buen ejemplo de la fuerza de los mercados en la determinación de la interoperabilidad de claves públicas es el funcionamiento de los modelos de confianza.

1.4.4. Escalabilidad

[18] *http://www.rsa.com/rsalabs/html/standards.html*

La escalabilidad es una característica necesaria definida por el crecimiento paulatino del sistema. Se puede aplicar a diversos "campos" dentro de la Infraestructura de Clave Pública:

- Número de usuarios;
- Número y tipo de certificados emitidos;
- Número de CRLs almacenadas;
- Tipos de mecanismos de registro;
- Número de ACs y ARs en ejecución;
- Número de aplicaciones soportadas.

1.4.5. Confianza en la AC/AR

Una de las formas por las que se establece la confianza en una AC para un usuario consiste en la "instalación" en el ordenador del usuario (tercero que confía) del certificado autofirmado de la AC raíz de la jerarquía en la que se desea confiar. El proceso de instalación puede hacerse, en sistemas operativos de tipo Windows, haciendo doble click en el fichero que contiene el certificado e iniciando así el "asistente para la importación de certificados". Por regla general el proceso hay que repetirlo por cada uno de los navegadores que existan en el sistema, tales como Opera (navegador), Firefox o Internet Explorer, y en cada caso con sus funciones específicas de importación de certificados.

Si está instalada una AC en el repositorio de ACs de confianza de cada navegador, cualquier certificado firmado por dicha AC se podrá validar, ya que se dispone de la clave pública con la que verificar la firma que lleva el certificado. Cuando el modelo de AC incluye una jerarquía, es preciso establecer explícitamente la confianza en los certificados de todas las cadenas de certificación en las que se confíe. Para ello, se puede localizar sus certificados mediante distintos medios de publicación en internet, pero también es posible que un certificado contenga toda la cadena de certificación necesaria para ser instalado con confianza.

CAPITULO 2

MARCOS LEGALES NACIONALES E INTERNACIONALES SOBRE CERTIFICACIONES DIGITALES

2.1. Marco Legal Internacional

Existen sólo diecisiete países en el mundo con un marco legal establecido por sus respectivos gobiernos en el desarrollo de tecnología PKI. Esto da una idea de la situación en la que se encuentra la utilización de la Infraestructura de Clave Pública en el mundo.

España fue uno de los primeros países pioneros en la implementación de la firma digital y certificación digital, así como también han dado un gran aporte tecnológico al desarrollo de nuevas tecnologías orientadas a la seguridad informática.

La Unión Europea y Estados Unidos son los primeros que han definido modelos de estrategias globales para el desarrollo de Tecnologías de Información y Comunicaciones, y han sido para los demás países ejemplos a seguir en este campo.

La Infraestructura Nacional de la Información[19] es el modelo norteamericano impulsado por el gobierno de Bill Clinton, mientras que la conocida *Sociedad de la Información*[20] es el modelo adoptado por la Comunidad Europea, cada uno de estos modelos presentan características muy particulares, pero dentro de una concepción más general coinciden en señalar a la empresa privada como el motor que debe impulsar el desafío del cambio y a los gobiernos con la imperiosa necesidad de participación, fijando las pautas generales para crear un escenario propicio para el desarrollo de la investigación, encaminada a alcanzar un nuevo horizonte.

La situación en Europa es muy distinta de la estadounidense. En Estados Unidos reina una mayor libertad de mercado, porque las reglas no siempre son claras. Por el contrario, en Europa la Directi-

[19] *The National Information Infrastructure (NII)*
[20] *The Information Society (IS)*

va de Firma Electrónica y las correspondientes leyes nacionales sobre la materia han restringido el ámbito en el que se pueden mover los prestadores de servicios de certificación y los proveedores de estas tecnologías.

Además, en los países de la Unión Europea suele haber una autoridad auspiciada por el gobierno con vocación de establecerse como prestador de servicios genérico para facilitar el acceso a la firma electrónica por parte de los ciudadanos, como el **Proyecto Ceres**[21] en España o las fábricas de moneda y timbre de cada país.

Como es de suponerse, el sector privado ha sido el más interesado en el desarrollo de estas herramientas, presionando a los gobiernos a definir los marcos legales y regulatorios indispensables para su normal desenvolvimiento, pero como todo lo que brilla no es oro, los fabricantes de tecnología PKI que se crearon confiando en el boom de final del siglo pasado se han dado un buen tropiezo debido a varios factores entre los que se encuentran el antagonismo de la adopción masiva del comercio electrónico y el Ecuador no ha sido la excepción muchas empresas privadas esperan muy atentas a que este mercado sea realmente rentable.

¿Pero como puede el Estado construir el escenario necesario para que este mercado sea aprovechado por los empresarios?

Esta es una de las interrogantes que se han hecho muchos de los países en América Latina, y que las Naciones Unidas con el propósito de fomentar la armonización y unificación del derecho mercantil internacional y el progreso del comercio internacional de los países en desarrollo, el 16 de diciembre de 1996 la ***Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*** **(CNUDMI)** aprobó la ***Ley Modelo sobre Comercio Electrónico,*** así como también la elaboración de una ***Guía para la Promulgación de la Ley Modelo.*** Estos documentos, se elaboraron con la intención de ayudar a los gobiernos a fortalecer la legislación que rige la implementación de las nuevas tecnologías de información y comunicaciones, elementos que sustituyen a los medios manuscritos utilizados actualmente.

[21] *http://www.csi.map.es/csi/tecnimap/tecnimap1998/sp7.htm*

Como se había anotado anteriormente, la Comisión de las Naciones Unidas elaboraron un formato de **LEY SOBRE COMERCIO ELECTRÓNICO** para facilitar a los países que poco o nada conocían sobre el tema, la modificación o incorporación en sus legislaciones de una Ley que permita crear un marco jurídico coherente a las necesidades del uso del comercio electrónico en cada uno de las naciones, con la finalidad de proporcionar las reglas necesarias para sortear los obstáculos jurídicos que puedan presentarse en el ejercicio del mismo, de igual forma consientes de la complejidad y dificultad que podría presentarse para los Estados que no estaban familiarizados con las técnicas de comunicación presentadas en este documento, elaboraron una **GUIA** en base a la recopilación de sus primeras experiencias en el desarrollo de esta Ley, la que orientaría a los usuarios de los medios electrónicos de comunicación en los aspectos jurídicos de su empleo y a la implementación de las herramientas por parte de los estudios en el tema.

Otro de los aspectos considerados por la comisión es el de establecer un formato de **LEY** que permita en un futuro cercano, fomentar el comercio electrónico internacional, creando en cada uno de los países una legislación similar lo que permitiría llegar a tener un **entorno legal neutro** o como se conocería en la parte técnica estandarizar la ley para que las comunicaciones, convenios, entre otros, permitan facilitar el uso del comercio electrónico haciéndola más rápida, segura y eficiente.

Una vez que la Comisión de las Naciones Unidas proporcionaron la herramienta y su correspondiente manual de uso, realizaron una serie de sugerencias a gobiernos, estudiosos del tema, investigadores para que consideren esta normativa en sus actividades y hagan referencia al mismo con la intención de promulgar la estandarización del marco legal sobre uso del comercio electrónico, además como es lógico pensar recomiendan también utilizar a esta **LEY MODELO** como la base para aplicarla a los regimenes internos ya que podrá ser modificada según el marco jurídico en el que se pretenda establecer, existen también algunas consideraciones muy importantes como la **neutralidad tecnológica,** la **equivalencia funcional** y las **reglas de derecho supletorio o imperativo.**

Como se ha mencionado al inicio de este capítulo, los gobiernos cumplen un rol fundamental en el desarrollo de estas nuevas tecnologías de información y comunicaciones, una de estas herramientas que permiten que este cambio sea realidad es la Infraestructura de Llave Pública (PKI), ya que en ella se sustenta toda la **confianza** de este modelo al asegurar la autenticidad, integridad, no repudio, confidencialidad y auditabilidad de la información, bajo este esquema de seguridad que debidamente legalizado y regulado constituyen una gran aporte para el desarrollo comercial local e internacional de las naciones, de igual forma la empresa privada, el sector público pueden vislumbrar un futuro muy prometedor y la solución a muchos de sus problemas.

Pero es necesario destacar el compromiso de las naciones que conforman la Unión Europea, al agotar todos los esfuerzos necesarios para llegar a establecer consensos que han permitido conseguir un gran avance en materializar su **"Sociedad de la Información",** a pesar de las diferencias que puedan existir entre sus países han trabajado de forma conjunta para alcanzar los objetivos propuestos y proporcionar a sus pueblos de instrumentos valiosos para el desarrollo comercial, social y humano.

Este es el ejemplo a seguir pero lo debemos hacer con inteligencia no adoptando sus leyes o regulaciones por que lógicamente no somos iguales, sino haciendo un trabajo consiente en determinar cuales son nuestras fortalezas y debilidades, creando nuevas oportunidades y disminuyendo las amenazas que puedan presentarse en la implementación o utilización de las mismas, pero como poder conseguir este sueño, pues yo creo que la única manera es la de comenzar a trabajar de forma conjunta en poner en práctica lo que nos enseñan estas naciones, como mencionada el *Dr. Miguel Ángel Davara Rodríguez*[22] *"El desarrollo tecnológico es una realidad, y el derecho debe estar presente para que exista equilibrio en el uso de la tecnología, el hecho de que existan o no las normas que permitan regular su funcionamiento no frena el desarrollo y uso de la tecnología."*

Desarrollar nuevas tecnologías que permitan solucionar problemas en nuestras instituciones públicas, con la finalidad de disminuir el riesgo que puedan presentarse en transferencias de comercio

[22] *Doctor en Derecho Informático e impulsador de la Ley de Firma Electrónica en España.*

electrónico o de información por medios poco seguros, creando un esquema de certificación que pueda ser regulado y en el que se puedan establecer reglas y políticas claras y seguras, y tener el coraje de poder romper los paradigmas del cambio son algunas de las cosas que nos permitirán sacar adelante a nuestro país.

En lo que se refiere a los gobiernos esta es la lista de los que tienen iniciativas en este campo:

- Argentina: www.pki.arg.gov
- Australia: Government Public Key Infrastructure
- Austria: Supervisory Authority for Electronic Signatures
- Bélgica: Service public fédéral Technologie de l'Information et de la Communication (FEDICT) ó Centre d'Information sur la Signature Electronique
- Brasil: ICP-Brasil – Infra estrutura de Chaves Públicas Brasileira
- Canadá: GOC Public Key Infrastructure
- EEUU: Federal Public Key Infrastructure Steering Committee ó NIST PKI Program ó Department Of Defense PKI
- España: Fábrica Nacional de Moneda y Timbre - Proyecto CERES
- Francia: Le site du programme d'action gouvernemental pour la société de l'information ó Agence pour les Technologies de l'Information et de la Communication dans l'Administration
- Holanda: Dutch government PKI Task Force
- Hong Kong: Digital Certificate and Public Key Infrastructure
- Italia: Autorità per l'informatica nella Pubblica Amministrazione
- Nueva Zelanda: Secure Electronic Environment PKI
- Panamá: Proyecto Firma Digital y Comercio Electrónico (SENACYT)
- Reino Unido: HMG Public Key Infrastructure (PKI) ó Government Gateway
- República de Corea: Korea Certification Authority Central
- Singapur: Controller of Certification Authorities

2.2. Marco Legal Nacional

2.2.1. Antecedentes en la Superintendencia de Bancos y Seguros

La Superintendencia preocupada por cumplir con lo dispuesto en la Constitución de la República y salvaguardar los intereses Institucionales desde varios años atrás ha propuesto algunos proyectos sobre Seguridad Informática donde se incluyen la utilización de Firmas Electrónicas para el intercambio de información, a continuación una cronología de la evolución de estos proyectos:

- Con fecha 07 de Marzo del 2002, el Ing. Patricio Salgado Zapata, Director General de Gestión de Información envía al Dr. Alberto Chiriboga Acosta Presidente del Comité Informático Tecnológico un memorando[23] solicitando, se analice la prioridad de emprender el Proyecto de Seguridad Informática y Firmas Electrónicas en la Institución. En este documento se describe la necesidad y la importancia de la iniciación de dicho Proyecto.

  Se adjunta además un Proyecto piloto donde se describe el objetivo, los módulos necesarios y los costos para llevarlo a cabo.

- Con fecha 14 de enero del 2003, el Lcdo. Patricio Moreno Huras, Gerente Nacional de Estrategia y Gestión[24] hace referencia a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos publicada el 17 de abril del 2002, y a la vez solicita al Ing. Patricio Salgado Z. Gerente Nacional de Recursos Tecnológicos se sirva informar a ese despacho el impacto tecnológico de la aplicación de dicha Ley y los pasos que se deberían seguir para su eventual implementación. Se adjunta la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

- En contestación al memorando anterior, el Ing. Patricio Salgado da a conocer [25]que anteriormente se había expuesto al Presidente del Comité Informático la necesidad de emprender un Proyecto de Seguridad Informática y Firmas Electrónicas.

---

[23] Memorando No. DGGI-2002-047, solicitando emprender Proyecto de Seguridad Informática y Firmas Electrónicas.
[24] Memorando No. GNEG-SE-029, Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
[25] Memorando No. GNRT-2003-007, Proyecto de Seguridades Informáticas y Firmas Electrónicas.

En este documento se solicita además la recalificación del Proyecto de prioridad media a prioridad alta por el impacto institucional que tiene la misma.

Debido que el proyecto consta no solo de requerimientos tecnológicos, sino también de requerimientos jurídicos, se solicita que el área jurídica provea de los lineamientos y normativas para el efecto. Se menciona la contratación de una consultoría multidisciplinaria por la complejidad e importancia del Proyecto.

- En respuesta al pedido realizado por la Gerencia Nacional de Estrategia y Gestión, se elabora un memorando [26]con fecha 07 de marzo del 2003, donde se realiza un estudio del impacto jurídico y pasos para implantar la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su reglamento por parte de la Superintendencia de Bancos y Seguros.

  Este documento se convierte entonces como la parte más importante dentro del marco jurídico requisito indispensable para el normal desarrollo del Proyecto.

  Proyecto para implementación de Firmas Electrónicas para el intercambio de información entre la Superintendencia de Bancos y el Sistema Financiero.

  Este documento consta de los Objetivos, Antecedentes, Definiciones, Fases y Conclusiones referentes a la implantación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Aquí se describe en forma mas detallada algunos conceptos y fases que debería cumplir el Proyecto.

- En la Planificación Operativa del 2003, del Programa de Fortalecimiento de Tecnología Informática de la Gerencia Nacional de Recursos Tecnológicos, se hace referencia al Proyecto de Implementación de Firmas Electrónicas para el Intercambio de Información entre la Superintendencia de Bancos y el Sistema Financiero en el punto 4.1.7. el mismo que es considerado como de prioridad media.

---

[26] Memorando No. DNJ-DAL-2003-0078, Implementación de la Ley de Comercio Electrónico, Firmas Electrónicas y su normativa en la Superintendencia de Bancos y Seguros.

Como podemos apreciar desde el año 2002 la Superintendencia de Bancos y Seguros, comenzó a realizar gestiones para poder dotar de herramientas tecnológicas que permitan mejorar la seguridad en el intercambio de información con las entidades financieras.

2.2.2. Legislación

La Superintendencia de Bancos y Seguros del Ecuador (SBS) fue creada el 6 de septiembre de 1927 en el marco de una transformación del sector bancario y financiero del país, impulsada por la Misión Kemmerer que incluyó la expedición de la Ley Orgánica de Bancos, la Ley Orgánica del Banco Hipotecario (Banco Nacional de Fomento) y la Ley Orgánica del Banco Central.

Durante los 79 años de funcionamiento, la SBS ha desempeñado un rol fundamental en la economía y sociedad ecuatoriana mediante la expedición de normas para el funcionamiento de las instituciones que están bajo su ámbito de control, la supervisión del cumplimiento de las leyes y de la normatividad conexa; el control de las entidades supervisadas; y, en determinados casos, la intervención y liquidación de esas entidades, cuando los intereses del Estado y de la comunidad así lo han demandado.

La Constitución Política de la República del Ecuador, establece que la SBS es un organismo técnico con autonomía administrativa, económica y financiera, con personería jurídica de derecho público, encargada de controlar instituciones públicas y privadas, a fin que las actividades económicas y los servicios que presten se sujeten a la Ley y atiendan al interés general.

La Ley General de Instituciones del Sistema Financiero (LGISF), la Ley General de Seguros (LGS) y la Ley de Seguridad Social (LSS), por su parte, determinan que la SBS es la Institución que tiene a su cargo la supervisión y control de las entidades que integran los sistemas financiero, de seguro privado y de seguridad social, respectivamente.

De igual manera, la Ley de Régimen Monetario y Banco del Estado señala que, corresponde a la SBS realizar el control externo de las operaciones financieras y administrativas del Banco Central del Ecuador; y, complementariamente, las leyes de creación o constitutivas de las instituciones fi-

nancieras públicas: Banco del Estado, Corporación Financiera Nacional, Banco Nacional de Fomento, Banco Ecuatoriano de la Vivienda, Fondo de Solidaridad e Instituto Ecuatoriano de Crédito Educativo y Becas, imponen a la SBS la obligación del control y vigilancia de las mismas.

