ESCUELA POLITECNICA DEL EJERCITO

SEDE LATACUNGA

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

DESARROLLO DE UNA METODOLOGÍA PARA EL DISEÑO DE UN PKI (PUBLIC KEY INFRASTRUCTURE) Y SU APLICABILIDAD PARA LA ESPE-LATACUNGA.

PROYECTO PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS E INFORMATICA

VERÓNICA JANETH CHILIQUINGA SALAZAR

Latacunga, julio del 2003

CERTIFICACION

Se certifica que el presente trabajo fue desarrollado por Verónica Janeth Chiliquinga Salazar, bajo nuestra supervisión.

Ing. Santiago Jácome
DIRECTOR

Ing. Edison Espinoza
CODIRECTOR

DEDICATORIA

Esta tesis está dedicada a mis Padres Gustavo y Olga por el amor y el esfuerzo que día a día me brindaron en mi vida universitaria, por todo el apoyo moral que siempre me dieron para seguir adelante y cumplir mis metas, también a mis hermanos Santiago y Javier por ser la alegría de mi existencia.

CONTENIDO

I. LA SEGURIDAD EN INTERNET

1.1.- INTRODUCCIÓN

Inicialmente Internet se crea con una serie de redes, que permiten el intercambio de información entre investigadores sobre proyectos comunes, en esta etapa la información viajaba libremente sin ninguna preocupación por la privacidad de los datos ni de su seguridad.

La conceptualización de la red debe concebirse como un gran universo que se extiende para que el hombre pueda expresar sus formas culturales, tecnológicas, sociológicas y por supuesto las que se desarrollarán por la interacción de sí mismo con este nuevo medio. La humanidad ha puesto mucho de su parte para entrar en este medio, aprender sus códigos y lenguajes e involucrarse con esta tecnología que invade todos los campos.

Los protocolos creados para Internet fueron simples y sencillos lo que produjo su fácil ruptura y por lo tanto la violación de la información, esto ha dado la pauta para que se piense más en la seguridad y vaya de acuerdo al ritmo de crecimiento de las tecnologías de información y comunicación.

Cuando se habla de seguridad se suele referirse a accesos no autorizados a ordenadores para obtener información, la destrucción de información por venganza, espionaje, etc., pero esto, cuando se habla exteriormente, sin embargo existen otros riesgos que quizás pueden ser más peligrosos y son los internos como pueden ser los errores humanos, la falta de una política de seguridad, inexistencia de copias de seguridad o el compartir passwords, es una realidad que debería cambiar.

La seguridad en Internet es un tema que se ha venido tratando con el propósito de disminuir los riesgos a los que se enfrenta un usuario cuando realiza transferencia de información confidencial, por lo que personas y organizaciones

han venido desarrollando modelos en los que la intervención de firewalls, claves, protocolos, control de accesos, criptografía, certificados digitales, etc, han tomado impulso para fortalecer las comunicaciones en este medio.

El mundo actual cada vez se ve amenazado en la integridad de su información, por la falta de medidas de seguridad en una red tan compleja como es Internet, y a menos que la computadora no este conectada y se encuentre en un lugar cerrado y con vigilancia estará en peligro de encontrase con piratas informáticos, esto ha sido confirmado por un experto en seguridad al decir que “Un sistema se vuelve inseguro simplemente con el mero hecho de encenderlo”, esta frase define muy bien la probabilidad de que un sistema sea seguro.

Al mismo tiempo que Internet ofrece ventajas y oportunidades a sus usuarios, queda de manifiesto la imperiosa necesidad de seguridad y confidencialidad, pues, el constante asecho de personas mal intencionadas que mediante los delitos informáticos han limitado a que estos usuarios utilicen libremente y se favorezcan de este mundo electrónico.

La misma complejidad de esta red hace dificultoso el detectar y corregir los múltiples problemas seguridad que se presentan, por este motivo es de gran importancia la vigilancia constante y sistemática de parte de los gestores de las redes.

El momento en que millones de archivos están a disposición de todo el mundo y que esto no está orientado hacia todos los usuarios de la red, es cuando se debe implementar mecanismos de seguridad para poder restringir el acceso a determinadas personas y ordenadores dando el paso solo a unos pocos. Estas restricciones se basan en direcciones IP o nombres de usuario y claves.

El contar con un entorno confiable no solo depende de las claves de seguridad, direcciones IP o protocolos de comunicación seguros, hace falta un esquema en

el que estén involucrados varios elementos que puedan dar soporte necesario a los servicios de seguridad que se pretende dar.

Estos elementos que darían el soporte necesario a las organizaciones, usado más en transacciones de comercio electrónico son las autoridades de certificación, certificados digitales, sistema de gestión de claves, revocación de certificados (CRL) que son parte de una Infraestructura de clave pública (PKI). Esta solución sería la más conveniente para las transacciones económicas a través del Internet, debido principalmente a que en los últimos años han ido tomando fuerza justamente por el crecimiento de páginas en las que se ofrece productos, software y artículos de toda índole que dan a este mercado el impulso necesario para su desarrollo.

La mayoría de las personas ven en Internet un modelo de cómo serán los negocios en el futuro, es sencillo encontrar tiendas virtuales en las que se compra mediante el número de la tarjeta de crédito, pero ¿cómo se está completamente seguro de que esta información llegará a su destino final sin que otros la hayan interceptado?. A todo esto se le agrega la gran cantidad de tiempo y dinero que se está invirtiendo para conseguir una red segura.

El conseguir una red casi segura no es una tarea fácil debido principalmente a los hackers, crakers, phreakers y lammers, que no tienen diferencia alguna pues su finalidad será siempre la maldad en sus acciones y que de cualquier forma se introducen a los sistemas de grandes organizaciones para causar graves daños y por tanto pérdidas económicas.

Tanto la instalación de un antivirus como de un firewall no garantiza la total seguridad tanto en redes como en computadoras personales, aunque con estas acciones no se está protegido en un 100% si se habrá ganado la batalla a la gran mayoría de estos delincuentes informáticos.

1.2.- LA SEGURIDAD E IDENTIFICACIÓN EN INTERNET

1.2.1.- SEGURIDAD

El concepto de seguridad representa todo tipo de precauciones y protecciones que se llevan a cabo con el fin de evitar cualquier acción que comprometa la integridad de la información.

Se concibe por información a todo conjunto de datos llamado también mensaje que al receptor le interesa o no, antes de recibirlo, por lo tanto se puede decir que la frase seguridad de la información se refiere a la protección y prevención a través de ciertos mecanismos para evitar que ocurra de manera intencionada o accidental la transferencia, modificación o destrucción no autorizada de la información.

A partir de esta concepción surgen conceptos importantes a tomar en cuenta en la seguridad de la información que son: seguridad informática y seguridad en la red.

La seguridad informática nace con la necesidad de obtener herramientas automatizadas para proteger la información almacenada en una computadora, es decir herramientas creadas para salvaguardar los datos de los intrusos que pueden atentar la confidencialidad, integridad o disponibilidad de la información.

La seguridad en la red surge con los sistemas distribuidos, introducidos por la utilización de redes y el desarrollo que la tecnología le da a la comunicación, debido que por este medio se dan los elementos para transportar datos entre una terminal de usuario y una computadora o viceversa.

Debido al avance de la tecnología de las redes, ha permitido que las computadoras de todo el mundo se encuentren interconectadas y por lo tanto el crecimiento de la inseguridad rodee a organizaciones y usuarios.

La protección de los recursos de la red, la información y servicios en contra de las amenazas de seguridad se denomina seguridad de la red, cualquier medida o mecanismos realizado tiene como objetivo proteger los datos durante su transmisión.

Hoy en día tanto el Internet como el correo electrónico son los medios más utilizados para la comunicación, sin embargo la mayoría de los usuarios no son conscientes de la simplicidad con que sus mensajes pueden ser interceptados en Internet o intranets desprotegidas, se puede deducir con facilidad que la mayoría de estos usuarios creen en la posibilidad de que sus números de tarjetas de crédito sean robados en transacciones de comercio electrónico.

Por este motivo es importante contar con un esquema de seguridad así como de los medios legales para asegurar que los documentos electrónicos transmitidos por este medio sean tan confiables, válidos y legalmente reconocidos como los del papel tradicional.

Por una parte es indispensable avalar la identidad de los cibernautas u organizaciones, de tal modo que se tenga la certeza de quien envía la información y que realmente sea la persona que dice ser y no un tercero que pueda hacerse pasar por dicha persona.

Esta seguridad toma mayor alcance en el e-commerce que aún está en desarrollo, por lo que se debe afianzar los elementos involucrados en estas transacciones, para que sean fiables y perdurables en el tiempo y que los interlocutores estén tan bien identificados como en el mundo real. La base fundamental en el que estos elementos puedan tener progreso y viabilidad es la seguridad política, seguridad jurídica y previsibilidad económica.

1.2.2.- NIVELES DE SEGURIDAD

La seguridad de un sistema informático siempre ha estado relacionada con los elementos que lo componen es decir el hardware y software, en general la protección de un sistema informático no se limitará a la integridad de la información, o el acceso restringido a personas no autorizadas sino también se deberá poner especial atención a los equipos de computo donde se opera y almacena información.