El Superintendente de Bancos y Seguros es la máxima autoridad de la Institución y entre sus principales responsabilidades asignadas en la Ley General de Instituciones del Sistema Financiero constan: velar por la estabilidad, solidez y correcto funcionamiento de las instituciones sujetas a su control; establecer programas de vigilancia preventiva y practicar visitas de inspección a las instituciones controladas; mantener un sistema de registro crediticio a través de una central de riesgos que permita contar con información clasificada sobre los principales deudores de las instituciones del sistema financiero; y, exigir que las entidades controladas presenten y adopten las correspondientes medidas correctivas y de saneamiento en los casos que así lo requieran.

La SBS tiene además como parte de su estructura a la Junta Bancaria, conformada por cinco miembros: el Superintendente de Bancos y Seguros, quien la preside; el Gerente General del Banco Central del Ecuador; dos miembros designados por el Presidente Constitucional de la República; y, un quinto miembro designado por los cuatro antes referidos. La Junta Bancaria formula la política de control y supervisión del sistema financiero y del sistema de seguro privado, resuelve casos no consultados en la Ley General de Instituciones del Sistema Financiero y en la Ley General de Seguros, casos de revisión de orden administrativo y aprueba el presupuesto de la SBS, entre otras funciones.

El ámbito de control y supervisión de la SBS comprende 133 entidades operativas que administran aproximadamente un total de 16 mil millones de dólares en activos, que representa alrededor del 47 por ciento del Producto Interno Bruto del Ecuador, al mes de agosto del año 2005.

Cuadro 1. Resumen de entidades financieras controladas por la SBS.
Elaborado por: el autor

ENTIDAD	NÚMERO DE ENTIDADES	MILLONES DE US$	% PIB
Bancos Privados	25	8.892,00	28,00
Banca Pública	4	1.177,00	3,70
Cooperativas	35	723,00	2,20
Mutualistas	5	336,00	1,10
Sociedades Financieras	11	527,00	1,60
Casas de Cambio	1	5,00	-
Almaceneras	4	20,00	0,10
Compañías de Titularización	1	26,00	0,10
Tarjetas de Crédito	1	74,00	0,20
Empresas de Sguro Privado	40	397,00	1,20
Compañías de Reaseguros	2	6,00	-
IESS	1	3.339,00	8,10
ISSFA, ISSPOL, SCPN	3	261,00	0,80
TOTAL	**133**	**15.783,00**	**47,10**

Adicionalmente, la SBS ejerce el control a:

- Fondos Complementarios Previsionales, de los cuales 55 han presentado la documentación para su registro en la SBS. Hasta el momento han sido autorizados 10 Fondos con activos superiores a los 360 millones de dólares.
- Asesores productores de seguros (752), Intermediarios de Reaseguros (16) y Peritos de Seguros (124).

En el ámbito de la supervisión a las entidades que integran el sistema financiero nacional, la promulgación de normas sobre la administración de los diversos tipos de riesgos, así como el desarrollo de metodologías, herramientas y procedimientos uniformes de control, fueron los avances más destacados en esta materia y es precisamente donde se enfoca el aporte tecnológico de las nuevas tecnologías de información.

Dentro de la marco práctico de la supervisión, la SBS recibe periódicamente información sensible de las entidades del Sistema Financiero a través de medios poco seguros, los cuales son procesados y

direccionados a las instituciones financieras hacía un mejoramiento en su gestión de los riesgos de liquidez, de mercado y de productos derivados, en cumplimiento de los Principios 12 y 13 del Comité de Basilea.

Otro producto importante que se obtiene del tratamiento de esta información es el riesgo crediticio, basado en la premisa que este es el principal riesgo que se presenta en la actividad de intermediación financiera, se expidieron al respecto varias normas de control del riesgo crediticio acordes con los Principios 7 y 8 del Comité de Basilea.

Una característica importante de estas normas se refieren a que las instituciones financieras cuenten con una **"tecnología crediticia"** adecuada para el otorgamiento de los diferentes tipos de crédito, es decir el desarrollo de buenas prácticas y procedimientos de calidad en el manejo de sus carteras.

Otro aspecto importante de resaltar tiene que ver con la entrega de información oportuna y veraz sobre la calidad crediticia de los deudores como un requisito ineludible para una correcta supervisión de este riesgo; con ese propósito, se estableció un marco regulatorio para la creación y operación de los **BUROS DE INFORMACION CREDITICIA**.

Analizando estos antecedentes, se puede determinar la importancia y la necesidad de utilizar nuevas tecnologías de información que permitan de alguna manera, efectuar un mejor, más seguro y eficiente intercambio de información, entre las entidades financieras, que forman parte del Sistema Financiero del Ecuador y la Superintendencia de Bancos y Seguros.

Existe además en el país la "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos" expedida el 17 de abril del 2002, así como también su respectivo Reglamento lo cual permite sustentar el proyecto dentro de un marco legal adecuado.

También existe un "Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación de Información y Servicios Relacionados" emitido por el

CONATEL encamina al uso de firma electrónica, registro de datos y sellado de tiempo entre otras actividades relacionadas con el presente proyecto. Este es el último documento regulado por el Consejo Nacional de Telecomunicaciones, que tiene como finalidad llamar a una Audiencia Pública para calificar a todas las Entidades Públicas o Privadas como Autoridades Habilitantes de Servicios de Certificación de Información.

Este reglamento establece las normas y procedimientos aplicables a la prestación de Servicios de Certificación, así también como los deberes y derechos de los prestadores de estos servicios y de sus usuarios.

Por otra parte, muchas instituciones en el ámbito internacional han adoptado soluciones similares para mejorar sus seguridades informáticas; por ser la Superintendencia de Bancos y Seguros, una institución que maneja información muy sensible del Sistema Financiero, es prioridad y obligación de la misma hacer los esfuerzos necesarios por aumentar los niveles de seguridad en sus servicios de transferencias y aplicaciones.

CAPITULO 3

ESQUEMAS DE CERTIFICACIÓN

3.1. ARQUITECTURAS DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA

Una infraestructura de clave pública, generalmente está constituida de una o varias Autoridades de Certificación o Círculos de Confianza. Un círculo de confianza puede establecer rutas de confianza con una o varias Autoridades de Certificación o varios Círculos de Confianza, de tal manera que el Círculo de Confianza puede estar seguro de la validez del certificado.

Los receptores de un mensaje firmado que no tienen relación con la Autoridad Certificadora que emitió el certificado para el emisor del mensaje, puede todavía validar el certificado encontrando una ruta de confianza entre las dos Autoridades Certificadoras.

Para poder cumplir con esta meta existen tres tipos de arquitecturas de infraestructura de clave pública:

1. Jerárquica Subordinada,
2. metch (malla) y
3. bridge (puente)

3.1.1. Jerárquica

Las Autoridades Certificadoras están organizadas jerárquicamente bajo una autoridad Certificadora raíz que emite certificados a Autoridad Certificadas subordinadas.

En una Infraestructura de Llave Pública Jerárquica cada parte que la compone, conoce la clave pública de la autoridad certificadora raíz.

Además, cualquier certificado puede ser validado al verificar la ruta de certificación de los certificados de la Autoridad Certificadora raíz, como se muestra en la **Figura 8.**

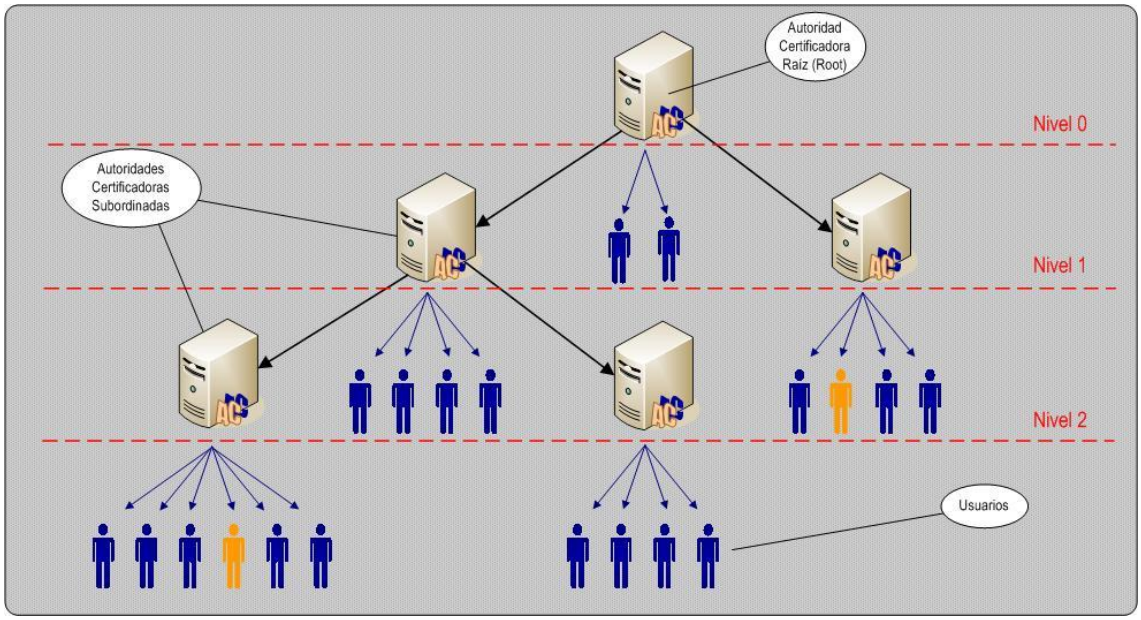

Figura 8. Esquema de una Infraestructura Jerárquica Subordinada
Elaborado por: el autor

3.1.2. Mesh (Malla)

Autoridades Certificadoras independientes se certifican de manera cruzada entre ellas (emiten certificados una a la otra) dando como resultado una malla general de relaciones de confianza entra Autoridades Certificadoras pares. **(Ver Figura 9)**

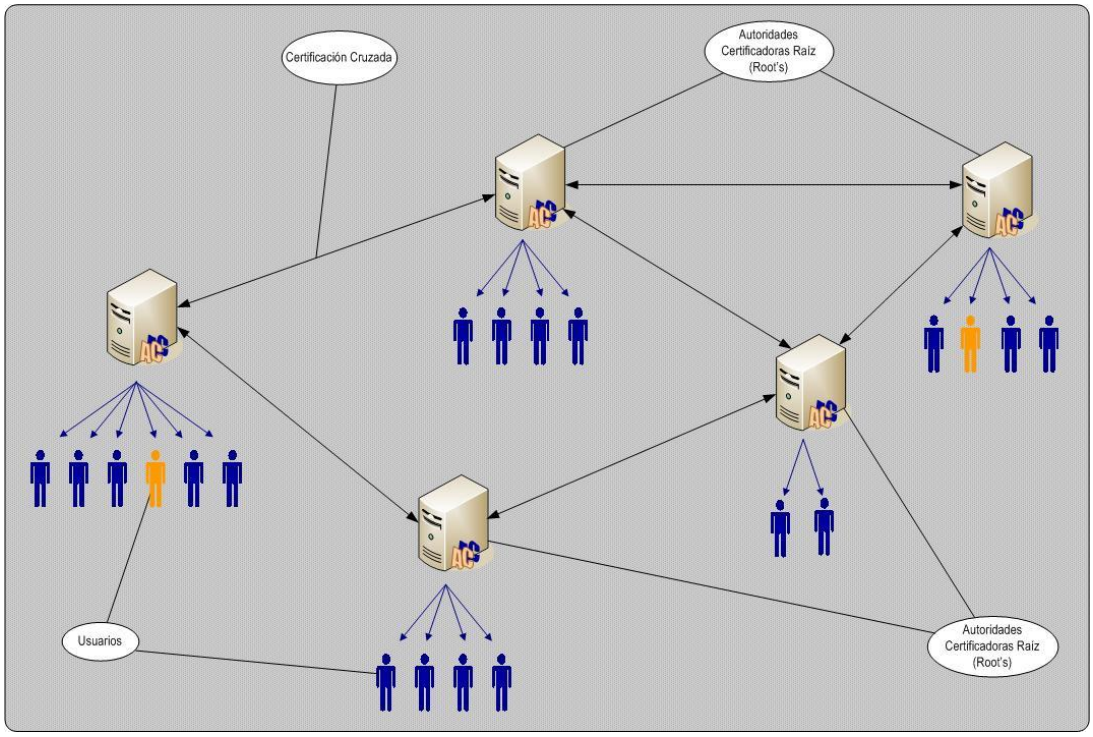

Figura 9. Esquema de una Infraestructura en Malla
Elaborado por: el autor

3.1.3. Bridge (Puente)

El propósito principal de esta arquitectura es establecer a una Autoridad Certificadora como puente entre varias Infraestructuras de llaves Públicas empresariales, a diferencia de la arquitectura de malla la Autoridad Certificadora que sirve de puente no puede emitir certificados directamente a los usuarios.

Todos los usuarios que componen las diferentes Infraestructuras sólo deben considerar a la Autoridad Certificadora como intermediaria ya que ella establece todas las relaciones par a par con las diferentes PKI empresariales, además estas relaciones pueden ser combinadas para realizar puentes de confianza que conecten a los usuarios de las diferentes PKI´s.

Si el dominio de confianza es implementado como una PKI de nivel jerárquica la Autoridad Certificadora Puente establecerá una relación con la Autoridad Certificadora raíz.

Si el dominio de confianza es implementado como una PKI de malla la Autoridad Certificadora Puente solo establecerá la relación con una de las Autoridades Certificadoras de la malla.

En cualquiera de los dos casos la Autoridad Certificadora que entra en relación con la Autoridad Certificadora puente es la principal.

Estas Autoridades Certificadoras pueden emitir certificados a Autoridades Certificadoras que se encuentren debajo de ellas en jerarquía o a usuarios. **(Ver Figura 10)**

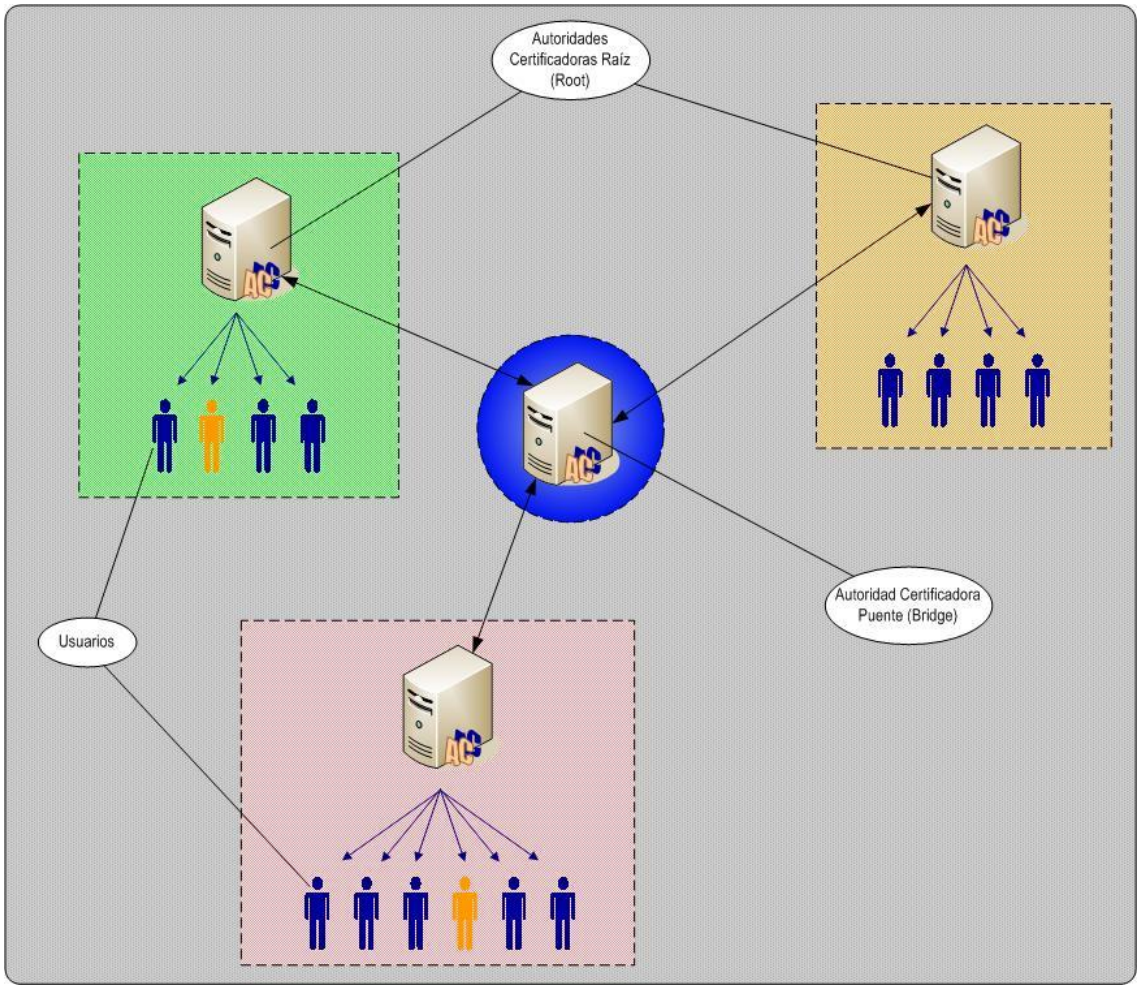

Figura 10. Esquema de una Infraestructura en Puente
Elaborado por: el autor

Una vez analizados las diferentes arquitecturas o esquemas que puede adoptar una Infraestructura de llave pública, se estudiará las consideraciones que debe tomar la Superintendencia de Bancos y Seguros para poder generar y administrar adecuadamente las firmas y certificados digitales, a continuación se presenta las ventajas y desventajas de cada una de ellas así como también una breve descripción del marco técnico y legal que deberá adoptar para su correcto funcionamiento.

Para que una Autoridad Certificadora sea acreditada[27] como tal es necesario tener en cuenta lo siguiente:

- Consideraciones Operativas
- Consideraciones Legales

[27] *Acreditada por el CONATEL como autoridad habilitante para Prestar Servicios de Certificación de Información y Servicios Relacionados., según Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas.*

- Consideraciones Técnicas
- Arquitectura

La Superintendencia de Bancos y Seguros deberá asegurarse que siempre exista un equilibrio entre estas cuatro consideraciones, ya que estas determinarán la responsabilidad dentro de su desenvolvimiento y actuación en el proceso de certificación, a continuación se presentarán los casos que podrían ser adoptados.

3.2. Como Autoridad Certificadora (SBS AC)

a. Consideraciones Operativas

Para poder cumplir con las funciones y responsabilidades de una Autoridad Certificante, la Superintendencia de Bancos y Seguros, deberá contar con el personal necesario para llevar a cabo procesos de certificación, en este caso la Dirección Nacional de Recursos Tecnológicos dispondrá del personal técnico del área para la distribución de funciones y responsabilidades según la necesidad, entre otras tareas que deberán ser asignadas serán la de emitir, renovar, revocar y actualizar los repositorios de certificados, esto en cuanto a la administración de los certificados y su ciclo de vida, otra parte técnica importante de considerar es que en la parte de comunicaciones se debe contar con un esquema de seguridad que pueda brindar la confianza necesaria para poder operar la certificación para esto se deberán utilizar equipos de software disponibles por la institución.

Se deberá contar con el personal necesario para la verificación ý actualización de información de entidades.

b. Consideraciones Legales

Adicionalmente, una comisión multidisciplinaría deberá crear el marco jurídico necesario para que los procesos de certificación estén debidamente enmarcados en las Leyes y Reglamentos. En este estudio se podrá determinar la factibilidad de que la Superintendencia de Bancos y Seguros pueda ser una Autoridad de Certificación, debido a que al adoptar esta figura la institución

estaría realizando actividades no prescritas o dispuestas en la Constitución o en las Leyes de la República.

De igual manera, según la Ley de Comercio Electrónico, Firmas Electrónicas y mensajes de Datos, la Superintendencia de Bancos y Seguros debería cumplir con todos los requisitos para obtener el título habilitante como Autoridad Certificadora.

c. Consideraciones Técnicas

Es muy importante en la parte técnica proporcionar a la Infraestructura de Llave Pública todas las herramientas necesarias para que puedan cumplir con las obligaciones y responsabilidades que implica ser una Autoridad Certificante, como se anotó anteriormente es imprescindible contar con un ambiente seguro donde se pueda mantener la información sensible debidamente resguardada y asegurada para no poner en riesgo la PKI, actualmente la Institución mantiene un nivel de seguridad de la información aceptable, las políticas y procedimientos proporcionan la confianza necesaria para la implementación del prototipo.

Otro aspecto muy importante que se debe considerar es que las herramienta hacer utilizada para la generación y administración de Certificados Digitales cumpla con las normas y estándares técnicos definidos en las Leyes y Reglamentos de Comercio Electrónico.

d. Arquitectura

La arquitectura utilizada en este caso es la jerárquica, la Institución deberá contratar los servicios de una autoridad superior fuera o dentro del país, está la reconocerá como una Autoridad Certificadora debidamente acreditada para prestar servicios de certificación.

En este primer caso la Superintendencia de Bancos y Seguros será una entidad certificadora reconocida por un nivel superior[28]. (**Ver figura 11)**

[28] *Autoridad Habilitante Nacional o Internacional debidamente reconocida por el CONATEL*.

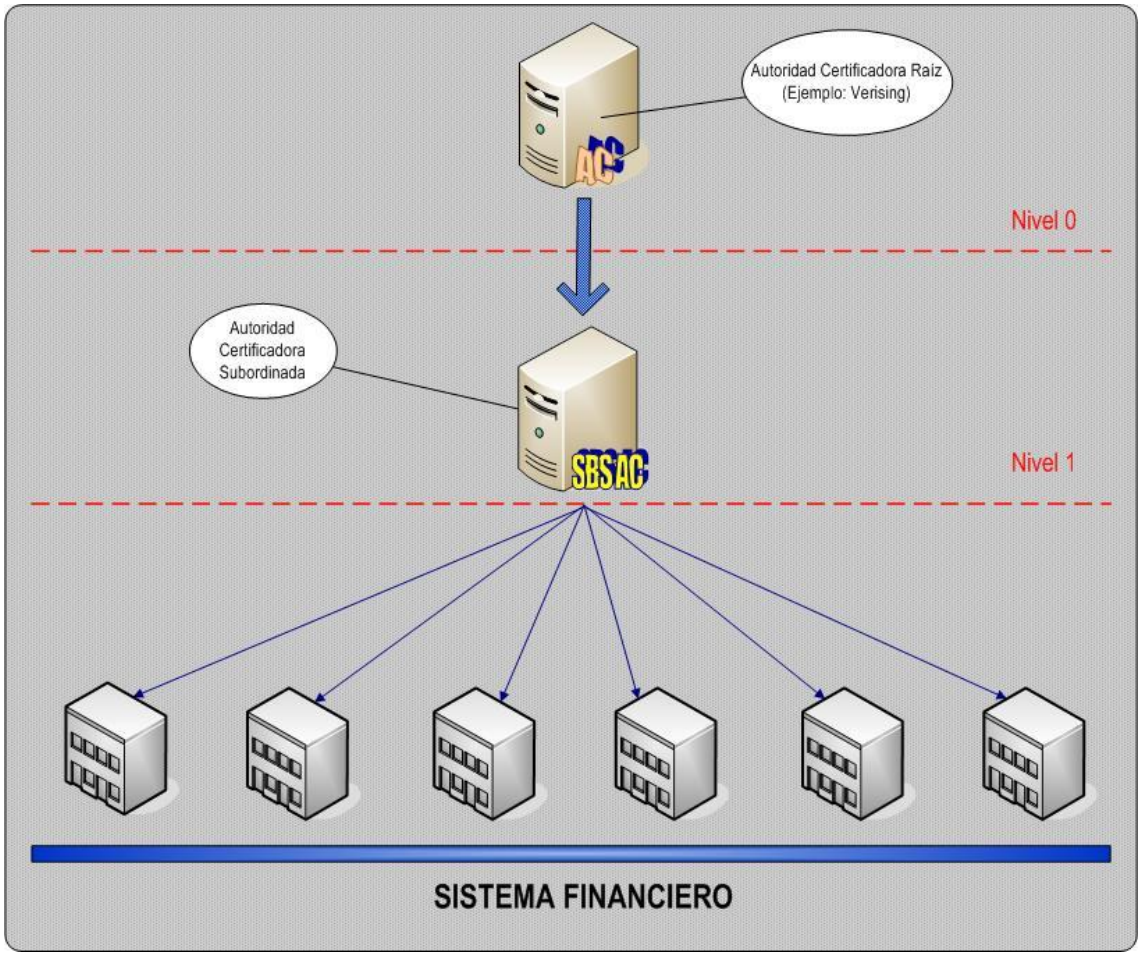

Figura 11. Esquema de certificación donde la SBS es reconocida por un nivel superior
Elaborado por: el autor

La arquitectura usada en este caso es la de jerarquización pudiendo en algún momento convertirse en una de malla, si el crecimiento de las necesidades y usuarios lo ameriten, pero en realidad es poco probable que en algún momento se pueda adoptar esta arquitectura ya que el alcance del servicio es muy reducido.

La clave raíz será firmada por una Autoridad Certificadora Superior quién será responsable de la firma de las otras Autoridades Certificadoras Subordinadas. En todos los certificados generados, la Autoridad Certificante de la Superintendencia de Bancos y Seguros aparecerá dentro de la cadena de certificación, debajo de la Autoridad de Certificación Superior.

3.3. Como Autoridad de Registro (SBS AR)

a. Consideraciones Operativas

En este caso se considera que la responsabilidad de la administración del ciclo de vida de los certificados se encuentra a cargo de la Autoridad Certificadora de nivel superior esto implica una reducción del personal operativo,

b. Consideraciones Legales

La entidad certificador deberá previamente a prestar los servicios de certificación, solicitar la acreditación en el Consejo Nacional de Telecomunicaciones y cumplir con las disposiciones establecidas en el Capitulo III de la **Ley de Comercio Electrónico, Firmas y Mensajes de Datos, artículos 32, 33, 34, 35 y 36** así como también los artículos 7, 8 y 9 del Capitulo I del **Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación de Información y Servicios Relacionados**, **RESOLUCION No.584-23-CONATEL-2003.**

c. Consideraciones Técnicas

La responsabilidad de los equipos de comunicación, servidores, bases de datos, definición de protocolos estarán bajo la responsabilidad de la entidad certificadora, así como también su mantenimiento y la administración del ciclo de vida de los certificados, de igual manera como se había anotado anteriormente deberán responder por los daños y perjuicios que la entidad certificadora pudiera causar por el manejo inadecuado de los equipos e información.

d. Arquitectura

En este caso la Superintendencia de Bancos y Seguros, podría adoptar cualquier de las arquitecturas señaladas al inicio de este capítulo, debido a que su función o relación entre los usuarios y la Autoridad Certificante es mediadora, es importante considerar que la definición de las políticas y procedimientos que deberá seguir la institución, estén claramente señaladas y esta-

blecidas, tanto en las Políticas de Certificación como en los manuales de procedimientos, ya que así se podrá evitar inconvenientes en el futuro.

3.4. Esquema seleccionado por la Institución

Al principio de este capitulo se presentó los tipos de arquitecturas más utilizados, tres fueron las arquitecturas que se han establecido como las más comunes o más usadas en la Certificación Digital, debido a que esta tecnología se encuentra en desarrollo no existen camisas de fuerza en la selección de las arquitecturas que se deben implementar, por lo que es lógico pensar que según la naturaleza de los servicios que pueda prestar una Institución (Autoridad Certificante o de Registro) se podrán crear nuevos esquemas de certificación siempre y cuando estos mantengan la esencia de una Infraestructura de Llave Pública así como sus elementos.

En el caso estudiado, se presenta una arquitectura tipo estrella a continuación se mostrará la figura **(Ver Figura 12)**, así como sus flujos y explicación:

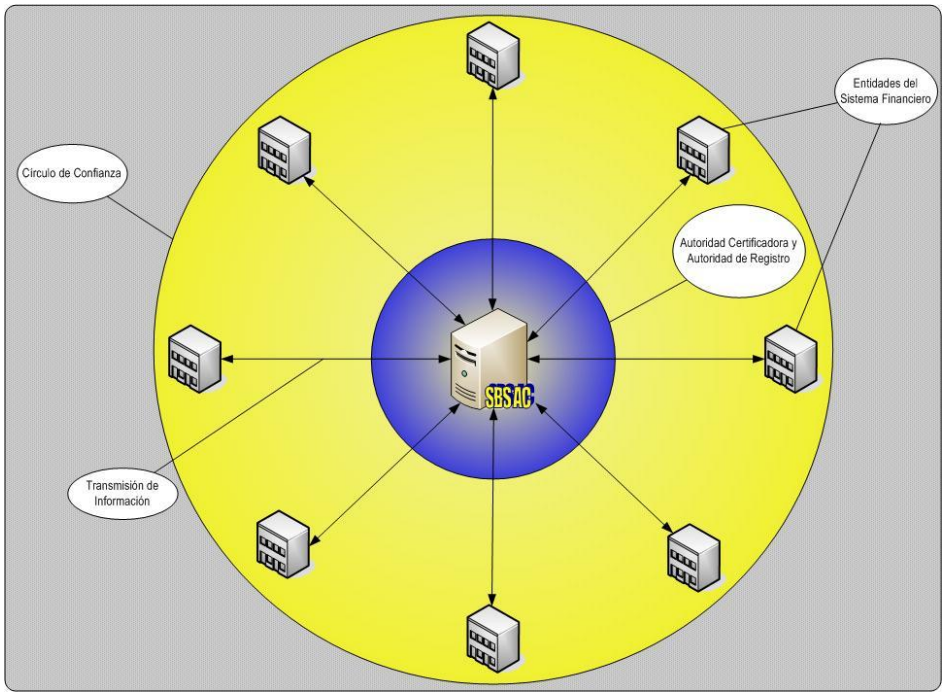

Figura 12. Arquitectura Tipo Estrella
Elaborado por: el autor

En la parte central de la Infraestructura está localizada las Superintendencia de Bancos y Seguros, esta delimita un círculo de confianza a nivel del sistema financiero, donde cada una de las entidades

que están bajo su control y que envían información, deberán solicitar la generación de un certificado digital así como también su llave privada, para esto deberá seguir muy detenidamente los manuales de procedimientos y políticas de certificación previamente difundidas por la Institución.

Una vez generados los certificados y llaves privadas, estas deberán ser entregadas a los usuarios por medios seguros, lo que permitirá aumentar la confianza de los usuarios en la infraestructura, de igual manera la forma de entrega deberá estar claramente establecidas en las políticas de certificación.

Una vez que los usuarios cuenten con sus certificados y llaves privadas podrán realizar intercambios de información, utilizando una aplicación disponible en la WEB donde podrán acceder a un sitio seguro considerado como un repositorio de información, ahí podrán depositar o sustraer información sensible dentro de un marco de seguridad, rapidez y sencillez.

3.5. Modelo de Seguridad para la AC

Como se ha anotado anteriormente, la base de la confianza de una infraestructura de clave pública radica, en cuan seguro puede ser el ambiente en el que se encuentran sus elementos, así como también las operaciones de certificación y del negocio, de tal forma que el ambiente de la red comunicaciones debe ser integrada con todos los participantes o usuarios, esto puede ser con la utilización de una intranet o Internet, basado en protocolo TCP/IP, con las condiciones de seguridad adecuadas, condiciones que deben satisfacer además la red de comunicaciones del sistema financiero.

A continuación se presenta el esquema de comunicaciones desarrollada para el prototipo:

DIAGRAMA DE COMUNICACIONES
SUPERINTENDENCIA DE BANCOS Y SEGUROS

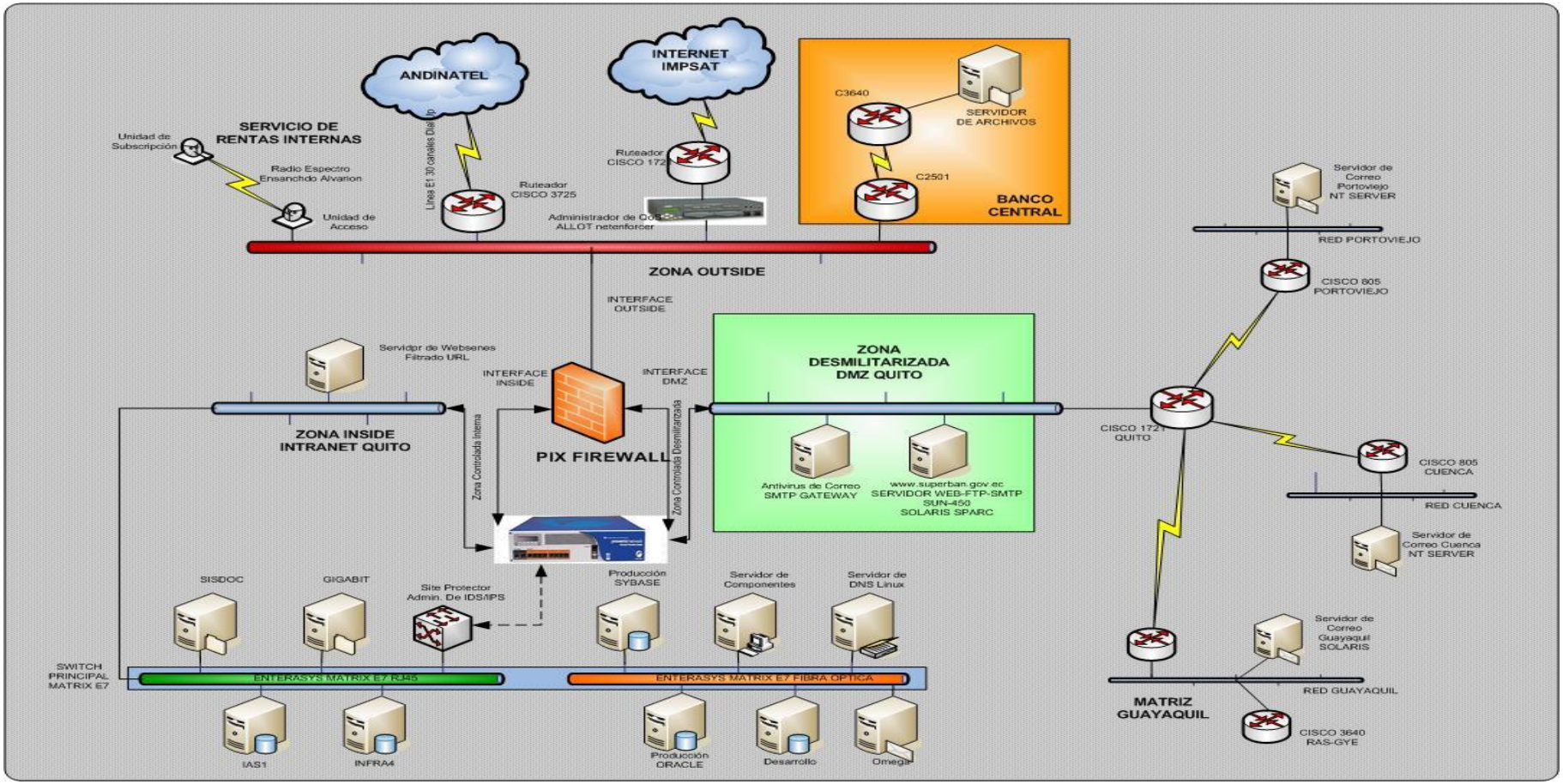

Figura 13. Diagrama de Comunicaciones
Elaborado por: el autor

3.6. Estándares Tecnológicos Utilizados

A continuación, se revisará las herramientas y los estándares con los que cuenta la Institución, se presenta también algunas herramientas disponibles en Internet que servirán para mejorar la seguridad del ambiente de comunicaciones y datos.