Estos elementos mencionados deberán tener la misma importancia en lo que respecta a la seguridad, sin embargo cabe destacar que los errores mal intencionados de empleados debería ser la mayor preocupación de los jefes, debido a que este es el mayor riesgo en una organización y por lo tanto tendrá una mayor pérdida económica. Mientras que los errores provocados por la energía eléctrica o daños por la naturaleza constituye en un menor porcentaje de riesgo para las organizaciones.

De todo lo mencionado hay que destacar que los administradores de una red se preocupan más por la filtración de intrusos externos que pueden engañar a firewalls, e introducirse para causar daños, por este motivo es que la tendencia a preocuparse más por el software que por el hardware ha ido aumentando.

Para que exista un completo equilibro entre el software y hardware se debe realizar un estudio de los niveles de seguridad que permitirá salvaguardar la información almacenada y manejada por el hardware y software de la red.

1.2.2.1.- Estudio de los niveles de seguridad.

El Departamento de Defensa de los Estados Unidos ha acordado y establecido normas de seguridad y a las que se puede acceder en el denominado Libro Naranja. En este se determinan criterios básicos de evaluación de computadoras confiables.

Los niveles de seguridad a los que se refiere van desde la seguridad física, autentificación de usuario, confiabilidad en el software del sistema operativo, etc.

El Libro Naranja es el estándar del Departamento de Defensa de los Estados Unidos desde 1985, año en que fue aprobado y desde entonces no ha sufrido cambio alguno. Por varios años este ha sido el método básico para evaluar a los sistemas operativos, bases de datos y redes a acuerdo a interpretaciones del libro.

1) Seguridad Estadounidense

- Nivel D1

Este es el nivel más bajo de seguridad, y de acuerdo al estándar el sistema entero es inseguro, no tiene protección para el hardware, no existe autentificación para los usuarios ni tampoco existe control de accesos a la información almacenada en la computadora.

En este nivel de seguridad se puede mencionar como ejemplo a MS-DOS, este sistema operativo no distingue a los usuarios que lo están manejando ni tiene control de la información a la cual están accediendo.

- Nivel C

Este nivel a su vez contiene a dos subniveles de seguridad denominados C1 y C2. El nivel C1 denominado Sistema de Protección de Seguridad Discrecional, trata de la seguridad en el sistema Unix tradicional, tiene un cierto nivel de protección para el hardware y en cuanto a los usuarios tiene que identificarse antes e ingresar al sistema por medio un nombre o login y una contraseña o password, con este método se podrá restringir el acceso a la información.

Para determinar el acceso a la información se debe dar los permisos a los archivos y directorios de los usuarios registrados en el sistema, esto lo debe realizar el administrador de la red que en este caso es el root. Sin embargo esto no es totalmente seguro ya que un administrador con mala intención puede dañar o modificar archivos de los usuarios.

El nivel C2 es el que cubre los problemas del subnivel anterior, además posee otras características que permitirán tener un entorno de acceso controlado, pues se podrá restringir más a los usuarios mediante una auditoria de lo que realice cada usuarios que acceda al sistema.

En este nivel además de los permisos se cuenta con los niveles de autorización, es decir la auditoria al sistema, pues el llevar el registro de todas las acciones realizadas por los usuarios traería muchas ventajas a la hora de determinar quien es el responsable de acciones que vayan en contra de la organización. Llevar este registro haría que se utilicen más los recursos del procesador y del subsistema de disco, aunque con la capacidad de las computadoras actuales esto dejaría de ser una desventaja.

El uso de estas autorizaciones adicionales permitiría a los usuarios realizar tareas de administración sin contar con la contraseña del root, es decir ejecutar comandos específicos o acceder a tablas restringidas.

- Nivel B

En este nivel se han clasificados tres subniveles. El primero, el nivel B1 denominado Protección de Seguridad Etiquetada, es el que da soporte a la seguridad multinivel, es decir que el dueño de un archivo no puede modificar los permisos de un objeto que este bajo control de acceso obligatorio.

En el nivel B2 denominado Protección Estructurada, se requiere que todos los objetos estén etiquetados, los dispositivos externos como discos, terminales, impresoras pueden tener uno o varios niveles de seguridad. El nivel B2 es el primero que se acerca al problema de la comunicación de un objeto con otro objeto que se encuentra en un nivel de seguridad inferior.

El nivel B3 conocido como Dominios de Seguridad es el que da importancia a la instalación de hardware para dar mayor fuerza a sus dominios. Además este nivel debe contar con un enlace seguro desde un terminal de usuario al sistema.

- Nivel A

Denominado como de Diseño Verificado, este es el nivel que cuenta con más validaciones en el Libro Naranja, pues tiene un control estricto de todos los componentes de los niveles inferiores, además el diseño debe verificarse matemáticamente y realizar un análisis de los canales de distribución confiable, esto quiere decir que el hardware y software utilizados deben estar protegidos al máximo.

2) Seguridad Canadiense

Pero no solo el gobierno de los Estados Unidos se ha preocupado por establecer estándares, ya que el gobierno de Canadá ha hecho su propio esfuerzo y ha creado estándares de seguridad, en los que consta los Criterios de Evaluación de Productos Confiables de Cómputo Canadienses (CTCPEC) y los Criterios Comunes.

Los CTCPEC tienen a su cargo la funcionalidad que está relacionada con la confidencialidad, integridad, disponibilidad y responsabilidad, así como el aseguramiento que se centra en el grado de confianza con la los productos que se estén desarrollando o evaluando implementen las políticas de seguridad.

En cuanto a los criterios comunes se puede decir que se ha determinado siete niveles de aseguramiento que son: EAL-1, EAL-2, EAL-3, EAL-4, EAL-5, EAL-6 y EAL-7.

- Nivel EAL-1

Este es el nivel más bajo de aseguramiento, se fundamenta en el análisis de las funciones de seguridad del producto y resulta muy representativo tanto para el desarrollador como para el consumidor.

- Nivel EAL-2

El nivel EAL-2 es el de aseguramiento más alto, realiza un análisis de las especificaciones funcionales y de interfaz, puede dar al desarrollador tareas adicionales que son requeridas por el nivel anterior.

- Nivel EAL-3

Este nivel describe un grado moderado de seguridad debido a que la seguridad es validada por una fuente externa. Se aplica un aseguramiento máximo al producto ya que se ha concebido a la seguridad desde el diseño en lugar de que este se implemente después de esta etapa.

- Nivel EAL-4

En este nivel es posible de reparar una línea de productos existente, un producto con este nivel de aseguramiento está diseñado, probado y examinado lo que le da al consumidor el máximo nivel de seguridad, también realiza una búsqueda de puntos vulnerables en el producto un ejemplo de que este nivel está bien aplicado es en el desarrollo de software.

- Nivel EAL-5

En este nivel el desarrollador debe aplicar prácticas de desarrollo de software comercial y técnicas de ingeniería de seguridad, este nivel es de cuidado riguroso por lo tanto es para quienes requieran un alto nivel de aseguramiento. En este nivel también se debe presentar las especificaciones de diseño y la forma en que dichas especificaciones se implementan en el producto. No es sencillo que los productos existentes alcancen un nivel EAL-5.

- Nivel EAL-6

Este nivel consta de un diseño verificado semiformal, de una presentación estructurada de la implementación y de un componente de prueba, además incluye todos los elementos del nivel anterior. El producto es sujeto a una revisión alta y baja de diseño que pueda garantizar la resistencia a los ataques. En todo el ciclo del diseño existe un proceso de desarrollo estructurado, control de desarrollo y control de manejo de configuración.

- Nivel EAL-7

Este nivel es para aquellas aplicaciones de seguridad en las que existe una alto riesgo de rompimiento de seguridad, este nivel se fundamenta en una revisión independiente y formal del diseño, el desarrollador debe probar cada etapa del diseño indagando puntos vulnerables que luego serán verificados por una persona independiente, este proceso es exhaustivo ya que va desde la concepción hasta la terminación del producto.

1.2.3.- SERVICIOS DE SEGURIDAD

Un servicio de seguridad es aquel que incrementa la seguridad en un sistema de información y por lo tanto el flujo de información en la organización, estos servicios están dirigidos a evitar los ataques de seguridad y se valen de varios mecanismos de seguridad para proporcionar este servicio.

La gestión de los servicios de seguridad requieren de un nivel de conocimientos, así como especialización y dedicación constante. En incremento de la complejidad de los sistemas de información es la razón por la que la tarea de administrar los sistemas de seguridad se vuelve complicada.

El Modelo de Referencia OSI presenta en su segunda parte una Arquitectura de Seguridad “Information Processing Systems. OSI Reference Model - Part 2: Security Arquitecture", ISO/IEC IS 7498-2, y según este documento emitido por la ISO para proteger las comunicaciones de los usuarios en las redes es necesario dotarlas de servicios de seguridad.

Antes de explicar cada uno de estos servicios, se relacionará estos con cada capa del modelo OSI, así el nivel físico puede soportar confidencialidad de los datos utilizando protocolos de cifrado de extremo a extremo. El nivel de enlace de datos también puede soportar confidencialidad de datos utilizando protocolos de cifrado de enlace a enlace en vez de extremo a extremo.

Los niveles de red y transporte pueden soportar autenticación, control de acceso, confidencialidad e integridad de datos. El nivel de sesión según el ISO no soporta ningún servicio de seguridad. El nivel de presentación puede soportar confidencialidad de datos.

El nivel de aplicación OSI puede soportar los cinco servicios de seguridad. La arquitectura de seguridad OSI sólo analiza los servicios que puede soportar cada nivel, más no dice que servicios deberían soportar cada nivel.

1.2.3.1.- Autenticación

Este servicio verifica la fuente de los datos, es el más sencillo de comprender pues simplemente verifica la identidad. Este proceso en la vida cotidiana es el que

más se practica ya que a cada momento se autentica a personas, organizaciones y direcciones sin la mayor importancia ya que se lo hace de manera informal.

Se podría ejemplificar cuando se compara la ubicación de una casa que conoce con la que se tiene en la memoria, pues la ubica por su color, dirección o número de casa. Una forma muy común de autenticación es por medio de la una firma que posee cada persona y le permite identificarse ante una transacción, además sirve como autorización.

El servicio de autenticación trata de asegurar que una comunicación sea auténtica, su función es la de aseverar al receptor que el mensaje es de la fuente que él espera. Este servicio puede ser solo de la entidad origen, de la entidad destino o de ambas a la vez.

La autenticación debe asegurar que la conexión no pueda ser interferida por una tercera persona que pueda hacerse pasar por una de las dos entidades legítimas con el propósito de realizar una transmisión o recepción no autorizada.

1.2.3.2.- Control de Acceso

Este servicio verifica que los recursos sean utilizados por quien tiene autorización a hacerlo. Para este servicio se cuenta con varios elementos como son dispositivos pasivos o activos. Entre los dispositivos pasivos está una puerta cerrada que necesita de una identificación para ser abierta y entre los activos está un monitor de control de acceso que determina que usuario está autorizado a ocupar un recurso, el monitor antes de otorgar el acceso valida la identidad del usuario, con esto se deduce que la autorización está ligada con la autenticación.

En lo que se refiere a la seguridad en la red, el control de acceso es la habilidad para restringir y controlar el acceso a los sistemas anfitriones y las aplicaciones mediante los puentes de comunicación, para conseguir este control las entidades que quieren acceder deben autenticarse con sus propios derechos de acceso.

Los componentes básicos de un control de acceso son las entidades de la red, recursos de la red y los derechos de acceso, estos representan los privilegios de la entidad bajo los cuales las entidades pueden tener acceso a los recursos de la red y como estas son permitidas para tener acceso a estos recursos. Estos permisos pueden ser cambiados y/o revocados por el administrador autorizado de la red.

Los recursos, usuarios e información pueden ser clasificados en diferentes niveles de seguridad, esta selección permitirá que solo las personas autorizadas para un cierto nivel puedan acceder a la información, mientras que los niveles inferiores nunca podrán acceder a los superiores.

Algo importante que cabe destacar es el tener una lista de control de accesos (LCA) puede ser utilizada para proteger los recursos individuales. Una LCA es una lista de permisos que determina quienes pueden tener acceso a los recursos individuales de la red, esta lista permite que el propietario de uno o varios recursos permita o deniegue el acceso a los recursos a una entidad o a un grupo de entidades. Los permisos de una entidad pueden ser de lectura o escritura, creación o destrucción, adición, eliminación o modificación de datos, importación o exportación, ejecución.

1.2.3.3.- Confidencialidad

El servicio de confidencialidad o privacidad previene que se rebele accidental o deliberadamente datos a través de una comunicación, es decir que solo las personas autorizadas podrán acceder a dichos datos.

En la sociedad común la forma de proteger los objetos de personas ajenas es por medio de candados y cerraduras, pues es frecuente que dos o más personas que habitan en un mismo lugar posean las llaves de estas cerraduras, es el caso de casas, oficinas o lugares de trabajo.

Este servicio es algo a que la mayoría de las personas se enfrenta diariamente ya que las consecuencias del descubrimiento no autorizado a la información puede ser desastroso, es sencillo imaginar que tan grave puede ser el daño si se llegara a quebrantar la privacidad.

El control de la seguridad depende lo que se quiera proteger, es decir el grado de importancia de la información y la medida en que puede afectar en caso de romperse su confidencialidad. El poseer una llave permite la autenticación, autorización y por lo tanto la confidencialidad de la información, al realizar la analogía con la llave de una casa, se puede decir que al darse el robo de ésta, se habilitará para que el ladrón pueda acceder a cualquier sitio de la casa, esto hará que el dueño se prevenga y tenga que cambiar de cerradura, estas son las medidas que se tomaría en el mundo físico.

Pero en el mundo de Internet y las redes, esto no ocurre ya que si alguien logra interceptar una comunicación puede realizar una copia de la contraseña sin nuestro consentimiento y romper el servicio de confidencialidad. Las razones son variadas por las que personas sin autorización acceden a la información de organizaciones, estas razones pueden ser adquirir ventajas competitivas, publicidad o producción, entre otras.

La confidencialidad facilita la protección de los recursos informáticos para asegurar que nadie pueda leer, copiar o modificar información sin autorización, esto es llamado servicio de confidencialidad de contenido, que no puedan interceptar las comunicaciones entre entidades, lo que se denomina servicio de confidencialidad de flujo de mensaje.

Para dar el servicio de confidencialidad se utiliza la criptografía, que mediante el desarrollo de métodos matemáticos se pueda asegurar que sea casi imposible el ingreso no autorizado a la información. Esta ciencia se ha especializado en crear algoritmos para que nuestros mensajes sean posibles de comprender solo para

las personas que tienen la debida autorización y sean ilegibles para el resto, afirmando así la confidencialidad.

1.2.3.4.- Integridad

Este servicio se verifica que los datos que son enviados por el transmisor no se alteren hasta su llegada al receptor. En la sociedad generalmente la verificación de la integridad de los objetos se ha realizado en forma visual, pues la falta de señales de alteración significaría que dicho objeto no ha sido manipulado. La utilización de sellos para la integridad es de utilización en al área comercial, pues en muchas organizaciones para garantizar la calidad de los productos se los envía en cajas selladas y se sabe que si existe alguna alteración en esta, solo con la simple observación se percataría que la integridad ha sido violada.

Sin embargo en Internet esto no es tan sencillo, debido a que los datos están virtualmente en todos lados, esto hace que la información guardada en una computadora sea potencialmente fácil de acceder. Para evitar que la integridad sea quebrantada se hace necesario la creación de algún “sello” que sea utilizado para verificar que los datos no han sido modificados.

Los controles que da el servicio de integridad aseguran que los datos no hayan sido modificados y que la secuencia de los datos transmitidos por una red se mantenga, de ésta forma se evitará que la inserción, borrado o modificación no autorizada sea efectuada. Si la integridad no existiese la personas desautorizadas podrán manipular los datos según su conveniencia y utilizada para su provecho.

El servicio de integridad se relaciona con los ataques activos, se refiere más a la detección que a la prevención, pues si se detecta que se ha violado la integridad de un sistema, se lo reporta para que mediante el software o la intervención humana se pueda recuperar de esta violación.

Los servicios que se disponen pueden ser de integridad de contenido o servicio de integridad de la secuencia el mensaje. Los mecanismos utilizados para ofrecer la integridad pueden ser: código de detección de modificación, código de autenticación de mensaje, firma digital y número de secuencia de mensaje.

1.2.3.5.- No repudio

Denominado también de irrenunciabilidad, este brinda la prueba ante una tercera parte de que las entidades involucradas en una trasmisión hayan participado realmente en este proceso. Por tanto cuando un mensaje es enviado el receptor él puede probar que el mensaje fue remitido por el supuesto emisor de manera similar se puede decir cuando el mensaje es del remitente y éste puede probar que el presunto receptor ha recibido el mensaje.

El no repudio ofrece protección de un usuario frente a otro, que posteriormente puede negar que haya tenido alguna comunicación o recibido mensajes de este usuario, esta protección se realiza mediante una colección de evidencias irrebatibles que podrán dar solución a cualquier discrepancia. Este servicio se aplica al problema de la denegación falsa de la información que se recibe de otros, el no repudio suministra pruebas que pueden ser demostradas por una tercera entidad.

Los servicios que se proporciona son: no repudio de origen, no repudio de envío, no repudio de presentación, no repudio de transporte, no repudio de recepción. Además se debe agregar que este servicio es de dos tipos:

- Con prueba de origen o emisor, en este caso el destinatario tiene la completa seguridad de quien es el emisor concreto de datos.

- Con prueba de entregar o receptor, en este tipo de servicio el emisor tiene la prueba que los datos de la comunicación han llegado íntegramente al destinatario correcto.

Para suministrar los servicios de no repudio se utiliza las firmas digitales que son adquiridas por una sola persona y pueden ser verificadas por terceras personas, que proporcionarán la garantía de que los firmantes no evadan las responsabilidades adquiridas con la firma digital.

1.2.4.- MECANISMOS DE SEGURIDAD

Uno de los aspectos relevantes dentro de la seguridad son los mecanismos que se efectúen para salvaguardar la información. Se define a un mecanismo de seguridad como una técnica que se utiliza para implementar un servicio, es decir el mecanismo está diseñado para detectar, prevenir o recuperarse de un ataque de seguridad.

Para implementar los mecanismos de seguridad se utilizan los servicios de seguridad o la combinación de estos. Para tener una idea más clara de los servicios y mecanismos, se puede decir que los servicios especifican “que ” controles son necesarios y en cuanto a los mecanismos se especifica “como” deben ser ejecutados los controles.