Debido a la mayoría de las operaciones se la realizarán a través de los navegadores, es importante contar con un modelo SSL de comunicaciones, para lo cual es necesaria la instalación del servidor HTTP Apache y de su módulo mod_ssl lo que nos permitirá tener una vía de comunicación segura (para acceso a directorio LDAP, POP3, IMAP). Esto en relación a las comunicaciones, en lo referente a la aplicación se presenta la siguiente tabla donde se muestra de mejor manera los estándares tecnológicos:

Tabla 1. Estándares tecnológicos.
Elaborado por: el autor

CARACTERÍSTICA	ESTANDAR	OBSERVACIÓN
Normas de Certificados	A.509 V3 incluyendo las extensiones estándar	Se puede utilizar para SSL, S/MIME, IPSec[29], SET
Atributos del Directorio de Certificados	Repositorio Integrado LDAP v2/v3 y X.500	Es muy importante utilizar este estándar con SSL, para la comunicación entre los componentes.
Atributos de Ambiente de Clave Pública	Publicación de CRL Certificados Cruzados Recuperación de Certificados y certificados cruzados	
Atributos de Certificados	Formato X.509 v1/v3	

[29] *IPSec.- es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado.*

Algoritmo de Llave Pública	RSA (512 -1024) DSA (1024)	
Algoritmo de llave de sesión	3-DES	
Función HASH	MD5,SHA-1	

ESTÁNDARES PKCS

Tabla 2. Estándares PKCS.
Elaborado por: el autor

# PKCS	Versión	Nombre	Observación
PKCS#7	1.5	Estándar sobre la sintaxis del mensaje criptográfico	Usado para firmar y/o cifrar mensajes en PKI. También usado para la diseminación de certificados. Fue la base para el estándar S/MIME, ahora basado en la RFC 3852, una actualización del estándar [[CMS] Cryptographic Message Syntax, utilizado par firmar digitalmente, obtener el digest, autenticar, o cifrar arbitrariamente el contenido de un mensaje (no confundir con Sistema de gestión de contenido -Content Management System-)]
PKCS#11	2.20	Interfaz de dispositivo criptográfico ("**Cry**ptographic **Tok**en **I**nterface" o cryptoki)	Define un API genérico de acceso a dispositivos criptográficos.
PKCS#12	1.0	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.

CAPITULO 4

DESCRIPCIÓN DE APLICACIONES COMERCIALES

En este capítulo se pretende realizar una recopilación de distintos software proporcionado o disponible en el mercado tanto americano como en la unión europea, ya que es preciso conocer si los estándares utilizados por estas empresas desarrolladoras cumplen con las exigencias y especificaciones técnicas mostradas en capítulos anteriores, además se pretende dar un vistazo de que tan amigables son estas herramientas y determinar la complejidad de su funcionalidad y uso.

4.1. Productos de Entrust.

a. Antecedentes de la empresa

Entrust es una empresa que ofrece productos de seguridad, colaborando con empresas y gobiernos en la solución de problemas y obstáculos que se presentan en las comunicaciones e Internet.

Desde 1994 Entrust ha ido desarrollando tanto sus productos como la tecnología, para acoplarla a las necesidades de los usuarios, su participación en el mercado ha sido muy productiva tanto es así que su producto **Entrust Authority™** se encuentra en su séptima edición esto nos da la pauta de que es una empresa que ha sabido ubicarse en un sitial importante en el mundo de la certificación.

Es importante considerar también que analizando su desenvolvimiento en la atención a sus clientes, la empresa tiene muy en cuenta aspectos muy importante como son la seguridad, funcionalidad y flexibilidad de la herramienta, lo que obviamente permite tener una gran escalabilidad en el negocio de cualquier empresa privada o de gobierno.

Entre algunas participaciones destacadas de Entrust en el mercado, es la participación en la creación de un prototipo para la creación de una Autoridad Certificadora Federal para el Gobierno de los Estados Unidos, conocida actualmente como United States Federal Bridge Certification Authority (FBCA), y es considerado como la base fundamental para proveer de servicios de comunicaciones

seguras para el intercambio de información gubernamental e intergubernamental. La implementación de esta solución a permitido alcanzar grandes ventajas tanto en las agencias como en las organizaciones de gobierno.

b. Características del producto

A continuación se presenta las funcionalidades y características del PKI de Entrust, información y experiencias recopiladas de su sitio web[30] y pruebas realizadas con la herramienta.

El PKI de Entrust tiene múltiples **funcionalidades** que hacen la diferencia con diversas soluciones existentes en el mercado.

1. Entre las múltiples funcionalidades que se tendrán serán:
    a. Correo Seguro.
    b. Encriptación y firma de archivos confidenciales.
    c. Control de acceso, autentificación en la web.
    d. Implementación de Single Sign On (Un solo user /password para muchas aplicaciones).
    e. Protección de la Información confidencial que es robada en laptops, PC o discos duros.
    f. Implementación de VPN entre dispositivos y usuarios finales.
    g. Implementación de Certificados en conexión WAP.

Entre sus principales características tenemos:

2. Con el PKI de Entrust se manejan servicios de seguridad tales como:
    a. **Confidencialidad** para mantener la privacidad de la información.
    b. **Integridad** la información no debe ser modificada.
    c. **No repudio** no se puede negar el involucramiento en una acción.
    d. **Autentificación** asegurar la identidad de algo o alguien.
    e. **Control de Acceso** que recursos tiene permitido.
3. La infraestructura de Pki de Entrust tiene:

[30] *www.entrust.net*

a. **Certificación Cruzada.-** Permite estar en una estructura jerárquica muchas entidades certificadoras y en esta estructura jerárquica la Superintendencia de Bancos puede ser el root en Ecuador, creando root de confianza para el sistema financiero ecuatoriano. De esta manera se podría acceder a la red IDENTRUST que una red de confianza a nivel mundial del sistema financiero.

b. **Manejo de Histórico de llaves.-** Es sumamente importante debido a que si una llave es comprometida esta puede ser revocada pero el usuario final puede acceder a su información encriptada anterior sin ningún inconveniente.

c. **Key Backup and Recovery.**- Utilizando la Infraestructura de Pki se convierte en un servicio crítico, por lo que es indispensable que los procedimientos de Backup y Recovery sean confiable y rápidos.

d. **Revocación de Certificados.-** La revocación de certificados se hace indispensable, muchas infraestructuras de Pki se vuelven vulnerables debido a que no tienen un mecanismo para comunicación de certificados revocados. Entrust lo tiene.

e. **Actualización automática de llaves y certificados.-** Una de las principales causas de fracaso de los PKI es que no tienen un mecanismo seguro, automático para la distribución de llaves. Entrust provee este mecanismo de manera transparente para el usuario final y los administradores. Permitiendo que se ahorren tiempo sus administradores y usuarios.

f. **Repositorio de Llaves de encriptación.**- Entrust en forma automática y con mecanismos seguros solo respalda las llaves de encriptación y puede acceder solamente el cliente dueño de las llaves. Esto se hace para tener respaldo de las llaves de encriptación para evitar la perdida de acceso a información confidencial en caso de perdida de la llaves por parte del usuario. Este respaldo no se hace con la llave de firma digital .

g. **Timestamping.-** Con esta característica podemos certificar la veracidad de un documento electrónico en determinado tiempo.

4. Utiliza un arquitectura de doble par de llaves en un certificado es decir un par para encriptación y otro para la firma digital, esto se debe a que a nivel mundial se esta recomendando utilizar esta arquitectura para proteger lo que es firma digital de respaldos mal manejados.
5. Tiene un **modulo central** que contiene la CA (Entidad certificadora y la Entidad Registradora) que están certificados con el nivel mas alto de la industria FIPS 140 y Common Criteria.
6. Con esta infraestructura se implementa una **arquitectura de seguridad central** para la organización donde se podrá llevar en forma centralizada la seguridad de la organización.
7. Tiene **módulos para que las aplicaciones** que funcionan dentro de la organización puedan adaptarse a la infraestructura de PKI.
8. Tiene un set **completo de herramientas de desarrollo** que están disponibles totalmente gratis para que los desarrollos internos de la organización sean adaptados al PKI.

4.2. Productos Verising.

a. Antecedentes de la empresa

VeriSign, Inc. proporciona servicios de infraestructura inteligente que permiten a las personas y empresas ponerse en contacto, conectarse y reforzar la seguridad de las transacciones comerciales que se realizan en las complejas redes globales actuales. Empresas, distribuidores, gobiernos y personas de todo el mundo confían en VeriSign para obtener los beneficios de la continuada revolución del comercio y las comunicaciones, respaldando nuevas corrientes de beneficios y reduciendo el coste, el cumplimiento normativo y la complejidad.

Día a día, Verising trabaja con infraestructuras inteligentes que permiten que se produzcan catorce mil millones de interacciones en Internet, 2.700 millones de interacciones telefónicas y transacciones comerciales por más de 100 millones de dólares. También proporciona los servicios que permi-

ten trabajar con seguridad, fiabilidad y eficacia a más de 1.000 distribuidores, 3.000 empresas y 400.000 sitios web.

A medida que emergen las redes de próxima generación, VeriSign también trabaja en el desarrollo de las tecnologías de vanguardia, desarrollando las infraestructuras inteligentes necesarias para las cadenas de distribución con etiquetas RFID, V0IP entre empresas y distribución de contenidos y datos para teléfonos móviles. VeriSign trabaja con empresas de telecomunicaciones que buscan desarrollar nuevos servicios rápidamente y que necesitan servicios exhaustivos y proactivos de seguridad y líderes del sector del comercio electrónico que desean dotar de mayor seguridad a los procesos de pagos y reducir los niveles de fraude. Para muchas empresas en todo el mundo, VeriSign es un punto de encuentro.

b. <u>Características del producto</u>

El producto comercializado para brindar los Servicios de infraestructura de clave pública administrada por Verisign pone en el mercado es su **Managed PKI**, este producto permite a las empresas dotar de seguridad a sus aplicaciones y a su infraestructura de redes mediante transacciones y comunicaciones autenticadas, privadas y no rechazadas. Managed PKI de VeriSign, la piedra angular de la autenticación fuerte de VeriSign, permite a los clientes desembarazarse de la emisión de certificados digitales y de tareas administrativas tales como la *generación, validación, renovación y revocación de certificados digitales.*

Los servicios de Managed PKI se proporcionan a través de la infraestructura de clave pública de VeriSign, de nivel militar, y de sus centros de operaciones en red, lo que asegura una expansión, administración y seguimiento continuo 24 horas al día, 7 días a la semana, 365 días al año y en todo el mundo.

Entre algunos de los objetivos generales los servicios que proporciona Verising, es de proporcionar a sus clientes la confiabilidad de integrarse con sus socios comerciales, proporcionar acceso seguro

a los usuarios, asegurar la continuidad de los negocios, y cumplir con la normativa gubernamental, para esto entre algunas de las características más importantes se pueden anotar las siguientes:

1. Mecanismo de autenticación común para múltiples aplicaciones:
    a. Mensajería de confianza (Microsoft Exchange, IBM® Lotus Notes®, AOL® Instant Messenger™)
    b. VPN segura (Check Point, Cisco y Nortel Networks)
    c. Autenticación de dos factores (Aladdin™, Authenex™, ActivCard®, Schlumberger™)
    d. Formularios seguros (Adobe®, Evincible™)
    e. Servicios web (servicio Trust Gateway de VeriSign®)
2. Host local:

    El cliente puede localizar, identificar y albergar páginas de inscripción de usuarios finales.
3. Gestión completa de la vida útil del certificado:

    El centro de control de VeriSign® proporciona a los administradores de la empresa el control completo para inscribir, aprobar, revocar y renovar los certificados digitales.
4. Métodos de autenticación flexibles:
    a. Autenticación manual
    b. Autenticación mediante passcode
    c. Administración automatizada
5. Entidad emisora de certificados integrada:
    a. Infraestructura de entidad emisora de certificados integrada y operada por VeriSign en nombre del cliente
    b. Funcionamiento continuo del centro de datos de VeriSign®
    c. Recuperación de desastres
6. Programa de asistencia Gold Support de VeriSign®:

a. Contratos de prestación de servicios con el programa opcional de garantía NetSure®de VeriSign®

Entre algunos de los servicios, funcionalidades y consideraciones significativas que se deben considerar de este producto se presentan a continuación:

1. Autenticación a los usuarios internos y externos
2. Aseguramiento de intercambio de datos seguros en línea, las transacciones y las comunicaciones.
3. Aseguramiento de las aplicaciones de intranet, extranet e Internet a la vez que permite una interacción fluida con los socios comerciales.
4. Establecer rápidamente una sólida infraestructura de clave pública y un sistema de entidades emisoras de certificados (AC), al mismo tiempo que se reduce la carga del desarrollo, del mantenimiento y de la supervisión de PKI.
5. Las empresas conservan el control total de la política de seguridad, los modelos de autenticación, y la gestión de la vida útil del certificado.
6. Permite la interoperabilidad con casi cualquier aplicación o dispositivo y está integrado previamente con las soluciones líderes listas para su uso[31].
7. Reducir el coste y la complejidad de las implementaciones PKI a la vez que proporcionan servicios avanzados y de confianza de la autenticación, la codificación, la firma digital y el no rechazo, dentro y fuera de la empresa.
8. Desarrollado sobre estándares abiertos para asegurar la máxima flexibilidad

4.3. Productos de PGP Corporation.

a. Antecedentes de la empresa

PGP Corporation es una empresa creada en 1991 por Phil Zimmermann creador del programa Pretty Good Privacy o PGP (privacidad bastante buena) cuya finalidad es proteger la información distri-

[31] Existe un convenio entre Verising y Microsoft para integrar Managed PKI a Microsoft Windows Server 2003.

buida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

Curiosamente esta herramienta fue diseñada como una herramienta para los derechos humanos, se publicó gratis en la Internet en 1991. Esto convirtió a Zimmermann en el objetivo de una investigación criminal que duró tres años, debido a un trasfondo en asuntos de política militar lo que a la larga incrementaría su interés en la parte política de la certificación; el gobierno americano advirtió que las restricciones estadounidenses de exportación para software de encriptación fueron violadas cuando PGP se extendió por todo el mundo. A pesar de las carencias, PGP se convirtió en el software de encriptación de correo electrónico más extensamente utilizado en el mundo. Después de que el gobierno dejara el caso en 1996, Zimmermann fundó PGP Inc. Esta compañía fue adquirida por Network Associates Inc (NAI) en diciembre de 1997, donde permaneció durante tres años como uno de los más importantes socios. En agosto de 2002 PGP fue adquirido de NAI por una compañía llamada PGP Corporation, donde ahora Zimmermann sirve como asesor especial. Zimmermann usualmente es asesor para un número de compañías y organizaciones industriales en cuestiones de criptografía, y es además socio en Stanford Law School's Center for Internet and Society (Centro de Enseñanza de Derecho de Stanford para Internet y la Sociedad).