Se puede utilizar una combinación de los mecanismos para proporcionar los servicios de seguridad, sin embargo estos mecanismos ofrecen tres componentes principales:

- Una información secreta, la que se refiere a claves y passwords conocidas por las entidades autorizadas.

- Un conjunto de algoritmos, necesarios para lograr el cifrado, descifrado y generación de números aleatorios.

- Un conjunto de procedimientos, que son los que definen como se utilizarán los algoritmos, así como quién envía a quién y cuando deberá hacerlo.

Hasta ahora no existe un solo mecanismo capaz de proveer todos los servicios, pero la mayoría utiliza técnicas criptográficas basadas en el cifrado de la información y de acuerdo al objetivo se tiene pueden ser clasificados como preventivos, detectivos y recuperables.

Pero es necesario definir los tipos de mecanismo de seguridad y para esto se puede dividir en dos categorías que son:

- Mecanismos de seguridad generalizados.

- Mecanismos de seguridad específicos.

1.2.4.1.- Mecanismos de seguridad generalizados.

Estos mecanismos se relacionan directamente con los niveles de seguridad requeridos y están relacionados con la gestión y el grado de la seguridad del sistema. Dentro de este tipo se encuentran:

1) Funcionalidad de confianza, se utiliza para desarrollar los demás mecanismos de seguridad, esta puede proveer protección de asociaciones encima de la capa en la que la protección es ejercida, esto ayudará a determinar el nivel de confianza de un servicio o persona.

2) Etiquetas de seguridad, se asocian a los recursos por medio de números que permiten determinar el grado de sensibilidad de los datos, clasificando la información por niveles de seguridad que puede ser: secreta, confidencial, clasificada, no clasificada, etc. Estas son las etiquetas deberían ser transmitidas con los datos o estar implícitas en estos.

3) Detección de eventos, en esta se involucra a la violación de la seguridad y de manera opcional la detección de eventos normales. La detección de eventos

puede accionar respuestas como el reporte de un evento local o remoto, la terminación de un evento, por lo tanto este mecanismo detecta movimientos normales o peligrosos que ocurren en el sistema.

4) Seguimiento de auditorias de seguridad, este mecanismo se refiere a un análisis de los registros que se lleva de las actividades del sistema, esto es muy útil y necesario cuando se lleva a cabo las auditorias de seguridad. Su finalidad es comprobar que tan apropiados son los controles del sistema para asegurar su funcionalidad. El seguimiento de una auditoria de seguridad implicar que los registros de información sean analizados detalladamente.

5) Recuperación de seguridad, realiza acciones de recuperación basándose en una serie de reglas para tomar acciones y así satisfacer las peticiones como manejo de eventos y funciones de administración. Las acciones de recuperación pueden ser inmediatas, temporales o a largo plazo.

1.2.4.2.- Mecanismos de seguridad específicos.

Definen la implementación de los servicios concretos y son:

1) Intercambio de autenticación, ésta es más sencilla cuando se trata de realizarla físicamente, mientras que esto no ocurre en las redes debido a que la persona no está presente. Este mecanismo trata con la autenticación de las entidades de la red, hace uso de información de autenticación, técnicas criptográficas y características y/o posesiones de la entidad.

Este mecanismo se utiliza para corroborar la identidad de quienes envían los mensajes, verificando de esta manera la identidad origen o destino de la persona deseada. Este mecanismo pueden ser fuertes o débiles.

Las de autenticación fuerte debido a que utilizan técnicas criptográficas para proteger los mensajes que se van a intercambiar, en este caso se encuentran los

sistemas de clave pública, en la que un usuario se identifica por su clave privada y su interlocutor lo hará a través de la clave pública que deberá a su vez poseer un certificado firmado por una Autoridad Certificadora (AC), que será en este caso la tercera parte de confianza y que será válida por un período de tiempo.

Las débiles o las de autenticación simple debido a que se basan en técnicas de control de acceso, funciona cuando un emisor envía su identificación y contraseña y el receptor tendrá que comprobarlo.

2) Integridad de datos, este mecanismo asegura que los datos no sean alterados o destruidos, trata con la integridad de una unidad de campo o datos simple o una secuencia de estos.

Su funcionamiento implica el cifrado de una cadena de datos a transmitir denominada Integrity Check Value o ICV traducida significa Valor de Comprobación de Integridad, este mensaje se envía junto con los datos ordinarios, el receptor repite la compresión y cifrado posterior de los datos y compara el resultado con los que recibió para asegurarse que no han sido modificados.

El proceso empieza cuando se genera un valor en la entidad emisora y lo adiciona a la unidad o campo de datos, este valor es un código de verificación o cantidad criptográfica que se calcula en función de los datos y que se adjunta como información adicional. El proceso continua cuando se genera el valor correspondiente de la unidad o campo de datos recibido en entidad receptora y lo compara con el valor recibido.

Pero para esto se requieren de protecciones adicionales, si la transferencia es con conexión se debe utilizar la secuencia numérica, sellos de tiempo o cadena criptográfica, pero si es sin conexión se pueden utilizar sellos de tiempo con lo que se proporcionaría una forma limitada de protección contra el reenvío de unidades individuales de datos.

Es importante decir que una herramienta valiosa es la auditoria de datos pues resguardaría la integridad de los mismos, esta idea nació del mundo real cuando las compañías empleaban auditores externos para que su posición fiscal sea correcta.

4) Firma digital, se puede definir como un conjunto de datos que se añaden a una unidad protegiéndola de cualquier falsificación y permitiendo que el receptor conozca el origen y la integridad de los datos, para ello se cifra la unidad de datos junto con algún componente secreto del firmante y se obtiene un valor relacionado al resultado final.

La firma digital es utilizada en los sistemas de clave pública, en este una persona puede cifrar un mensaje y solo el destinatario de este podrá descifrarlo. Este mecanismo tiene ventajas como:

- La firma es auténtica.
- La firma no puede ser violada.
- El documento firmado no puede ser alterado.
- La firma no es reutilizable.

Aunque sean varias las ventajas de la firma digital siempre existe el riesgo de un ataque que atente la integridad de los datos, ya que el receptor no está totalmente seguro de que el mensaje ha sido enviado por el emisor, pero para verificar esto existen las Autoridades de Certificación (AC).

Cuando se firma un documento en papel se da por entendido que la firma compromete a lo estipulado en el documento, que este no cambiará después de la firma y que esa firma no se transferirá a otro documento. Todo esto es válido en el mundo real porque existen leyes que dan el soporte para este sistema.

En el mundo de las redes también podría hacerse con la utilización de la clave privada para cifrar el documento, sin embargo el uso de tiempo máquina sería alto debido a los algoritmos utilizados. Pero la solución está en el denominado mensaje reducido que utiliza algoritmos para reducir documentos la mínimo y que se utiliza para confundir al atacante.

Un mensaje reducido no puede revertirse sin el documento original que creó la reducción y el tiempo para cifrar la reducción con un algoritmo de clave privada y pública es mayor. El mecanismo de firma digital soporta los servicios de autenticación, integridad y no repudio del mensaje.

5) Control de acceso, se utiliza para autenticar las capacidades de una entidad para acceder a un recurso dado, puede funcionar en el origen o en el intermedio y asegura que el emisor está autorizado a comunicarse con el receptor o a utilizar sus recursos.

En este mecanismo es muy importante la confianza, definida en internet como la capacidad para autenticar a personas y compañías que intercambian información a través de la red y es un punto que fortalece el e-commerce.

Si los mecanismos que se utilizan en la actualidad no ofrecen los servicios de autenticación, confidencialidad, integridad y no repudio los usuarios dudarán en emplearlos. Pero el mayor problema de los cibernautas es que no comprenden el término confianza y es una barrera que se deberá superar para progresar en este mundo electrónico.

6) Tráfico de relleno, conocido también como relleno de tráfico, este mecanismo genera un tráfico falso, crea un flujo constante de mensaje vacíos o basura junto con los datos válidos. Esto puede ser efectivo en el caso de que un atacante realice un análisis de tráfico entre nodos que ocasionalmente tienen comunicación, esto hará que el atacante no sepa si se está enviando información

o cuantos datos útiles se está enviando, dificultando el análisis del tráfico de la red y de esta forma confundirlos.

Se llaman rellenos porque generan eventos de comunicación, unidades de datos y datos falsos de forma semi-aleatoria con el objetivo de confundir al analizador de tráfico, con la salida de texto cifrado continuo el atacante no podrá distinguir el ruido de los datos verdaderos. Este mecanismo puede ser utilizado para dar varios grados de protección contra el análisis de tráfico.

7) Control de encaminamiento, este mecanismo se lo conoce como control de ruta y su finalidad es la de seleccionar de manera física cada una de las rutas alternativas para que puedan ser utilizadas según el nivel de seguridad y la información que se esté transmitiendo, es decir en estos mecanismos se cubren todos los aspectos de la ruta que sigue los datos en la red.

En el control de encaminamiento se solicita y utiliza rutas alternas para el envío de datos, en el caso de que se detecte continuas violaciones de integridad en la ruta determinada. En el proceso de conmutación se selecciona para una comunicación determinados enlaces, redes o repetidores buscando una mayor confidencialidad, para realizar esto se lleva a cabo una recodificación de rutas y tablas del sistema.

Cualquier mecanismo de control de encaminamiento se utiliza para lograr la selección dinámica o pre-establecida de rutas específicas para la transmisión, es por eso que ciertos datos con etiquetas se les prohíbe pasar por determinadas líneas. Existen algunos mecanismos más sofisticados que reaccionan ante la persistencia de ataques en una ruta, dejándola fuera de posibles selecciones.