Además de los premios por las versiones de PGP desarrolladas antes de que Zimmermann empezara en una compañía, las subsiguientes versiones de PGP de perfeccionamiento por el equipo de ingeniería de la compañía siguen siendo reconocidas cada año por muchos otros premios industriales.

b. Características del producto

PGP Universal Server

La serie universal del PGP proporciona cifrado integrado, end-to-end para las empresas, provee de organizaciones de una solución centralizada de fácil comprensión, utilizando una poderosa herra-

mienta de encriptación en muchos utilitarios. PGP Universal Server asegura el tráfico y la comunicación de mensajería interna así como también entre socios internos y externos a la empresa. Además la serie universal del PGP proporciona seguridad completa, permite la administración centralizada de las políticas de la seguridad.

PGP Universal Server provee toda la funcionalidad de un servidor de llaves, generándolas y administrándolas de una manera fácil y eficiente.

PGP Verified Directory

El PGP Verified Directory ha sido desarrollado en base a la funcionalidad de un servidor de llaves públicas provee de una simple e intuitiva interfase que permite manejar las llaves de los usuarios.

El PGP Verified Directory permite la actualización automática de las llaves internas de los usuarios a los directorios públicos para la verificación de los mismos.

4.4. Productos de Adexus (RSA)

a. Antecedentes de la empresa

La misión de RSA es ayudar a organizaciones a estructurar esquemas de seguridad de información, asegurando sus infraestructuras, protegiendo su información sensible, y manejando esta información así como también los acontecimientos de seguridad para garantizar la satisfacción y seguridad de los clientes.

La fácil administración del control de las identidades, así como el cifrado, la seguridad de la información y la protección antifraude, hacen que la gerencia tome un rol positivo en la empresa, a su vez brindan de confianza a todos los usuarios, transacciones y datos que se manejen en la Infraestructura.

Esta empresa provee también de un sin número de estrategias que se ajustan a las necesidades de las empresas o instituciones, uno de los pilares fundamentales es el robusto cifrado y la verificación

de la identidad que es la principal preocupación, además de las mejoras operacionales y un sin número de ventajas que el usuario puede aprovechar.

b. Características del producto

El producto utilizado para brindar los servicios de certificación digital se enumeran a continuación, el **RSA Keon Certification Authority** se constituye como aplicación de administración de certificados digitales, la cual es elemento base para la operación de la entidad certificadora. Los módulos que lo componen son:

- RSA Keon CA (Certificate Authority)
- RSA Keon Registration Authority
- RSA Keon Recovery Module
- RSA Keon WebSentry

RSA Keon CA (Certificate Authority)

Genera, administra y valida certificados digitales. La aplicación incluye servidores seguros de administración, inscripción, directorio y bitácoras, así como un servidor SCEP que provee inscripción automática para dispositivos VPN que operan con dicha norma. También provee un robusto modulo que firma digitalmente certificados y eventos de sistema, un repositorio integrado para almacenar los certificados, datos de sistema e información sobre el estado de los certificados. Puede publicar sus certificados a cualquier directorio que satisfaga las normas LDAP, e incorpora un servidor que opera con el protocolo OCSP para suministrar la capacidad de revisión en línea del estado de los certificados.

Un producto de RSA Security empresa líder mundial en seguridad informática.

Provee de todos los elementos esenciales para establecer un ambiente de seguridad robusta:

- Autentificación fuerte
- Confidencialidad de datos

- Integridad
- Autorización
- No repudio

RSA Keon Registration Authority

Ambiente integrado con RSA Keon Certificate Authority que facilita el proceso de solicitud de certificados para grandes volúmenes de requerimientos.

Es responsable de la verificación de antecedentes de los solicitantes y la diseminación de los certificados emitidos.

Permite realizar una distribución geográfica de los centros de enrolamiento al soportar múltiples entidades de registro, instaladas en forma local o remota. La cercanía del proceso de aprobación con los usuarios minimiza el riesgo de emitir certificados al individuo o instituciones no autorizadas.

RSA Keon Recovery Module

Componente opcional, orientado al almacenamiento y recuperación segura de las claves privadas de encriptación de los usuarios, como solución a los problemas de pérdida o de daño. Esto permite la recuperación de datos en situaciones de emergencia y satisfacer los requerimientos de algunas entidades reguladoras.

Opera en combinación con equipos especializados para la generación y distribución segura de claves, así como soporta un proceso de recuperación de claves privadas en colaboración, basado en tarjetas inteligentes. El proceso de recuperación del tipo “m” de “N” significa que se requiere la participación de al menos M personas (y sus certificados) de un conjunto total de N supervisores, para autorizar la recuperación de la clave privada de un usuario.

RSA Keon WebSentry

RSA Keon WebSentry es un módulo incorporable a los sitios web orientados a comercio electrónico y otras transacciones seguras. Provee la habilidad de validar en forma instantánea sus certificados antes de permitir a los usuarios la realización de transacciones o el acceso a archivos protegidos.
Cuando un usuario intenta acceder una pagina Web o archivo protegido se verifica en tiempo real su certificado contra la entidad certificadora.

4.5. Estado del Arte en Ecuador

a. Las Tecnologías de Información en Ecuador

Las Políticas Públicas se entienden como la institucionalización de objetivos nacionales definidos para atender necesidades públicas. Se concretan a través de estrategias de referencia y actividades operativas permanentes. En el ámbito de las Tecnologías de Información y Comunicación, los objetivos nacionales son diversos y corresponden al modelo de sociedad decidido por las naciones y sus gobiernos.

Desde una perspectiva de sociedad civil, las políticas públicas son relevantes porque constituyen uno de los instrumentos socialmente disponibles para atender las necesidades de la población. En este sentido, la visión de política pública que se quiere enfatizar en este proyecto es el de dar una visión instrumental, de "medio para", la resolución de los problemas sociales.

Al referirse a las políticas públicas para Internet, éstas actualmente están asociadas a procesos de desarrollo nacional. Sin embargo la realidad latinoamericana se caracteriza por su diversidad y ésta se manifiesta también en los distintos modelos de desarrollo adoptados en la región, los cuales responden a la diversidad de sus procesos de cambio, que se explican por la especificidad de las relaciones entre las estructuras históricas, la organización político-económica y la intervención de los actores sociales en el territorio de los distintos países.

Insistiendo, el enfoque de políticas públicas es instrumental y en el caso de las Tecnologías de Información y Comunicación (TICs), Internet incluida, éstas se presentan en nuestro continente en un documento llamado Agenda Digital o Agenda de Conectividad.[32]

El desarrollo de los servicios de valor agregado, entre ellos la Internet, esta estructuralmente vinculado con el de las telecomunicaciones. Que al momento, se observa que el sector se encuentra estructurado bajo las orientaciones de los procesos de modernización que en los años 90 se introdujeron en los países latinoamericanos, con distintos matices y resultados, y que, en un sentido concreto, significaron la privatización de las empresas estatales y su transferencia a operadores particulares.

Sin embargo y en el marco de la diversidad y dinamia estructurales ya expuestos, los procesos modernizadores adquirieron diversas formas en el continente: desde la concreción efectiva de la transferencia de la propiedad y la operación a organizaciones privadas, hasta la transformación de las empresas públicas constituyéndolas como compañías anónimas, en las cuales la propiedad de las acciones societarias es del estado, como ocurre en el Ecuador.

En la región el sector de las telecomunicaciones ha sufrido una rápida transformación desde la situación de prestación en régimen de monopolio estatal de los servicios básicos, a un modelo liberalizado en el que se está abriendo el mercado de los servicios de telecomunicaciones, tanto básicos como avanzados, a la competencia. Sin embargo este proceso no es universal, efectivamente Uruguay, Costa Rica, Ecuador son excepciones a este proceso de apertura del mercado de telecomunicaciones.

Desde una perspectiva tecnológica, en los últimos años se ha producido una auténtica revolución en el sector de las telecomunicaciones debido al incremento de la capacidad de transmisión, la mayor inteligencia de la red, mediante la integración del software en los equipos de telecomunicaciones y el aumento de la capacidad de integración de los transistores. Los avances tecnológicos y sobre todo la digitalización, permite utilizar las mismas infraestructuras para prestar distintos servicios. Se

[32] *Proyecto a cargo del Consejo Nacional de Telecomunicaciones (CONATEL)*

pasa a utilizar la misma base tecnológica, con lo cual desaparecen las diferencias entre sectores próximos.

Las tecnologías de la información no son ellas mismas ni positivas ni negativas, pero tampoco son neutras. Toman la forma y dirección de las sociedades en las cuales se introducen y al mismo tiempo son factor fundamental en el modelado de las relaciones y modos de interacción en dichas sociedades. América Latina, por su cuenta, está compuesta por una multiplicidad de culturas e identidades, todas inscritas en sociedades en las cuales el acceso a los recursos, conocimiento y oportunidades están distribuidos injustamente. Aunque existen democracias formales en la mayoría de sus países, los gobiernos de América Latina son por lo general corruptos, elitistas y no muestran responsabilidad pública por sus actos y omisiones.

b. Penetración de la Internet en Ecuador

Con la incursión del desarrollo de las nuevas tecnologías, el poder determinar los índices de utilización de las TIC's ha sido un gran problema debido a la complejidad y la falta de metodologías adecuadas para la medición, es por esta razón que mucho se especulaba sobre el porcentaje de penetración de la Internet en el Ecuador, los porcentajes fluctuaban desde el 3% al 6%, pero en realidad no se podía terminar a ciencia cierta el verdadero valor.

Sin embargo, es hasta finales del primer semestre del 2006 que una comisión del programa Sociedad de la Información de la Comisión Económica para Latinoamérica y el Caribe (CEPAL) alertó al Consejo Nacional de Telecomunicaciones (CONATEL) para que tome cartas en el asunto, es así que se conformó un equipo técnico que tenían entre uno de sus retos el desarrollo de una metodología para determinar los indicadores de la sociedad de la información.

Entre algunos de los nuevos factores considerados en esta metodología son los usuarios por cada centro de conectividad (cibercafés, puntos de acceso y telecentros), que sumados a los ya anteriormente utilizados, número de usuarios de cuentas dial up y cuentas dedicadas.

Es importante mencionar también que Ecuador es el tercer país en temas de acceso colectivo[33], luego de Argentina y Perú.

Con la finalidad de proporcionar índices más precisos, el Consejo Nacional de Telecomunicaciones, prevé socializar su estudio para definir una metodología similar y medir el impacto de las tecnologías de información y comunicación en el país, además en coordinación con el Instituto Nacional de Estadísticas y Censos se planificará en el próximo censo poblacional varias preguntas relacionadas con las TIC's.

Cuadro 2. Penetración del Internet en el Ecuador.
Fuente: Superintendencia de Telecomunicaciones del Ecuador[34]

Mes	Cuentas Dial Up totales	Cuentas Dedicadas totales	Cuentas totales	Usuarios Dial Up totales	Usuarios Dedicados totales	Usuarios totales
Enero	106603	31976	138579	426412	121101	547513
Febrero	105515	32228	137743	422060	121295	543355
Marzo	103756	36983	140739	415024	120207	535231
Abril	106589	47080	153669	426356	250170	676526
Mayo	108765	48012	156777	435060	256053	691113
Junio	110372	50589	160961	441488	273228	714716
Julio	110089	50857	160946	440356	273964	714320
Agosto	109700	50894	160594	438800	274477	713277
Septiembre	115783	54287	170070	463132	287551	750683
Octubre	115354	54286	169640	461416	286510	747926
Noviembre	115195	54803	169998	460780	289743	750523

c. Gobierno Electrónico

Como diagnóstico general de la situación de Gobierno Electrónico ecuatoriano, así como de acceso general a TICS se puede afirmar que se encuentra en una etapa inicial, básicamente presencial.

Solamente uno de los trámites presenta algunas características de interacción, pero todavía mantiene varias etapas en las que el ciudadano tiene que dirigirse personalmente a las instalaciones públicas, por lo tanto se encuentra en una fase pre-electrónica. Este trámite es el Impuesto a las Rentas cuyo responsable es el Servicio de Rentas Internas[35].

[33] Estudio realizado por la CEPAL, Diario El Comercio, jueves 23 de noviembre del 2006, página 10
[34] http://www.supertel.gov.ec/telecomunicaciones/v_agregado/estadisticas/anual.htm
[35] SRI .- Sistema de Rentas Internas

Este trámite ha avanzado mucho, se ha modernizado considerablemente su retaguardia, pero todavía mantiene varias etapas necesarias de presencia física, por lo que por las comparaciones internacionales, no lo podemos considerar un trámite electrónico.

Lo mismo pasa con el proceso de apertura de empresas, que ha mejorado considerablemente, pero mantiene la mayor parte de las etapas, requerimientos y procedimientos, exigiendo la presencia física del ciudadano, lo que nuevamente lo elimina de una definición internacional de trámite electrónico.

En este caso concreto, el de apertura de empresas, notamos una gran resistencia al cambio, lo que limita notablemente la posibilidad de acción. Todavía Ecuador está lejos de llegar a los padrones internacionales más avanzados de abertura de empresas, que en general, dejan de requerir presencia física del ciudadano. En el caso de Ecuador, la presencia es necesaria en todas las etapas del trámite.

Los citados dos trámites porque han sido considerados la vanguardia del proceso de Gobierno Electrónico, pero a partir de las estudios realizadas en campo, se afirma que de hecho son dos procesos con poca posibilidad de cambio a corto plazo, por limitaciones institucionales.

En lo concerniente a la firma electrónica no existe aún una entidad certificadora usada como argumento central para el mantenimiento del trámite con fases presénciales, y su no evolución para el trámite electrónico. Pero durante la investigación se verifico que este argumento no es totalmente válido, una vez que en la práctica algunos de los países consultados utilizan formas de certificación digital seguras, que cuentan con las seguridades suficientes para que los trámites se realicen por medios electrónicos.

Los grandes sistemas electrónicos de Brasil, Chile, México, no exigen firma electrónica y si formas de seguridad en las transacciones. Por ejemplo, TODOS los trámites y procesos que son realizados en Brasil de forma electrónica no requieren la ley de firma digital, ya que ella no fue todavía aprobada en el país. Son ellos:

- Impuestos a la renta
- Impuesto a los Vehículos automotores (IPVA)
- Impuesto anual de licencia de vehículos (Licenciamiento de Vehículos)
- Certificados de denuncias electrónicas (Boletín de Ocurrencia)
- Votación Electrónica
- Certificados diversos

CAPITULO 5

DESARROLLO DEL PROTOTIPO

Durante el desarrollo del prototipo, se encontraron muchas dificultades al momento de poner las cosas en blanco y negro, debido a la gran cantidad de información y al no contar con procedimientos definidos que puedan orientar el camino a seguir, se desarrolló una **Metodología para el Diseño de una Infraestructura de Clave Pública**, para definir aspectos importantes dentro del prototipo propuesto, lo que permitió identificar y establecer con mayor claridad los requerimientos, servicios, herramientas y procesos de certificación.

Esta metodología se encuentra detallada en el Anexo A.

5.1. Análisis de Requerimientos

Es necesario tener muy claro el objetivo del desarrollo del prototipo, por lo que a continuación se define claramente el para que del mismo:

a. Objetivo y Alcance de la SBS AC

El **objetivo** principal del desarrollo de este prototipo es la de mejorar el nivel de seguridad en la transmisión de información de las diferentes entidades financieras a la Superintendencia de Bancos y Seguros, la aplicación de una infraestructura de llaves públicas permitirá mantener la confidencialidad, la integridad, la autenticidad y el no repudio en el envío y recepción de estructuras para su validación.

La aplicación a desarrollarse en Lotus Notes servirá, como un **sitio seguro**, donde los usuarios mediante la validación de los certificados entregados por la **SBS AC** podrán acceder y depositar sus estructuras, las cuales deberán ser tomadas por las aplicaciones para las validaciones correspondientes, el resultado de las mismas se las dará a conocer a las entidades por medio un correo electrónico el cuál será enviado firmado y encriptado.

Con la finalidad de cumplir con lo descrito anteriormente es necesario crear en la Superintendencia de Bancos y Seguros, la Autoridad de Certificación que se le denominará **SBS AC**, la misma que desempeñará también el rol de Autoridad de Registro y que tendrá a su cargo las funciones de generar, administrar, revocar y renovar los certificados emitidos a las entidades, así como también mantener el **CRL** actualizado.

b. Requerimientos de Diseño

La **SBS AC** tendrá la capacidad de generar n cantidad de claves o llaves públicas, las cuales se utilizarán para la firma digital, certificado digital y cualquier otra codificación, para el presente proyecto solo se expedirán llaves con el propósito de crear un ambiente seguro para el intercambio de información, esto con el objetivo de disminuir el riesgo, mejorar la seguridad y funcionalidad del prototipo.

- La arquitectura propuesta para el funcionamiento del prototipo se encuentra detallada en el capítulo 3 de este documento, es importante definir en este punto la responsabilidad en:
- Definición del tiempo de vida de la Autoridad SBS AC: diez años (10)
- Definición del tiempo de vida de los certificados para los clientes: cinco años (5)
- Niveles de Usuario: Debido a la diversidad en los aspectos tecnológicos de las entidades se ha definido tres niveles de usuario alto, medio y bajo considerando el desarrollo que estas tengan en el ámbito técnico, por lo general los bancos se encontrarán en el nivel alto, las compañías de seguro estarán en el nivel medio y cooperativas en el nivel bajo.