8) Unicidad, este mecanismo consiste en añadir a los datos un número de secuencia, fecha, hora y un número aleatorio o algún tipo de combinación de los mismos, de tal forma que la información tenga una única secuencia, lo que evitará que los datos enviados sean nuevamente acomodados o repetidos.

9) Cifrado, puede realizarse mediante la utilización de sistemas criptográficos simétricos o asimétricos. El cifrado es la clave del mecanismo de seguridad que provee confidencialidad a los datos.

Se hace uso de la criptografía, pues se utiliza los principios y métodos para la transformación matemática de los datos, con lo que se logrará ocultar el contenido de la información, previniendo el uso no autorizado. El cifrado avala que la información sea secreta para individuos, entidades o procesos que así lo requieren. Existen algoritmos de cifrado reversible e irreversible.

El algoritmo de cifrado reversible simétrico utiliza una clave de cifrado secreto y el conocer esta clave implica el conocimiento de la clave de descifrado, es decir cuando se utiliza la misma clave para cifrar y descifrar, se dice que el sistema criptográfico es simétrico. Estos sistemas son más ágiles que los sistemas de clave pública y son muy apropiados en al cifrado de grandes volúmenes de datos, se pueden clasificar en cifradores de bloque y cifradores en flujo, los primeros trabajan con bloques de datos fijos que pueden ser de 64 bits y los segundos trabajan sobre flujos continuos de bits.

Un algoritmo de cifrado irreversible asimétrico utiliza una clave pública y el conocimiento de esta clave no implica el conocimiento de la clave privada para el descifrado. En este sistema se utiliza una pareja de claves, es decir la primera la clave privada se mantiene secreta, mientras que la segunda clave es la pública y puede ser conocida por todos. En general las claves públicas se utilizan para cifrar y las privadas para descifrar, estos sistemas criptográficos son más lentos que los simétricos pero son muy adecuados para cumplir con las funciones de autenticación, distribución de claves y firmas digitales.

10) Notarización, provee de los elementos necesarios para asegurar la comunicación de datos entre dos o más entidades como la integridad de datos, origen, tiempo y destino, esto se logra con la participación de una tercera entidad

de confianza llamado notario, el cual tiene la credibilidad e información necesaria para proveer el seguro que requieren estas entidades.

La Notarización es conocida como certificación ya que recurre a terceras personas ya sea físicas o jurídicas que afirman la seguridad de los datos, así como la garantía del origen y destino de entidades involucradas.

Cuando se utiliza el mecanismo de Notarización los datos pueden ser comunicados entre las entidades, pues ante esta realidad se necesita de alguien que de fe de la identidad del remitente y que certifique que la clave privada pertenece a este remitente. Este proceso puede realizarse con los certificados y las Autoridades de Certificación (AC).

Las funciones primarias de una AC son: aceptar aplicaciones para certificados, verificar la identidad de la persona o la compañía empleada para el certificado, emitir certificados, revocar certificados, proveer la información del estado sobre los certificados que se han emitido.

1.3.- SEGURIDAD EN TRANSACCIONES ELECTRÓNICAS

1.3.1.- TRANSACCIONES ELECTRÓNICAS

La realidad de internet como un medio y herramienta que ayuda a la reducción de costos, a la ampliación de mercados y eliminación de barreras geográficas, cada vez está envolviendo a las sociedades y en espacial a la nuestra, que quiere incorporar esta tecnología a sus organizaciones.

Ya se está viendo que estas organizaciones empiezan con la colocación de páginas web que son un elemento más de publicidad de sus productos y/o servicios hacia sus clientes o proveedores. En este punto es donde surgen varias incógnitas para la empresa y su círculo, pues al querer efectuar transacciones

automáticas nacen necesidades técnicas y culturales, y siendo las segundas las más difíciles de incorporar.

Las soluciones técnicas que existen hoy en día en el mercado son muchas y muy efectivas que permiten la concepción de una comunidad virtual, donde todos los miembros son parte de una cadena productiva y/o servicios, estos miembros van desde proveedores de materia prima, fabricantes, puntos de venta que pueden ser mayoristas o minorista hasta llegar al consumidor final. Es importante mencionar que parte de esta cadena son los servicios financieros y de logística que hacen realizable cerrar los ciclos de producto (logístico) de dinero (financiero) y el comercial (venta).

Sin embargo existen mercados verticales en los que esta funcionalidad técnica ha sido aceptada y utilizada por sus miembros, pero también existen mercados en los que la cultura es el mayor problema. Es evidente que los clientes son los que pueden exigir a sus proveedores que participen de la cadena virtual, pues las ventajas serían reducción de costos y recursos, pero lo que no es factible aunque no imposible es que un proveedor obligue a sus clientes a incorporarse en la red.

Al existir tantos mercados verticales se debería implicarse primero con los estándares, los catálogos y la interacción con los miembros del sistema que se hayan definido en cada mercado. Es donde la red comercial toma mayor importancia y la necesidad de que las empresas unifiquen criterios y puedan ingresar en esta red.

Esta red no sería nada sin vendedores y clientes, para esto las algunas empresas han sido verdaderos impulsadores y motores de la red comercial, pero el nivel de inserción sigue aún siendo bajo, debido a los esquemas culturales de una parte de la sociedad renuente a las tendencias tecnológicas o talvez por problemas de bajo presupuesto.

Las redes comerciales tienen más beneficios que desventajas y si se rompe ese círculo vicioso que es “no ingreso a las redes porque son pocos los que están y son muy pocos porque nadie ingresa” las empresas tendrán que estar preparadas o por lo menos saber las implicaciones que se tendrían en caso de quedar fuera de ellas.

1.3.1.1.- Comercio Electrónico

El comercio electrónico o del inglés e-commerce es cualquier actividad de intercambio comercial en la que las órdenes de compra, venta y pago se realizan a través de un medio informático, en estos se incluyen servicios financieros y bancarios facilitados por internet.

El e-commerce es la venta a distancia aprovechando las ventajas que ofrece las nuevas tecnologías de información y comunicación, la ampliación de la oferta, la interactividad y la inmediatez de la compra, con la peculiaridad de que se puede comprar y vender a quien quiera, cuando se quiera y en cualquier parte del mundo. Se la puede definir como cualquier forma de transacción comercial o intercambio de información mediante la utilización de las TIC’s entre empresas, consumidores y administración pública.

El desarrollo del comercio electrónico es multiplicado por la presión del “no poder quedarse afuera”, respaldada por muchas empresas, esto es así porque para que este tipo de comercio exista no solo hace falta la presencia de dos personas sino también de un medio seguro. Por un lado el hardware que recoja e interprete digitalmente la voluntad de estas personas trasformándolas en unos y ceros para que luego sean transmitidas.

Pero también es necesario de programa o software que nos ofrecen los países del primer mundo, puesto que ellos ya han adquirido las ventajas que les proporciona el comercio electrónico. Este software es el que resolverá todos los

problemas en las transacciones por internet. Como ejemplo se puede mencionar al sistema de clave pública dotado de un algoritmo casi imposible de romper.

El término "comercio electrónico", de alguna manera, toma significados diferentes en América Latina y en América del Norte. En la primera se interpreta, primordialmente, como las disposiciones técnicas, organizacionales y regulatorias que establecen o permiten la comercialización electrónica de datos, incluyendo el suministro de información a firmas y la correcta configuración de la infraestructura nacional de telecomunicaciones.

Entre los proveedores de servicios de Internet y posiblemente en el pensamiento de la población, significa, mayoritariamente, un comercio minorista orientado a los consumidores a través de las páginas Web.

En contraste, en América de Norte, el término "comercio electrónico" significa, en forma creciente, un amplio rango de transformaciones en los negocios, favorecido por la tecnología de información y de comunicación (TIC), que incluye intranets, extranets, transmisiones abierta o cerrada de datos y sus recientes permutaciones, tales como las redes virtuales privadas con valor añadido y las aplicaciones de multimedia interactiva en redes.

En el Ecuador el comercio electrónico ha revuelto el mundo de los negocios y las empresas quieren estar al nivel de la competencia internacional. Es por eso que el Estado Ecuatoriano creyó indispensable el contar con las herramientas jurídicas que permitan utilizar los servicios electrónicos, incluido el comercio electrónico en las actividades de nuestra sociedad.

La Comisión de las Naciones Unidas sobre la Ley internacional del Comercio, se reunió desde el 28 de Mayo hasta el 14 de Junio de 1996 y como consecuencia de dicha reunión tenemos el modelo de ley sobre el comercio electrónico. Este trabajo se apoya en los usos internacionales sobre contratos en materia de comercio electrónico. En el modelo de ley se establecen las reglas y

normas que validan y dan reconocimiento a los contratos formados electrónicamente y sienta las bases de desarrollo del comercio electrónico.

Con este antecedente se da la iniciativa para crear la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que se encuentra en vigencia a partir del 11 de abril del 2002. Esta ley basada en la Ley Modelo sobre el Comercio Electrónico (UNCITRAL) tiene los siguientes objetivos:

- Legalizar los contratos efectuados por medios electrónicos.
- Legalizar el uso de la firma electrónica.
- Legalizar el uso del documento electrónico.
- Establecer la figura de los certificados digitales, certificadores digitales, sus condiciones y responsabilidades.
- Establecer la institución Estatal de control y regulación en varios campos.
- Establece normas para la protección al consumidor, publicidad, privacidad y temas relacionados.
- Propone modificaciones al código penal ecuatoriano para considerar como delitos los denominados delitos informáticos que en la ley se describen.

Las empresas ecuatorianas han dado los primeros pasos para migrar sus negocios a la red, aunque no a la velocidad deseada y exigida por los tiempos actuales. Las empresas que más podrían favorecerse serían las de turismo debido a los montos alcanzables que pueden realizarse a través de las tarjetas de crédito, también porque el turismo siempre terminan con la visita física del usuario lo que permite firmar facturas, recibos, bouchers, etc.

También se cuenta con la Corporación Ecuatoriana de Comercio Electrónico CORPECE que es una ONG privada que involucra a los sectores públicos, privados, educativos, medios de comunicación y otros organismos cuyo único propósito es el de promover el e-commerce así como el uso de internet con fines empresariales.

Para el desarrollo del e-commerce es necesario ofrecer a los consumidores la confianza y seguridad en las transacciones electrónicas, al menos las mismas que ofrecen las que son hechas en papel. En la actualidad uno de los mecanismos que se ha creado y sigue en desarrollo para conseguir dicha confianza y seguridad, es la Firma Electrónica.

La Firma Electrónica permite la autenticación de las comunicaciones realizadas a través de Internet y da la posibilidad de comprobar la procedencia de los mensajes intercambiados y su integridad, así como evitar el repudio de la comunicación electrónica por su destinatario.

Según el Art. 13 del Capítulo I Título II de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se define a la Firma Electrónica de siguiente manera: “Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.”

Por consiguiente la Firma Electrónica es el mecanismo que facilitará, en gran medida el definitivo despegue del e-commerce en nuestro país. Pues este mecanismo se levanta como el más fiable para identificar a cada uno de los elementos que intervienen en una transacción electrónica, permitiendo saber si las partes involucradas son en realidad quienes dicen ser.

1.3.1.2.- Ventajas y Oportunidades

Es el comercio electrónico en internet nuestro futuro mercado de productos y servicios, aunque la mayoría lo crea, existe un pequeño grupo que todavía es desconfiado y no siente el cambio social en donde las TIC’s están transformando cualquier idea tradicional. Es por este motivo que a continuación se describirán algunas de las ventajas y oportunidades que se alcanzarían con el e-commerce.

El e-commerce le permite al empresario:

- Rebajar considerablemente los costos de inversión en los presupuestos publicitarios.
- La posibilidad de reducción de precios por el bajo costo del uso de Internet en comparación con otros medios de promoción, lo cual implica mayor competitividad.
- Acercarse más a los clientes, es decir mayor interactividad y personalización de la oferta.
- El diseño y desarrollo de ventas electrónicas.
- Globalización y el favorable acceso a mercados potenciales de millones de clientes ávidos para comprar los productos que se ofertan.
- Les permite crear e implantar tácticas en la venta de productos para fortalecer la fidelidad en los clientes.
- Enfocarse hacia un comercio sin el uso del papel, lo cual es posible a través de los mecanismos, modelos, protocolos y demás seguridad que son posibles de implantarse en el medio.
- El bajo riesgo de inversión en comercio electrónico.
- La forma más rápida de actualización de la información de productos y/o servicios que una organización ofrecen una página web, esto es promociones, descuentos, ofertas, etc.
- El obtener nuevas oportunidades de negocio, pues con la sola presencia en el mercado se estará a la altura de ofrecer los productos y/o servicios como las grandes multinacionales.
- La reducción del costo real al hacer estudios de mercado.
- Todas estas ventajas se ven reflejadas en la competitividad que la empresa requiere para dirigirse a un mercado globalizado, y los beneficios directos sobre el consumidor, que en la actualidad sin duda dispone de un poder de elección entre los mejores productos y/o servicios disponibles en la red.
- Desaparecer los límites de espacio o geográficos para su negocio.
- Le permite estar disponible las 24 horas del día, siete días a la semana y todos los días del año.

- La reducción de un 50 % en costos de la puesta en marcha del comercio electrónico si comparamos los costos con el comercio tradicional.
- Hacer de los negocios la forma más sencilla de trabajar con sus clientes.
- La reducción considerable de inventarios.
- Le permite agilizar las operaciones del negocio.
- Puede proporcionar nuevos medios para encontrar y servir a sus clientes.
- Incorporar internacionalmente nuevas estrategias de relaciones entre clientes y proveedores.

No solo el empresario es el único que obtiene ventajas del comercio electrónico, también el cliente pueden favorecerse de estas oportunidades, pues el propósito es abrir la puerta hacia el mercado global donde todos puedan tener las mismas oportunidades de comprar y vender. Las ventajas que tienen los clientes se detallan a continuación:

- Un medio que el World Wide Web que le da poder al consumidor de elegir en un mercado global a partir de sus necesidades y posibilidades.
- Por medio de las páginas brinda información pre-venta y la posibilidad de probar el producto antes de adquirirlo.
- La gran ventaja de realizar los pedidos de forma inmediata.
- El servicio pre y post-venta on-line.
- La posibilidad de reducción de la cadena de distribución, lo que le permite adquirir un producto y/o servicio a un mejor precio.
- Mayor interactividad y personalización de la demanda.
- La ventaja de tener información inmediata sobre cualquier producto y/o servicio.
- Además de la disponibilidad de acceder a la información en el momento que así lo requiera pues está disponible las 24 horas del día y durante todo el año.

1.3.1.3.- Tipos de Comercio Electrónico

El interés de muchas organizaciones es mejorar su presencia en internet para que sus ventas se incrementen, para efectuar el e-commerce se necesitan de varios agentes implicados y de acuerdo a estos se puede subdividir en cuatro categorías:

1) Empresa-Empresa, es la denominada Bussines to Bussines (B2B), está orientada a las transacciones entre empresas, lo que quiere decir es la venta de un producto y/o servicio de una empresa a otra. Está establecida desde hace bastantes años, usando en particular Intercambio Electrónico de Datos o Electronic Data Interchange (EDI) sobre redes privadas o de valor añadido.

En este tipo de comercio principalmente se da el intercambio de datos antes que las transacciones monetarias, comprende las relaciones comerciales de la empresa con sus proveedores y distribuidores, incluyendo envío de información en procesos comerciales con los proveedores y socios como puede ser pedidos pagos, servicios básicos de adquisición, gestión de logística, etc.

El objetivo principal es la automatización de la gestión empresarial y la eliminación de costos asociados como la facturación, gastos de papel, comunicación, etc.; esto haría que se multiplique los beneficios de las empresas y así se ofrezca al empresario mayor control de sus procesos.

2) Empresa-Consumidor, llamada también Bussines to Consumer (B2C) y se trata de la venta directa de la empresa al consumidor final. Generalmente se utilizan mecanismos de pago electrónico, algunas aplicaciones de internet que se pueden nombrar en este tipo de comercio son: juegos en línea, compras en supermercados, venta de libros, autos, acceso a la información, homebanking, entre otras.

Existe un contacto directo entre fabricantes y consumidores lo que permite eliminar intermediarios en el proceso de compra, esto se verá reflejado enormemente en el precio final del producto, ya que su costo sería inferior al normal. En los próximos años se espera que la venta directa a través del internet mueva grandes volúmenes de negocios en el mundo.

3) Empresa-Administración o Bussines to Administration (B2A), en este tipo de comercio se cubre toda clase de transacciones entre las empresas y las organizaciones gubernamentales. Esta categoría es bastante importante ya que se piensa que a través de ella se podrá promover la calidad, la seriedad y el crecimiento del comercio electrónico. El B2A puede crecer rápidamente si los gobiernos la usan para sus operaciones, para promover la calidad y el crecimiento del comercio electrónico. Además, las administraciones pueden ofrecer también la opción del intercambio electrónico para transacciones como determinados impuestos y el pago de tasas corporativas.

4) Consumidor-Administración, que se la conoce como Consumer to Administration (C2A), esta categoría es la que más dificultades parece encontrar para su emergencia. Sin embargo a medida que se extiendan las categorías anteriores la administración podrá extender las interacciones electrónicas a áreas tales como los pagos de pensiones, el asesoramiento, o las devoluciones de tasas, etc.

1.3.1.4.- Niveles del Comercio Electrónico

Los diferentes niveles de comercio electrónico dependen de la cantidad de acciones que se realizan electrónicamente. Los niveles básicos de e-commerce son los que se detallan a continuación:

1) Presencia electrónica, este nivel consiste simplemente en "estar ahí", en la disposición de una página web o de una simple dirección de correo electrónico, pues en el caso de que algún cliente o proveedor desee conocer dicha

información o algún dato nuestro podrá ponerse en contacto con la página o dirección dada.

2) Promoción de la empresa, dicho nivel implica la utilización de un paso más: este es el de utilizar Internet de forma activa para enviar información a clientes potenciales, en este nivel se utilizan servicios relacionados con el correo electrónico como mailings y newsletters.

3) Servicios pre/post ventas, aquí se ofrecen servicios concretos a los clientes reales, dicho servicios incluyen formularios para pedidos o reclamaciones, carros de compra, informaciones sobre tarifas, sistemas de envío o situación logística de los pedidos, etc.