La generación, verificación y entrega se la realizará en forma centralizada, la administración de los certificados estará a cargo del administrador de la SBS AC, el que será dispuesto por las autoridades correspondientes.

Es importante mencionar también que, el diseño, adaptabilidad, escalabilidad, funcionalidad, seguridad entre otros aspectos se la ha realizado siguiendo los estándares y normalizaciones existentes.

A continuación se presentará una descripción detallada de la red y la ubicación de la Autoridad Certificadora: **Ver Figura 13 y 14**

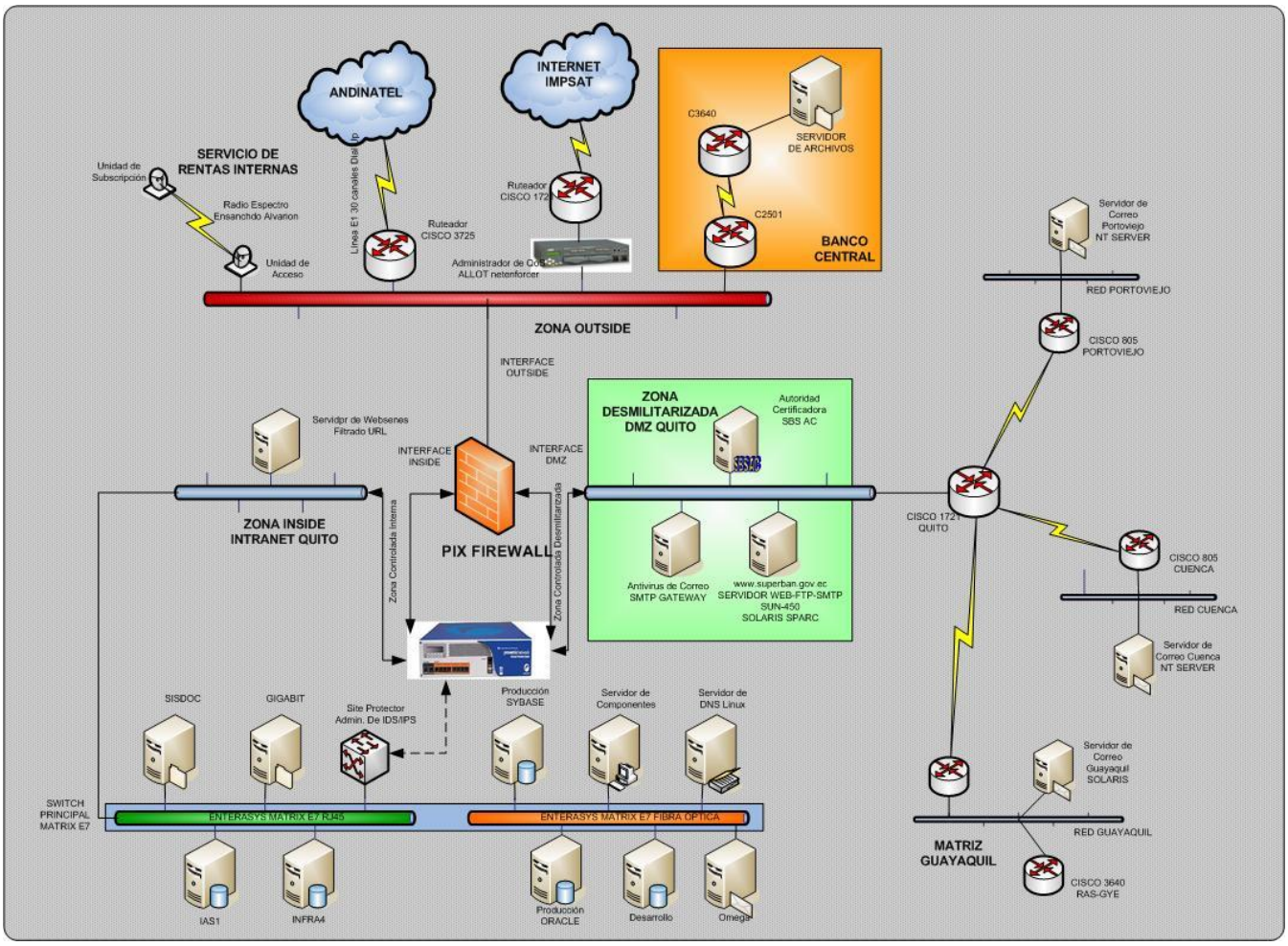

Figura 14. Diagrama de red, ubicación SBS AC.
Elaborado por: el autor

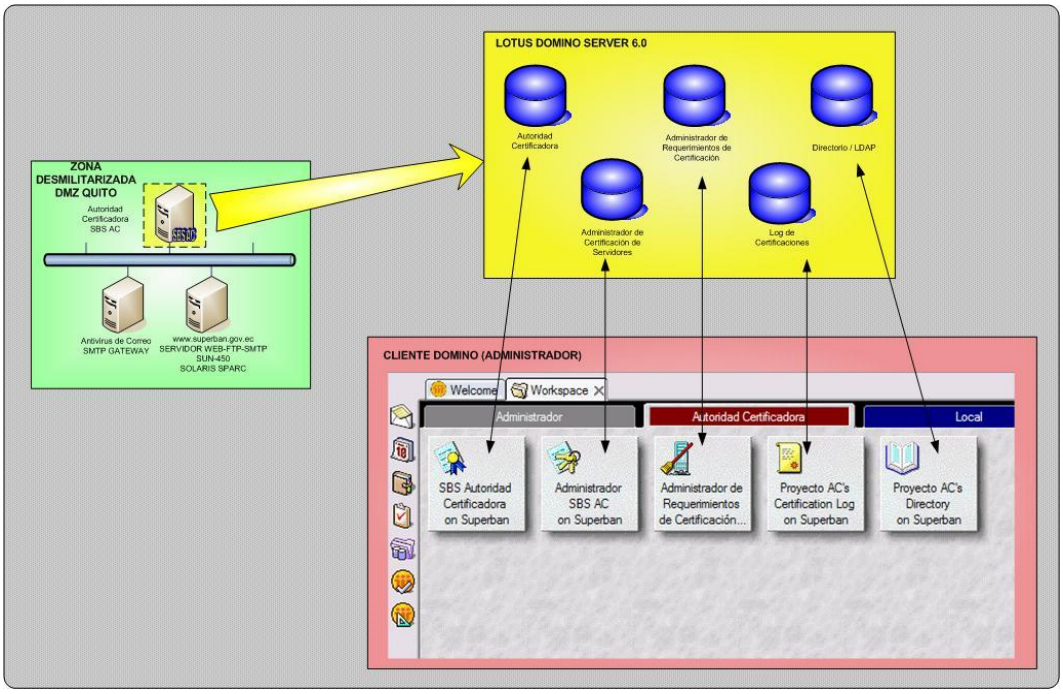

Figura 15. Estructura SBS AC
Elaborado por: el autor

c. Requerimientos del usuario

Como se anotó anteriormente existirán tres niveles de usuarios para los cuales se les deberá capacitar sobre conceptos criptográficos y sus herramientas, así como también los principios básicos de la Infraestructura de Llaves Públicas[36], esto permitirá una mejor compresión y utilización de la herramienta. Los planes de capacitación que se presentarán variarán en tiempo y complejidad dependiendo del nivel de usuario. El prototipo será transparente.

d. Requerimientos de Seguridad

Los requerimientos de seguridad que ostenta el prototipo se enfocan principalmente en cuatro aspectos primordiales:

1. Confiabilidad.- Toda la información generada en el proceso de Certificación y utilización de la PKI se la realizará bajo estrictos procedimientos de confidencialidad, enmarcados dentro de un marco legal,[37] el cual será elaborado para garantizar el normal funcionamiento del prototipo, es importante considerar también, que el alcance de este prototipo limita su uso a

[36] *Principios Básicos de la Infraestructura de Llave Pública. Capitulo 1*
[37] *Este marco legal deberá ser elaborado por un equipo multidisciplinario considerando aspectos legales, normativos y técnicos íntimamente relacionados.*

un grupo de usuarios con los que se realizarán pruebas sin ninguna implicación legal que comprometa a la entidad financiera o a la Superintendencia de Bancos y Seguros.

2. Integridad.- La información manejada en la PKI conservará las políticas y procedimientos utilizados en el servicio de mensajería y correo electrónico, ningún usuario podrá tener acceso a información para la cual no esté autorizado.
3. Disponibilidad.- Para mantener la disponibilidad de los procesos que involucran la certificación, será necesario elaborar los planes de contingencia.
4. Confianza.- La SBS AC estará ubicada físicamente dentro de la zona desmilitarizada del esquema de comunicaciones de la Institución, este esquema mantiene un alto nivel de seguridad con la utilización dispositivos de software y hardware, lo que permite brindar un nivel de confianza adecuado a los usuarios de la PKI.

5.2. Servicios Disponibles

Los servicios que se brindará la PKI son:

Obligatorios:

a. Servicios de manejo de llaves para firmas digitales
b. Servicio de manejo de certificados
c. Servicios de publicación y almacenaje de llaves, certificados y CRL

Opcionales:

d. Servicios de interfaz con el cliente
e. Servicio de no repudio
f. Servicio de entidad final

Los servicios que se han incorporado en el prototipo se enmarcan adecuadamente con lo descrito anteriormente, es importante manifestar que el grado de complejidad de la administración de estos servicios variará según la aplicación y la cantidad de información que se utilice.

A continuación, se describe con mayor detalle cada un de los servicios (obligatorios) que se prestarán en la Infraestructura de llave pública de la SBS.

a. Servicios de manejo de llaves para firmas digitales

Este es un servicio que es útil para el usuario final, así como también para el funcionamiento interno de la PKI, para firmar los certificados. Aquí aparece la autoridad certificadora denominada **SBS AC,** que se encargará de firmar con la llave secreta y verificar la firma con el certificado correspondiente. Algunos de los sub-servicios a tener en cuenta para firmas digitales son:

a. Aseguramiento de la integridad entre el que firma con la llave privada y el que verifica con la pública, considerando que una persona puede tener más de un certificado. Para este punto la SBS AC firmará y verificará los certificados a ser utilizados en cualquiera de las instancias de la Infraestructura.
b. Mecanismo de almacenamiento de las llaves. En la SBS AC se almacenará solo las llaves públicas (certificados), los usuarios instalarán la llave privada en su máquina en un lugar protegido y encriptado con una clave, este proceso será transparente para el usuario en los siguientes casos:
    - Recibe la llave privada en un disco, solamente tendrá que ejecutarla y todo el proceso será transparente para él, solo tiene que poner la clave.
    - En el caso de que el usuario haya solicitado el certificado por la red la llave se instalará automáticamente solicitándole su clave.
c. En lo referente a la generación de llaves, la SBS AC generará las llaves públicas utilizando los algoritmos RSA de 1024 bits, no se permitirá ninguna opción para que le usuario la pueda generar, esta tarea será de responsabilidad exclusiva de la SBS AC.
d. Lotus Notes posee bases de datos (extensión nfs) que permiten administrar los log de eventos y requerimientos efectuados, esto facilitará y mejorará la administración de los eventos que ocurren en la SBS AC.

b. Servicio de manejo de certificados

Los certificados son los documentos que distribuyen las llaves públicas, por lo tanto, deben manejarse tanto para firmas digitales como para confidencialidad, sin mencionar todavía certificados con diferentes políticas. Algunos de los sub-servicios a tener en cuenta para firmas digitales son:

e. Generación de certificados de llaves públicas para usuarios, lo hará la **SBS AC** estos certificados podrán ser de dos tipos, oficial y personal.

f. Publicación de certificados de firmas digitales, encriptado, Autoridad Certificadora y Generación de la lista de certificados revocados (CRL).- Para brindar estos servicios se configurarán directorios LDAP de lectura, que serán puestos a disposición de los usuarios.

1. Registro Inicial

El solicitante deberá complementar y enviar el formulario de solicitud de Certificado que estará a su disposición en el dirección de Internet: www.superban.gov.ec/autorida.nsf

El envío de estos datos solicitados en el formulario y el abono de las tasas de registro supondrá su consentimiento para ser registrado como solicitante de un certificado. Está solicitud no implica la obtención del certificado, se deberán cumplir los requisitos establecidas en las Políticas de Certificación.

Con el envío del formulario, el solicitante se compromete a comparecer ante la Autoridad de Registro (**SBS AR**) pudiendo ser este personal a cargo del Proyecto según previa coordinación.

La Autoridad de Registro le solicitará llenar una solicitud en el cual el solicitante escribirá información personal e información que lo acrediten como representante o funcionario de una entidad financiera.

La Autoridad de Registro (**SBS AR**) poseerá un documento donde se encuentren definidos los representantes de las entidades financieras que han sido designadas para el proyecto.

Una vez comprobado sus antecedentes, la Autoridad de Registro (**SBS AR**) enviará solicitud a la Autoridad Certificadora (**SBS AC**) para la generación del certificado, el cual estará disponible en un tiempo establecido no mayor a las 48 horas, ésta será entregada a la persona solicitante por algún dispositivo de almacenamiento definido por las personas a cargo del Proyecto.

2. Autenticación de la Identidad del Suscriptor

Para acreditar y garantizar la identidad del suscriptor, este deberá presentarse ante la Autoridad de Registro (**SBS AR**) con una fotocopia de su cédula de identidad y su original, fotocopia de la credencial de la Superintendencia de Bancos y Seguros y original, esto garantizará su Certificado el cuál quedará archivado en la Autoridad de Registro (**SBS AR**).

Es importante anotar, que para el uso legal del certificado emitido al suscriptor por parte de la Autoridad de Certificación, se debe considerar los puntos estipulados en el Capitulo II de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

3. Rechazo de la Solicitud

Si la Autoridad de Registro (AR) rechaza la solicitud enviada por el solicitante, se le enviará un documento electrónico informándole los motivos por el cual fue rechazada su solicitud.

4. Emisión de Certificados

Una vez aceptada la solicitud de certificado, la Autoridad Certificadora (la Autoridad de Registro (**SBS AC**) procederá a emitir el certificado.

La Autoridad Certificadora (la Autoridad de Registro (**SBS AC**) certifica que la llave privada generada para el suscriptor estará sólo en el medio en el cuál se haya designado por el Personal del Proyecto y que ésta no guarda copia alguna.

5. Entrega de Certificados

Los certificados serán entregados a las personas solicitantes por algún dispositivo de almacenamiento definido por las personas a cargo del Proyecto.

De manera independiente a la forma como se entregue el certificado se deberá determinar la persona que recepta el certificado.

Para la entrega del certificado se utilizará la aplicación desarrollada.

6. Publicación del Certificado

Una vez aceptado el certificado por el suscriptor, la Autoridad Certificadora (**SBS AC**) procederá a enviar a la Autoridad de Registro (**SBS AR**) el certificado público, el mismo que será instalado en el Repositorio de Certificados (LDAP), el que quedará de dominio público.

7. Contenido del Certificado X.509 V3 (Ver Figura 4)

- **Para el Emisor del Certificado**

Cuadro 3. Contenido de Certificados X.509 (versión 3)
Elaborado por: el autor

Campos	Descripción.
Nombre Común (CN)	Nombre a ser certificado
Organización o Compañía (O)	Nombre asociado con la Organización
Ciudad/Localidad (L)	Ciudad donde está localizado el CN
Estado/Provincia (SP)	Estado donde está localizado el CN.
País (C)	País donde está localizado CN.

Cuadro 4. Contenido de Certificados X.509 (versión 3) para certificación WEB.
Elaborado por: el autor

Campos	Descripción.
Nombre Común (CN)	Superintendencia de Bancos y Seguros
Nombre a ser certificado(O)	Proyecto SBS AC
Ciudad/Localidad (L)	Quito
Estado/Provincia (SP)	Pichincha
País (C)	EC

Cuadro 5. Contenido de Certificados X.509 (versión 3) para usuarios finales.
Elaborado por: el autor

Campos	Descripción.
Nombre Común (CN)	Superban.gov.ec
Nombre a ser certificado(O)	Proyecto SBS AC
Ciudad/Localidad (L)	Quito
Estado/Provincia (SP)	Pichincha
País (C)	EC

- **Para el Sujeto del Certificado**

Cuadro 6. Formulario para el solicitante del certificado.
Elaborado por: el autor

Campos	
Nombres	
Apellido Paterno	
Apellido Materno	
Cédula de Identidad	
Dirección	
Ciudad	
Cargo	
Departamento	
Correo Electrónico	
Repetir Correo Electrónico	

8. Extinción de Certificados

La extinción tendrá lugar cuando el personal del Proyecto de servicio de certificación constate algunas de las siguientes circunstancias:

1. Solicitud del titular del certificado.
2. Expiración del plazo de validez del certificado.

3. Según como lo establece el Art. 19 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que dice:

   "***Artículo 19.-*** *Extinción de la firma electrónica.- La firma electrónica se extinguirá por:*

   a) Voluntad de su titular;

   b) Fallecimiento o incapacidad de su titular;

   c) Disolución o liquidación de la persona jurídica, titular de la firma;

   d) Por causa judicialmente declarada.

   La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso."

9. Lista de Revocación de Certificados

La Autoridad de Registro publicará en el mismo repositorio la revocación de certificados, la cual quedará de dominio público.

Importante: Es importante señalar que estas políticas son utilizadas sin ninguna base legal para su aplicación, pero están elaboración está basada en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su respectivo Reglamento.

c. Servicios de publicación y almacenaje de llaves, certificados y CRL

Es el servicio que nos permite la distribución de certificados, así como otros datos de las personas u otras entidades funcionales que estén dentro de la Infraestructura. Este servicio debe:

a. Permitir que existan entradas a la base de datos para obtener los diferentes certificados con sus datos. Para cumplir con este sub-servicio Lotus Notes posee bases de datos de las que se puede obtener la información requerida.
b. Asegurarse que exista un solo nombre para cada objeto en la PKI, para esto la SBS AC mantendrá el control y la responsabilidad que garantizará el cumplimiento de este sub-servicio.

d. Servicios de interfaz con el cliente

Existen dos tipos de interfaces con los que se ha desarrollado el prototipo, estos relacionan a los administradores y usuarios con la SBS AC y las aplicaciones respectivamente. Entre las interfaces más utilizadas se encuentran las del administrador al momento de generar el primer certificado para la SBS AC, hay otra interfaz utilizada por los usuarios para solicitar los certificados y la última una interfaz que contiene un conjunto de funciones para que la aplicación pueda comunicarse con la SBS AC.

Otra de las interfaces que se debe considerar es la que se desarrollará como la aplicación segura donde se validará y certificará la autenticidad, integridad, no repudio y confidencialidad de las transacciones, estas deben proporcionar un mecanismo sencillo para permitir a usuarios menos experimentados un mejor y fácil entendimiento..

5.3. Definición de Herramientas y funciones para el desarrollo de los servicios

a. Instalación del Lotus Domino Server 6.0.2

IBM Lotus Domino Server proporciona una base multiplataforma para la colaboración y el e-business, con soluciones que van desde la mensajería empresarial hasta las transacciones basadas en Web, con todo el resto de posibilidades entre ellas. Este sistema de colaboración y mensajería de nivel empresarial está diseñado para maximizar la productividad del personal y sacar el máximo provecho de la experiencia y los conocimientos de individuos, equipos y comunidades ampliadas.

Esta herramienta ha sido utilizada como base del prototipo por la disponibilidad de las licencias y soporte técnico que posee la institución, además debido a su versatilidad y potencialidad soporta el marco técnico disponible para poder desarrollar el proyecto dentro de los requerimientos establecidos.

Dentro de las opciones de instalación como se muestra en el Anexo B, literal a se escogerá el tipo de instalación correspondiente al Domino Enterprise Server, ya que este dispone de un sin número de servicios que facilitan la implementación de varias plataformas entre algunas de ellas

podemos mencionar la plataforma de correo, servicios web, servicios de base de datos, autenticación Certificación, entre otros.

b. Instalación de Lotus Notes, Lotus Domino Administrador y Lotus Domino Designer.

Para poder administrar todo lo referente a la plataforma de correo y para el desarrollo de aplicaciones, es necesario la instalación de los módulos que se describen a continuación:

Lotus Notes.- Provee un cliente Lotus Domino seguro para e-mail, calendario, agendas de grupo y acceso a Web.

Lotus Domino Administrator.- Ayuda a construir e implementar rápidamente aplicaciones de colaboración en ambientes Lotus Domino.

Lotus Domino Designer.- Ayuda a construir e implementar rápidamente aplicaciones de colaboración en ambientes Lotus Domino.

Para cumplir con los objetivos propuestos estas tres herramientas son fundamentales, ya que como se muestra en el Anexo B, literal b, estas nos permitirán configurar el Lotus Domino Certificate Authority, atender los requerimientos de los clientes, diseñar y adaptar las plantillas disponibles por el servidor, entre otras.

c. Configuración del Lotus Domino Server 6.0.2

Antes de iniciar la configuración de la Autoridad Certificador SBS AC, es necesario configurar correctamente la plataforma de mensajería, para esto previamente es necesario determinar el nombre del Servidor, dominio, usuarios, bases de datos, directorios, llaves, certificados, entre otros.

Para una mejor comprensión favor remitirse al Anexo B, literal c.

d. Configuración de Lotus Domino Certificate Authority

Lotus Domino Certificate Authority es un módulo de la plataforma de correo Lotus Domino desarrollada por IBM, que soporta la infraestructura de PKI y mantiene los estándares de criptografía y comunicación.

En el Anexo B, literal d, se adjunta un documento para la configuración de la Autoridad Certificadora SBS AC.

Cada una de los servicios que lo requieran brindará una variante on-line y otra off-line.

e. Definición de políticas de administración y usuarios.

POLITICAS DE CERTIFICACIÓN

Las Políticas de Certificación (CP) son una descripción detallada de los distintos tipos de Certificados Seguros que emitirá la **SUPERINTENDENCIA DE BANCOS Y SEGUROS** a las Instituciones del Sistema Financiero del Ecuador que sean seleccionadas para formar parte de las pruebas en el prototipo.

Las Políticas de Certificación se enmarcan de conformidad a lo que dispone la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Ley No. 67. Registro Oficial Suplemento No. 557 de 17 de abril del 2002 y del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos para el uso de Certificación Digital por parte del Personal Interno de la Institución y posteriormente para el Sistema Financiero.

Estas Políticas de Certificación deberán estar a disposición de toda Persona Natural o Jurídica, que esté interesada en la adquisición de un Certificado Digital y que esté contemplada dentro del proyecto.

USUARIOS

En cuanto a los Certificados e-mail que la Superintendencia entregará, éste certificado permitirá hacer uso del correo electrónico de forma segura, es decir, permite cifrar y firmar correos electrónicos. Los mismos que permiten identificar a terceras personas que reconozca la misma Autoridad Certificadora (CA) como ente emisor de certificados.

Por ser este un Proyecto de Prueba, la validez legal de estos certificados es nula y sólo estarán dirigidos a ser utilizados en asuntos internos relacionados con el avance de la investigación de dicho Proyecto.

El uso de este tipo de certificado se limita para una única cuenta de correo, por lo que, sí un usuario posee varias cuentas, deberá solicitar un certificado para cada una de ellas.

En cuanto a la emisión de Certificados para el Sistema Financiero, serán emitidos de conformidad a las pruebas y al desarrollo del Proyecto.

Aplicabilidad

Los Certificados entregados por la Superintendencia podrán ser utilizados en las siguientes actividades:

- Firma de Correo Electrónico

  El receptor de un mensaje firmado con la llave privada puede utilizar la clave pública del emisor para verificar que este último ha usado su clave privada para firmar el mensaje. La llave pública del emisor deberá estar disponible en un sitio destinado para el efecto.

- Integridad de Correo Electrónico

  El uso de este sistema de claves asimétricas permite comprobar al receptor de un mensaje, que éste no ha sido alterado entre el envío y la recepción.

- Encriptación de Corro Electrónico

  El emisor podrá utilizar el servicio de encriptación que las personas a cargo del Proyecto lo definan, independientemente del algoritmo de encriptación usado, el usuario podrá encriptar el correo electrónico siempre que el receptor un certificado digital y el emisor lo tenga reconocido la clave pública de éste.

- Firmar y Comprobación de Firma de Documento

  El receptor podrá comprobar que el documento que ha sido enviado no ha sido modificado, alterado, repudiado, otros

- Usos no Autorizados

  Estos certificados no son medios de pago, sino que su finalidad es identificar a una determinada persona en un sistema de redes Intranet o Internet.

Estos certificados no son válidos para asumir responsabilidades económicas ni compromisos en nombre propio y en general no serán válidos para usos diferentes de los descritos en este documento.

Estos certificados no podrán ser alterados por los usuarios y deberán utilizarse tal y como son suministrados.

Recomendaciones Técnicas

Por ser Lotus Notes la plataforma utilizada para el uso de Correo Electrónico los protocolos de este deberán ser compatibles con protocolos, SMIME y HTTPS.

PROCESO DE CERTIFICACIÓN

Cuadro 7. Descripción del Proceso de Certificación.
Elaborado por: el autor

ORD.	ACTIVIDAD	RESPONSABLE	OBSERVACIÓN
1	Complementar y enviar el formulario de solicitud de Certificado	Solicitante	Formulario se encontrará disponible en la dirección de Internet: www.superban.gov.ec.
2	Cancelación del formulario	Solicitante	Se registra como solicitante de un certificado y no implica la acreditación del certificado
3	Presentación ante la Autoridad de Registro	Autoridad de Registro	Se solicitará al solicitante escribir una contraseña secreta para el uso de la llave privada
4	Comprobación de información	Autoridad de Registro	Comprobación de antecedentes
5	Solicitud Aceptada		
	5.1. Emisión de Certificado	Autoridad Certificadora	Con la información proporcionada por la SBS AR se generará el certificado para el solicitante
	5.2. Entrega de Certificados	Autoridad Certificadora	Se entregará al solicitante el cófigo del certificado generado por algún dispositivo seguro
	5.3. Publicación del Certificado	Autoridad Certificadora	El Certificado será registrado en el Repositorio de Certificados (Libreta de Direcciones)
	5.4. Extinción de Certificados	Autoridad Certificadora	Por: Solicitud del titular del certificado, expiración del plazo de validez del certificado y
			Según como lo establece el Art. 19 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
			Artículo 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por: a) Voluntad de su titular; b) Fallecimiento o incapacidad de su titular; c) Disolución o liquidación de la persona jurídica, titular de la firma; d) Por causa judicialmente declarada. La extinción de la firma electrónica no exime a su titular de las obligaciones previa-mente contraídas derivadas de su uso.
	5.5. Lista de Revocación de Certificados	Autoridad Certificadora	La SBS AC publicará los certificados revocados
5	Solicitud Rechazada		
	5.1. Envío de comunicación de la negación de la solicitud	Autoridad de Registro	Se enviará por correo electrónico o cualquier otro medio los motivos de la negación.
5	Envío de generación de certificados a la Autoridad Certificadora	Autoridad de Registro	Solicitud aprobada, plazo máximo para la generación 48 horas
6	Generación del certificado	Autoridad Certificadora	Una vez generado el certificado no quedará copia alguna de la solicitud (Formulario)
7	Autenticación de la Identidad del Suscriptor		
	7.1. Acreditación del Suscriptor	Autoridad de Registro	Deberá llevar una copia de la cédula y la original, esta documentación será archivada
Importante: Es importante señalar que estas políticas son utilizadas sin ninguna base legal para su aplicación, pero su elaboración se enmarca en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su respectivo Reglamento.			

5.4. Protocolos de Comunicación

En las **Figuras 13 y 14** se presentan los diagramas de red y comunicaciones propuestos, según el modelo OSI las capas 1, 2 y 3 (Nivel físico, de enlace de datos y red respectivamente) conforman la categoría de transporte de datos, los protocolos usados en estas capas serán heredadas y revisadas, con la finalidad de proveer de un adecuado nivel de seguridad.

En lo referente a la categoría de aplicaciones las capas 4, 5, 6 y 7 (transporte, sesión, presentación y aplicación respectivamente) se propone el uso de los siguientes protocolos:

- **Capa 4:** Nivel de Transporte se utilizará TCP/IP
- **Capa 5:** Nivel de Sesión se utilizará SSL
- **Capa 7:** Nivel de Presentación se utilizará HTTP, HTTPS, SSH.

5.5. Descripción de Entidades

SBS AC.- Es la Autoridad Certificadora y la raíz de confianza de la PKI (root), esta entidad será la responsable de generar y administrar el ciclo de vida de los certificados, definir procedimientos y políticas de certificación, autorizar a los usuarios finales de las entidades previa verificación de identidades.

Es importante mencionar que esta se constituye en muchos casos como una entidad abstracta al relacionarla con la herramienta tecnológica.

SBS AR.- La Autoridad de registro es la entidad encargada de receptar las solicitudes de los usuraos finales, esta previó el envío a la Autoridad Certificadora, verificará la identidad e información de los solicitantes, pudiendo así aprobar o negar la emisión del certificado.

De igual manera esta es una entidad abstracta pero que se encuentra administrada por el personal designado para cumplir con estas tareas.

Usuarios Finales.- Los usuarios finales son aquellos funcionarios o empleados de las instituciones financieras, que después de haber recibido la capacitación necesaria y que se encuen-

tran debidamente aprobados, están facultados para solicitar certificaciones, estas apegándose a lo que estipule las políticas y procedimientos emitidos por la SBS AC.

DIGRAMA DE RELACIÓN ENTRE LAS ENTIDADES Y EL PROCESO DE CERTIFICACIÓN

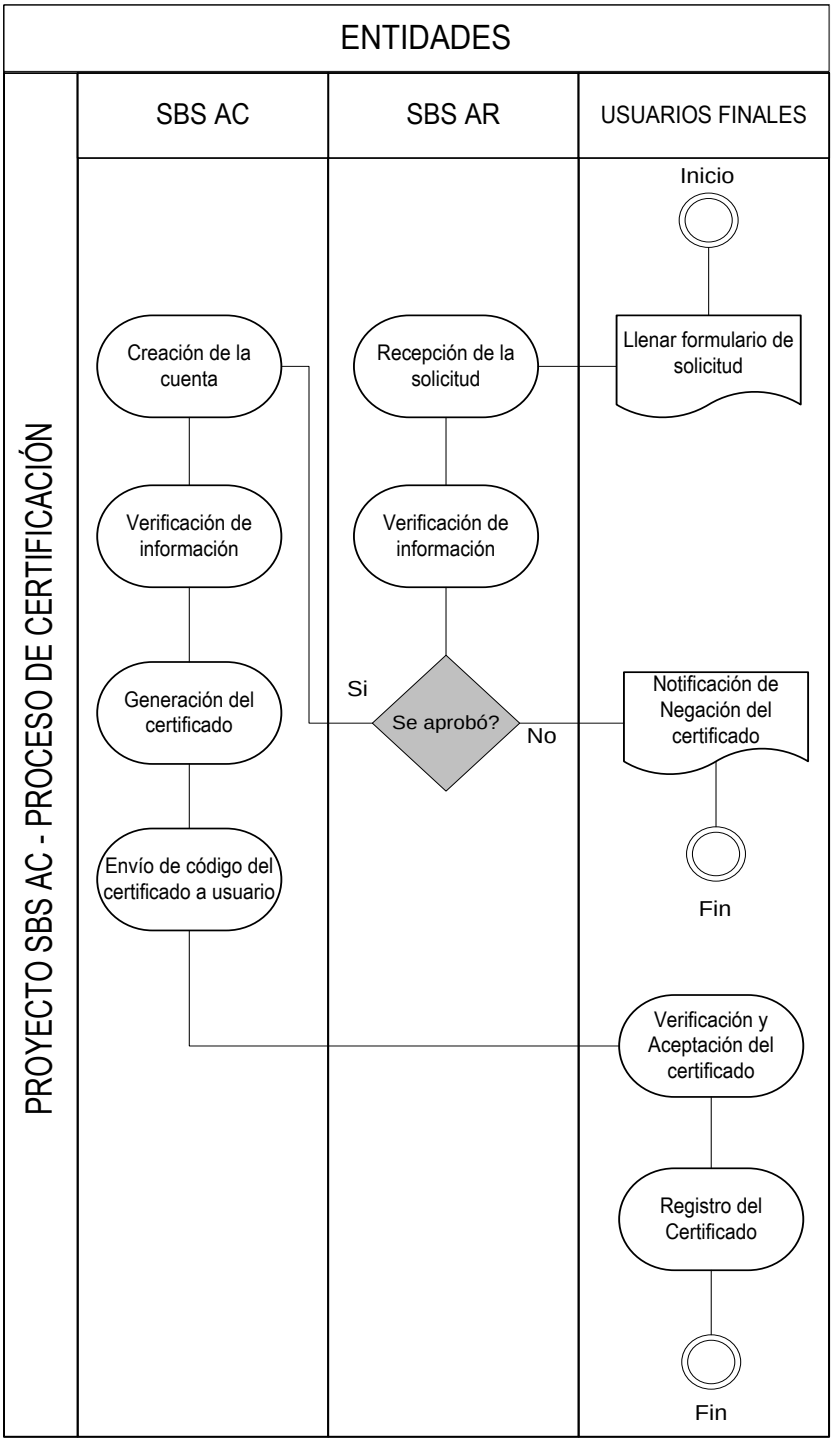

Figura 16. Diagrama de relación entre las entidades de la PKI.
Elaborado por: el autor

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- Como resultado final del estudio, se concluye que la falta de normalización de conceptos en cuanto a Firma Digital, Firma Electrónica, Criptografía, Seguridades, Infraestructura de Clave Pública así como la inaplicabilidad de leyes y reglamentos, constituyen barreras que dificultan la comprensión de conceptos importantes dentro de la Certificación Digital, esto limita la innovación de nuevas herramientas tecnológicas e inclusive afecta a la correcta y adecuada implementación de software desarrollado como base de estructuras e infraestructuras tecnológicas.
- El marco legal en los proyectos de desarrollo e innovación tecnológica se constituye en un aspecto fundamental, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, así como el Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación de Información y Servicios Relacionados, constituyen el marco jurídico necesario para el desarrollo e implementación de herramientas de innovación tecnológica.
- El conocer los esquemas de certificación utilizados en distintos países y empresas así como sus experiencias y dificultades en el tema, suministraron información de gran importancia al momento de definir el esquema propuesto, el cuál se ajusta a las necesidades y requerimientos técnicos y jurídicos para su funcionamiento.
- Otro aspecto significativo que se concluye, es la importancia que tienen el uso del software en la Infraestructura de Clave Pública, ya que este constituye la base fundamental de la administración de un esquema de certificación digital, por tal motivo las empresas dedica-

das al desarrollo de estas herramientas, pretenden normalizar y estandarizar sus productos para brindar sencillez, flexibilidad y compatibilidad.