4) Transacciones sencillas, es cuando un usuario se propone y acepta la mensajería electrónica, es decir utiliza los formularios web como un medio efectivo para hacer pedidos de productos y/o servicios.

5) Distribución electrónica nacional, este nivel se da cuando los productos y/o servicios que ofrece una empresa son completamente digitalizables y por lo tanto pueden ser expedidos electrónicamente.

6) Pagos nacionales, en este se utilizan sistemas de pago on-line, es decir las firmas electrónicas que permiten realizar una contratación efectiva.

7) Distribución electrónica internacional, este es parecido a la distribución electrónica nacional pero a través de fronteras aduaneras, lo que implica una mayor cuidado a los problemas jurídicos y de seguridad.

8) Pagos internacionales, se parece a los pagos nacionales pero a través de fronteras aduaneras, lo que significa una mayor consideración a problemas jurídicos y de seguridad.

9) Procesos comerciales compartidos, en este nivel se incluyen la utilización de ciertos servicios de Internet por distintas empresas que se agrupan con mayor o menor formalidad jurídica para la prestación conjunta de servicios a terceros.

1.3.2.- SEGURIDAD EN TRANSACCIONES ELECTRÓNICAS

El despliegue que se está produciendo en Internet últimamente, da motivo para pensar en prometedoras expectativas de su utilización como vehículo de comercio, ya que el acceso económico de millones de usuarios en todo el mundo hace de la red el mejor mercado global en el que se pueda comerciar. El solo pensar en la posibilidad de ofrecer un producto y/o servicio en los cinco continentes, los beneficios serían altos y lo único que sería necesario e imprescindible es un servicio de posventa, es decir un transporte capaz de llegar a donde el cliente quiera y por supuesto la seguridad en el medio del pago.

La capacidad de realizar transacciones comerciales de compra-venta se asocia a la capacidad de ejecutar los pagos correspondientes. Internet la novedad de los pagos a distancia física, además del cambio cultural y legal entre las partes geográficamente distantes y con ello la posibilidad de fraude, engaño o simplemente errores y malentendidos.

Internet ofrece acceso diversificado, un mercado global de compradores y vendedores, en el que se puede hablar de economías de escala capaces de rentabilizar una fuerte inversión con bajos costos por la vía del uso masivo. Esto implica la necesidad de mecanismos ampliamente aceptados y fácilmente accesibles.

La amplia difusión de las técnicas supone su exposición a delincuentes informáticos cuyo beneficio, lo obtienen del abuso de los mecanismos de pago, es tan grande la amenaza que es necesario restablecer fuertes inversiones buscando soluciones de seguridad que puedan garantizar las operaciones de los

usuarios de la red, dichas inversiones que prometen una elevada rentabilidad pese a su elevado riesgo.

Todo sistema de pago deberá contar con las siguientes propiedades:

1) Confidencialidad, es un servicio esencial para cualquier transacción económica. Si existe un cliente, un comercio y un Banco involucrados en una transacción, lo más conveniente sería que nadie lo supiera a excepción de los involucrados, el banco no conociera el detalle del pedido, el comercio no conociera los datos de la cuenta del cliente y el cliente no conociera los datos de la cuenta del comercio.

2) Anonimato, las transacciones electrónicas tienen una fuerte tendencia a dejar rastro, no así con el papel moneda que no tiene nombre, ni apellidos. El anonimato está estructurado de dos componentes: el primero el inmediato de que no se sepa que se adquiere alguna cosa y el segundo a medio plazo como es el que no se pueda identificar patrones de compra.

3) Integridad, se trata de un servicio básico frente a fraudes introducidos por terceras partes o por las mismas partes que ven el imposible cumplimiento del negocio. Es la prohibición de terceras partes para modificar el contenido de un intercambio de datos.

4) Autenticación del remitente, Solo en el caso de que el pago se haga con un valor indiscutible, es decir efectivo; en todos los demás casos el que paga deberá identificarse claramente, para luego pedir cuentas si el pago no llega a concretarse.

5) Autenticación del receptor, Asimismo los compradores deberán conocer la identidad del vendedor, excepto que el producto y/o servicio se remita en el instante de la transacción.

6) Irrenunciabilidad o no repudio, está relacionada conque una de las partes no renuncie su responsabilidad, aquí es donde aparece un tercero que da fe de la identidad y de los deseos de una o de ambas partes.

Con estas características habría que crear escenarios comerciales lógicos con la capacidad de al menos reproducir la mayor parte de ellas sino es que todas, pues para que el comercio electrónico triunfe en Internet depende en gran parte de que exista confianza en las transacciones electrónicas por parte del comprador así como del cliente.

Los usuarios de las TICs, deben saber que la información está protegida, y que puedan verificar a quién realmente le están transmitiendo o de quién están recibiendo información, y que no sufran de modificaciones no autorizadas.

Las nuevas tecnologías que hacen posible la sociedad de la información tienen a la información que es tratada digitalmente, es decir, codificada en unos y ceros. El fax, el correo electrónico, el vídeo, la televisión, la telefonía móvil, la transferencia electrónica de fondos (EFT), las tarjetas inteligentes, la telemedicina etc. Todo ello funciona con la información codificada en bits (unos y ceros) y transmitidos a través de cable, fibra óptica, satélites y almacenados como unos y ceros en medios magnéticos u ópticos.

Sin embargo los bits son vulnerables, ya que son accesibles fácilmente, la codificación en bits no aporta ningún impedimento para el conocimiento de la información que representan, no son seguros y no tiene personalidad, todos son iguales. La modificación, sustitución, borrado o destrucción de cualquiera de ellos puede modificar total o parcialmente, el origen, el destino, o el contenido de la información que representan.

De esta forma para evitar o protegerse de los errores que pudiera provocar el canal de comunicaciones por donde transitan los bits, se emplean las técnicas de detección y corrección de errores. Dichas técnicas son estándares de las

telecomunicaciones digitales, perfectamente conocidas e implementadas por los fabricantes, operadores y usuarios de las TIC.

No obstante, la protección contra el conocimiento no autorizado y la manipulación interesada de los bits, o lo que es lo mismo, de las comunicaciones y archivos digitales, se consigue con la criptología.

La criptología moderna, es decir la que se ha desarrollado a partir de 1976, es la tecnología que hace posible implementar las medidas de seguridad necesarias para crear la confianza en la Infraestructura Global de la Información.

1.4.- CRIPTOGRAFÍA Y SEGURIDAD DE DATOS

1.4.1.- CRIPTOLOGÍA

La criptología se define como aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Por tanto esta ciencia implica a la criptografía la que maneja datos, texto e imágenes, la criptofonía que manipula la voz y el criptoanálisis, ciencia que estudia los pasos y operaciones orientados a transformar un criptograma en el texto original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave.

1.4.2.- CRIPTOGRAFÍA

Esta palabra toma la denominación del griego Criptos que significa extraño y Graphos que representa escritura; por lo tanto se puede traducir como la manera de escribir raro.

Cifrar por tanto consiste en convertir una información (texto claro) en otra incomprensible (texto cifrado) según un procedimiento y usando una clave determinada, con esto se pretende que sólo quién conozca dicho procedimiento y

clave pueda acceder a la información original. La operación inversa se denomina descifrar.

La criptografía es esencial para realizar intercambios de información seguros en intranets, extranets e Internet. Desde un punto de vista empresarial, las funciones de seguridad que permite la criptografía son autenticación, que asegura al destinatario de un mensaje que el remitente es quien dice ser; confidencialidad, que asegura que un mensaje sólo puede ser leído por el destinatario previsto e integridad, que asegura que durante la transmisión no se ha alterado el destinatario de un mensaje. Desde un punto de vista técnico, la criptografía es la ciencia que se encarga de la protección de datos mediante la transformación matemática de los mismos a un formato ilegible.

Estos esquemas de seguridad deberían utilizar criptografía de clave secreta o criptografía de clave pública, aunque el más recomendable es el segundo ya que con la ayuda de otros elementos como certificados digitales, autoridades de certificación, un buen sistema de gestión de claves y con una definición clara de las políticas que permitan poner en funcionamiento este esquema se logrará el objetivo propuesto.

Cuando se utiliza criptografía de clave secreta o simétrica el sistema para generar las claves es muy sencillo puesto que no se requiere de una gran infraestructura, el inconveniente está en la difusión de las claves a los usuarios involucrados pues se debe tener cuidado de que intrusos puedan interceptarla.

La diferencia cuando se utiliza criptografía de clave pública o asimétrica está en la gestión de claves especialmente la pública porque como lo dice está a disposición de cualquier persona, en esta parte es donde se debe contar con autoridades de confianza conocidas como Autoridades de Certificación (CA Certification Authority) que emiten certificados firmados con su clave secreta bajo un estándar que en su mayoría es X.509 y que es válido para un cierto tiempo.

Si bien el origen de los sistemas criptográficos tienen carácter militar, en la actualidad su utilidad ha desbordado este campo, en áreas donde la información es tan valiosa como la informática.

1.4.3.- SISTEMAS CRIPTOGRÁFICOS

1.4.3.1.- Sistemas de Clave Simétrica

Son los sistemas más tradicionales, es decir, se utiliza una determinada clave en la transformación de la información encriptada así como para conseguir desencriptarla, el problema reside en la necesidad de que todas las partes conozcan la clave.