- Si bien es cierto el prototipo desarrollado posee las características principales para la ejecución de un proceso de certificación, esta herramienta de software al no ser desarrollado específicamente para el negocio, mantiene las limitaciones en cuanto a flexibilidad, sencillez y compatibilidad, así como también en algoritmos criptográficos y periodos de validez de certificados.

6.2. RECOMENDACIONES

- Se recomienda la utilización de firmas electrónicas y certificados digitales como mecanismos que puedan dar validez a un documento enviado por medios electrónicos cuando el remitente y el destinatario no se relacionan de forma física.
- Es importante impulsar las nuevas tecnologías de información y comunicación en países latinoamericanos, ya que ellas van cambiando nuestras vidas sin darnos cuenta y marcan un nuevo sendero en el ámbito profesional, generando así oportunidades que deben ser aprovechadas oportunamente para que sean un aporte efectivo para el desarrollo de nuestros pueblos.
- Es importante utilizar las nuevas tecnologías en el gobierno por cuanto esto permitirá, aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y proveer a las acciones del gobierno de un marco mucho más transparente en el control del Sistema Financiero.
- Finalmente, se recomienda enfocar los esfuerzos prácticos de implementar tecnologías de seguridad y certificación digital en las transacciones del gobierno, considerando que existe

el marco legal necesario para su ejecución, de igual forma se conoce de experiencias similares en otros países que han dado excelentes resultados.[38]

[38] *Administración del Canal de Panamá, Superintendencia de Bancos de Panamá, Bolsa de Valores de Chile.*

REFERENCIAS BIBLIOGRÁFICAS

- **"Plan Estratégico Institucional 2005 – 2008 de la Superintendencia de Bancos y Seguros"**, Edición 2005.
- **"Comercio Electrónico y Firma Digital",** Dr. Mauricio Devoto, Editorial La Ley S.A., Buenos Aires – Argentina, 2001, 486 págs.
- **"Domino Certification Authority and SSL Certificates"**, IBM Corporation, International Technical Support Organization, First Edition (November 2000), 74 págs, /www.ibm.com/redbooks.
- **"TECNICAS DE PROTECCIÓN CONTRA PIRATERÍA EN DISCOS COMPACTOS",** Ing. Ana Azucena Evangelsta, Tesis de Maestría en Ciencias, Telemática, página 31

LINKOGRAFÍA

- *http://en.epochtimes.com/news/7-1-11/50336.html*
- *http://www.schneier.com/blog/archives/2005/02/sha1_broken.html*
- *http://www.ietf.org/ids.by.wg/pkix.html*
- *http://www.rsa.com/rsalabs/html/standards.html*
- *http://www.verising.com*
- *http://www.csi.map.es/csi/tecnimap/tecnimap1998/sp7.htm*
- *www.entrust.net*
- *http://www.supertel.gov.ec/telecomunicaciones/v_agregado/estadisticas/anual.htm*
- *http://www.sri.gov.ec*

ANEXO A

METODOLOGÍA PARA EL DISEÑO DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA

INTRODUCCIÓN ---------- **¡ERROR! MARCADOR NO DEFINIDO.**

PROPÓSITO Y FUNCIONALIDAD ---------- **¡ERROR! MARCADOR NO DEFINIDO.**

PUNTOS IMPORTANTES EN EL DISEÑO DE UNA PKI ---------- **¡ERROR! MARCADOR NO DEFINIDO.**

1.- Análisis de los requerimientos iniciales. ----------***¡Error! Marcador no definido.***

a. Objetivo y Alcance de la PKI----------***¡Error! Marcador no definido.***

b. Requerimientos de Diseño----------***¡Error! Marcador no definido.***

c. Requerimientos de Usuario----------***¡Error! Marcador no definido.***

d. Requerimientos de Seguridad ----------***¡Error! Marcador no definido.***

2.- Descripción de los servicios disponibles.----------***¡Error! Marcador no definido.***

a. Servicio de manejo de llaves para firmas de certificados ----------***¡Error! Marcador no definido.***

b. Servicio de manejo de certificados ----------***¡Error! Marcador no definido.***

c. Servicios de publicación y almacenaje de llaves, certificados y CRL-----***¡Error! Marcador no definido.***

d. Servicios de interfaz con el cliente----------***¡Error! Marcador no definido.***

3.- Diseño de herramientas y funciones para el desarrollo de los servicios de PKI. ----- ***¡Error! Marcador no definido.***

4.- Protocolos de comunicación.----------***¡Error! Marcador no definido.***

5.- Descripción de las entidades. ----------***¡Error! Marcador no definido.***

Introducción

Durante el desarrollo del proyecto se fueron presentando algunos inconvenientes relacionados con la definición de elementos, procedimientos, políticas, entre otros aspectos relevantes y necesarios para la conformación de la Infraestructura de Clave Pública propuesta.

Debido a la falta de empresas privadas e instituciones públicas que hayan incursionado en el desarrollo de nuevas tecnologías en el campo de la certificación digital, se presenta una brecha tecnológica al momento de plasmar los conceptos teóricos en la práctica.

Por este motivo, la metodología que aquí se presenta pretende atacar esta brecha, proporcionado y delineando puntos importantes al momento de diseñar una Infraestructura de clave pública, sin lugar a duda esto no constituye en ningún momento una camisa de fuerza ni un estándar que pueda ser aplicado en cualquier negocio, al contrario está es una pequeña guía que ha servido para complementar el estudio realizado.

Propósito y Funcionalidad

Una infraestructura de clave pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

Las operaciones criptográficas de clave pública, son procesos en los que se utilizan unos algoritmos de cifrado que son conocidos y están accesibles para todos. Por este motivo la seguridad que pueden aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o Políticas de seguridad aplicados.

Es muy importante tener muy claro que la implementación de una infraestructura de PKI no asegura completamente la seguridad, refiriéndose a la integridad, autenticidad, no repudio y confidencialidad,

la definición de procedimientos sencillos, claros y concretos, reforzadas por políticas y herramientas de software, así como el correcto cumplimiento y uso de los mismos, provee de una herramienta eficiente para el uso de transacciones informáticas y un sin número de aplicaciones.

Puntos Importantes en el diseño de una PKI

Entre los puntos más significativos e importantes que se consideran como fundamentales para enmarcar el diseño de una PKI se enumeran los siguientes:

1.- Análisis de los requerimientos iniciales.

a. Objetivo y Alcance de la PKI

Este es uno de los puntos más críticos en la elaboración de la infraestructura, definir el objetivo que persigue la Infraestructura de clave pública y su alcance influirá en cada uno de los aspectos posteriores al diseño e implementación de la PKI.

Es recomendable analizar detenidamente todos los aspectos relacionados con la PKI, tales como legales, operativos, técnicos y arquitectura, ya que estas proveen pautas substanciales, ya que con estas se podrá definir bases sólidas en la elaboración de los proyectos.

b. Requerimientos de Diseño

No existe un diseño genérico de infraestructura de llaves públicas, porque cada red y cada lugar que lo necesita tiene sus propios requerimientos, restricciones y características. Es necesario analizar en este momento si existen restricciones de usos de algoritmos y estándar criptográficos; requerimientos en cuanto al tiempo de vida de las llaves, niveles de usuarios; exigencias del manejo de entrega de certificados (puede ser que se exija una entrega centraliza, o en ciertas zonas de la red, etc. influyendo esto en el diseño de la distribución de certificados); exigencias de manejo de la BD de certificados; adaptabilidad, interoperabilidad con externos PKI; restricciones de costo, de velocidad, entre otras que pueda imponer las características de la red. Es necesario tener una descripción detallada tanto física como lógica de la red en cuestión

c. Requerimientos de Usuario

Según el tipo de usuario que actuará sobre el PKI serán los requerimientos de su diseño, pueden existir usuarios que conocen a perfección los conceptos criptográficos y sus herramientas, mientras otros necesitan el proceso lo más transparente posible. Es importante recordar que usuarios de PKI pueden ser tanto personas, como software.

d. Requerimientos de Seguridad

Independientemente de los objetivos con que se diseñe el PKI (autenticidad, integridad, no-repudio y confidencialidad), existen algunos requerimientos de seguridad[39] que deben cumplir cualquier PKI y que hay que tener en cuenta en esta primera fase de requerimientos iniciales pues a lo largo del diseño se introducirán aspectos que lo aseguran estos requerimientos, estos son:

Confiabilidad de la información que el PKI maneja, como por ejemplo las llaves , certificados y mensajes.

Integridad de la información que el PKI maneja.

Disponibilidad continua y el tiempo de recuperación con respecto a compromisos, robos o ataques debe ser corto.

Confianza: Debe tener un nivel aceptable de seguridad y no afectar la vulnerabilidad de sistemas individuales cuando se enlacen con el PKI. Los riesgos no pueden ser mayor que un sistema similar en papel.

Estos requerimientos se irán logrando a lo largo del diseño.

2.- Descripción de los servicios disponibles.

a. Servicio de manejo de llaves para firmas de certificados

Este es un servicio que es útil para el usuario final, así como para el funcionamiento interno de la PKI, para firmar los certificados. Aquí aparece entonces una entidad que llamaremos **Autoridad Certificadora** que se encarga de firmar con la llave secreta y verificar la firma

[39] El diseñador puede incluir los suyos pero no deben faltar los que se mencionan.

con el certificado correspondiente. Esta entidad estará presente por lo tanto en los usuarios y en los servidores de PKI.

Algunos de los sub-servicios a tener en cuenta para el manejo de llaves para firmas digitales son:

- ❖ Asegurar la integridad entre el que firma con la llave privada y el que verifica con la pública (hay que tener en cuenta que una persona puede tener más de un certificado).
- ❖ Mecanismo de almacenamiento de llaves privadas
- ❖ Proveer un medio para archivar las llaves de verificación de firma (certificados).
- ❖ Proveer de un medio para recuperación de las llaves de verificación de firma en caso de pérdida o no haberla recibido antes.
- ❖ Proveer un medio de revocación de certificado que garantice que la llave de firma no está comprometida, cuando se está verificando.
- ❖ Crear un mecanismo de logs de las acciones que se ejecutan en todas las entidades.

b. Servicio de manejo de certificados

Los certificados son los documentos que distribuyen las llaves públicas, por lo tanto , deben manejarse certificados tanto para firmas digitales, como para confidencialidad, sin mencionar todavía certificados con diferentes políticas. Algunos de los sub-servicios que se deben tener en cuenta son:

- ❖ Generación de certificados de llaves públicas para firmas que se enlacen correctamente con las Autoridades Certificadoras.
- ❖ Generación de certificado para autoridades certificadoras AC
- ❖ Generación de la lista de certificados revocados (CRL).
- ❖ Publicación de los certificados de firmas digitales, encriptado, AC y la CRL.
- ❖ Proveer las facilidades que se necesiten para interrelacionarse con otros PKI.
- ❖ Proveer un mecanismo de auditoria de cada uno de los pasos que se realicen.

- ❖ Proveer un mecanismo cómodo para verificar certificados.

c. Servicios de publicación y almacenaje de llaves, certificados y CRL

Es el servicio que permite la distribución de certificados, así como otros datos de las personas u otras entidades funcionales que estén dentro de la PKI. Este servicio debe: permitir que existan entradas en las BD para obtener los diferentes certificados con sus datos, asegurarse que existe un solo nombre para cada objeto en la PKI, brindar servicio de directorio confidencial con entrada autorizada (que no tiene sentido con la CRL) pero sí con alguna información personal, brindar un directorio externo para que personas fuera del PKI puedan obtener información y además debe mantener un control estricto sobre la modificación de la información, garantizando siempre que sea el personal autorizado.

d. Servicios de interfaz con el cliente

Este servicio permite definir y llevar un correcto mantenimiento de las aplicaciones con las que interactúan las entidades o usuarios finales, en muchas herramientas de software estas aplicaciones se encuentran predefinidas, pero debido a su concepción y estandarización permiten la personalización de las mismas lo que se constituye en un aspecto positivo al adquirir las herramientas.

3.- Diseño de herramientas y funciones para el desarrollo de los servicios de PKI.

Es el momento de describir las funciones y herramientas necesarias para cada servicio y así como incluir el diseño de otras funciones que garantizan el buen funcionamiento de la PKI y los servicios en general, como pueden ser: funciones de protección, backup y protección de los movimientos por la red.

4.- Protocolos de comunicación.

Para definir los protocolos de comunicación que existirán entre las entidades de la PKI. Como ya han sido expuestos todos los servicios y sus funciones, conocemos las necesidades de cada uno de

ellos, por tal razón es necesario revisar los conceptos de lo que significa un Protocolo de Comunicación.

También conocido como Protocolo de red *es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.*[40]

Según la **OSI**[41] la comunicación entre dispositivos se puede clasificar en 7 niveles o capas, o a su vez en dos categorías, la de aplicación (Incluyen los niveles 7, 6, 5,y 4) y transporte de datos (3, 2 y 1).

En este punto, según las categorías descritas anteriormente debemos describir los protocolos que se utilizarán para la comunicación en la Infraestructura de clave pública, haciendo énfasis en los protocolos que brindarán algún tipo de seguridad que darán valor agregado a la PKI.

5.- Descripción de las entidades.

Según los estudios realizados de los Principios Básicos de la Certificación Digital, así como también los elementos que componen una PKI, se definen como imperativas a las siguientes entidades: Autoridad Certificadora, Autoridad de Registro y entidades o usuarios finales.

De acuerdo a la complejidad de los proyectos se definen como entidades complementarias a las siguientes: Entidad generadora de llaves, entidad tercera de confianza, entre otras.

Describir claramente cada una de las entidades que participarán en el proyecto así como también sus funciones darán un soporte al diseñador para enfocar mucho mejor como se ha dividido el diseño e incluso en el caso del desarrollo será un gran apoyo para el diseño de clases y módulos. Esto permite encontrar si hay tareas que no están bien definidas y que no tiene claro que entidad las realiza.

Es recomendable adjuntar un diagrama de flujo de nivel 0 de la relación de las entidades en el proceso de certificación.

---

[40] *http://es.wikipedia.org/wiki/Protocolo_de_red*

[41] *Organización Internacional para la Estandarización*

ANEXO B

INSTALACIÓN Y CONFIGURACIÓN DEL PROTOTIPO EN LOTUS

a. Instalación del Lotus Domino Server 6.0.2
b. Instalación de Lotus Notes, Lotus Domino Administrador y Lotus Domino Designer
c. Configuración del Lotus Domino Server 6.0.2
d. Configuración de Lotus Domino Certificate Authority

ANEXO C

MARCO LEGAL ECUATORIANO[42]

1. "Constitución Política de la República del Ecuador", codificada y aprobada el 5 de junio de 1998,

2. "Ley General de Instituciones del Sistema Financiero", esta codificación fue elaborada por la Comisión de Legislación y Codificación de acuerdo con lo dispuesto en el numeral 2 del artículo 139 de la Constitución Política de la República el 10 de enero del 2001.

3. "Reglamento a Ley General de Instituciones del Sistema Financiero", Decreto Ejecutivo No. 1852. RO/ 475 de 4 de julio de 1994

4. "Ley General de Seguros", elaborado el 25 de febrero de 1998 en el Honorable Congreso Nacional, publicado en el Registro Oficial No. 329 de 1 de junio de 1998.

5. "Ley de Seguridad Social", elaborado en la Sala de Sesiones del Pleno del Congreso Nacional del Ecuador, el 13 de noviembre del 2001.

6. "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", 10 de abril del 2002.

7. "Reglamento a La Ley De Comercio Electrónico", Decreto Ejecutivo No. 3496. RO/ 735 de 31 de Diciembre del 2002.

8. "Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar servicios de Certificación de Información y servicios relacionados", Resolución No.584-23-CONATEL-2003.

9. "Reglamento General a La Ley Especial de Telecomunicaciones Reformada", Registro Oficial No. 770 de 30 de Agosto de 1995.

10. "Ley Orgánica de Defensa del Consumidor", Registro Oficial No. 520 de Septiembre 12 de 1990.

---

[42] *Los documentos descritos se encuentran vinculados a los archivos pdf's correspondientes y se encuentran disponibles en el Cd adjunto.*

11. "Reglamento General a La Ley Orgánica de Defensa del Consumidor", Publicada en el suplemento del Registro Oficial No. 116 del 10 de Julio del 2000.