Sus principales características son:

- Rápidos y fáciles de implementar.
- La clave de cifrado y descifrado es la misma
- Cada par de usuarios tiene que tener una clave secreta compartida.
- Una comunicación en la que intervengan múltiples usuarios requiere muchas claves secretas distintas.

Actualmente existen dos métodos de cifrado para criptografía de clave secreta, el cifrado de flujo y el cifrado en bloques.

En el cifrado de flujo el emisor A, con una clave secreta y un algoritmo determinístico (ALG), genera una secuencia binaria (*s*) cuyos elementos se suman con los correspondientes bits de texto claro *m*, dando lugar a los bits de texto cifrado *c*, Dicha secuencia (*c*) es la que se envía a través del canal. En la recepción está B, con la misma clave y el mismo algoritmo determinístico, genera la misma secuencia cifrante (*s*), que se suma con la secuencia cifrada (*c*), dando lugar a los bits de texto claro *m*. Los tamaños de las claves oscilan entre 120 y 250 bits. A continuación se muestra un esquema del funcionamiento del cifrado de flujo.

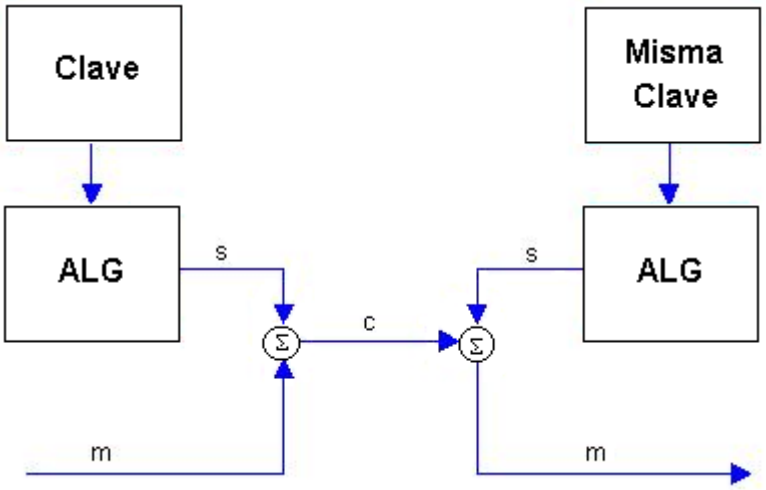

Figura 1.1

El cifrado de bloque se compone de cuatro elementos: la transformación inicial por permutación, una función geográfica débil, una transformación final para que las operaciones de encriptación y desencriptación sean simétricas y el uso de un algoritmo de expansión de claves que tiene como objeto convertir la clave de usuario, normalmente de longitud limitada entre 32 y 256 bits, en un conjunto de subclaves que puedan estar constituidas por varios cientos de bits en total.

1.4.3.2.- Sistemas de Clave Asimétrica, Pública o PKI

En estos sistemas asimétricos de cifrado o de clave pública, cada usuario dispone de dos claves, una pública, que debe estar a disposición para que los demás puedan comunicarse con él, y una privada que debe mantener en secreto.

Cuando un usuario desea mandar un mensaje protegido, cifra el mensaje con la clave pública del destinatario. De esta manera, sólo el destinatario puede descifrar, con su clave secreta el mensaje cifrado. Estos sistemas responden a la necesidad de comunicación en redes muy grandes, donde la gestión de claves secretas es inviable, además, ésta es la gran revolución de la criptografía moderna, solucionan los problemas de autenticación de emisor y receptor, proporcionan la posibilidad de firmar digitalmente los mensajes, y garantizan el contenido de los mismos.

Existen diferentes sistemas de clave pública pero el más extendido y el que se considera un estándar de facto es el RSA (algoritmo de encriptación asimétrica). Este criptosistema, creado en 1978 por Rivest Shamir y Adleman, de aquí sus iniciales, utiliza esencialmente la tarea de factorizar que resulta un poco difícil.

Así pues, parece que el problema de la seguridad quedaría solucionado, no obstante padece de un punto débil y es cuando se pregunta ¿cómo se asocian los pares de clave pública y clave privada correctos en sí mismos con personas físicas?. La solución la aportan las autoridades de certificación (notarios electrónicos) que son entes fiables y ampliamente reconocidos que firman las claves públicas de las personas, rubricando con su firma su identidad.

Como se observa, la clave pública no ha resuelto del todo el problema de la seguridad, ya que si bien ha contribuido a reducir el número de claves necesarias para comunicarse con múltiples usuarios, ha añadido el problema de la confianza con una tercera parte certificadora.

En definitiva, una PKI incluirá una o varias autoridades de registro para certificar la identidad de los usuarios; una o varias autoridades de certificación que emitan los certificados de clave pública; un repositorio de certificados, accesible vía web u otro medio, donde se almacenen los certificados; las listas de revocación de certificados (CRL), donde se listan los certificados suspendidos o revocados; y, por supuesto, los propios certificados.

Lo que debería hacerse es pensar en que una PKI puede ser la respuesta al futuro. Eso sí, no hay que olvide definir correctamente cuáles son sus necesidades exactas y entonces elegir la estrategia de una PKI que mejor se adapte a su modelo de negocio. Exija soluciones integrables centrados en su proceso de negocio, sólo entonces la tecnología probará ser su mejor aliado.

II. EL INTERNET Y SUS ESTÁNDARES DE SEGURIDAD

2.1. ORGANISMOS INVOLUCRADOS CON EL TEMA

El internet en su origen era un proyecto exclusivo para una sociedad específica en la que la seguridad estaba prácticamente garantizada, pero su evolución ha transformado esta red de redes en la que controlar la identidad de cada usuario que ingresa a este mundo se vuelve realmente difícil.

El incremento de personas que encuentran que el internet es el medio más óptimo para realizar sus procesos administrativos, financieros y comerciales, en los que se hace imprescindible la transferencia de datos confidenciales, ha convertido a la seguridad en uno de los principales condicionantes para lograr la consolidación y aprovechamiento de las funcionalidades de la red.

Para que el funcionamiento de esta gran red tenga la más alta seguridad se han creado normas y estándares por organizaciones que desde hace algún tiempo vienen dictaminándolas con la finalidad de utilizarlas en el mundo de las telecomunicaciones, la informática, el e-commerce, etc.

Estas organizaciones son las encargadas de entregarnos los estándares que maneja la comunidad de Internet, dichos estándares son analizados, estudiados y probados de acuerdo al objetivo que tengan y luego serán publicados para su divulgación y desde luego para que sean utilizados.

A continuación se dará una visión global de las organizaciones, que de cierta forma deberían ser parte de la cultura general de las personas que pertenezcan al mundo de la informática, pues ayudará a saber quién, que países o que empresas mueven y manejan este mundo, se conocerá quienes son los que en parte ha desarrollado el estilo de vida de las sociedades involucradas con la telemática y las redes.

2.1.1.- ISO

La ISO siglas de International Organitation for Standardization que en español se la denomina Organización Internacional de Estandarización, es una federación mundial integrada por los cuerpos de estandarización nacionales en más de 140 países. Es una organización no gubernamental establecida en 1947, su misión es promover el desarrollo de los estándares y actividades relativas en mundo, con el objetivo de facilitar el intercambio internacional de los productos y servicios, además el desarrollo y cooperación de las actividades científicas, tecnológicas y económicas.

En cuanto al nombre, ISO se deriva de la palabra griega “isos” que significa igual, de la cual se toma el prefijo ISO. Su sede principal se encuentra en Ginebra y es la que establece o fija los estándares internacionales, abarca todos los campos excepto la electricidad y la electrónica, pues este le pertenece a la International Electrotechnical Commission (IEC), respecto al procesamiento de la información la ISO y la IEC crearon la JTC1, Joint Technical Committee para la tecnología de información.

La ISO desarrolla su trabajo mediante 160 comités técnicos y 2300 subcomités, está constituida por organizaciones de estándares de más de 75 países, las cuales sirven como secretariados para los cuerpos técnicos. Los resultados de los trabajos de la ISO son acuerdos internacionales publicados y que se convierten en estándares internacionales.

La Organización Internacional de Estandarización emite los estándares de acuerdo a los siguientes principios:

1) Consenso, se toma en cuenta los puntos de vista de todos los interesados, en para el caso serían: fabricantes, vendedores, usuarios, grupos de

consumidores, laboratorios de análisis, gobiernos especialistas y las organizaciones de investigación.

2) Aplicación Industrial Global, se refiere a las soluciones globales para la satisfacción de los clientes mundiales y las industrias.

3) Voluntario, la estandarización internacional es conducida por el mercado y por consiguiente basada en el compromiso voluntario de todos los interesados en el mercado.

La influencia de cada miembro depende de los indicadores económicos como el producto interno bruto (PIB) y el valor de las exportaciones e importaciones, con lo que se deduce que los países desarrollados son los que realmente imponen sus reglas

2.1.2.- NSA

Proviene del acrónimo National Security Agency, Agencia de Seguridad Nacional pertenece a los Estados Unidos, fue creada por el presidente Truman en 1952, depende del Departamento de Defensa, y su objetivo era interceptar e interpretar cualquier comunicación que hiciera peligrar la seguridad de los EE.UU.

La NSA se dedica a la investigación criptológica dividiéndola en dos partes, en la primera diseña algoritmos de cifrado seguros para proteger las comunicaciones de los Estados Unidos, y en la segunda diseña técnicas criptoanalíticas capaces de romper cualquier comunicación de interés, con lo que se puede deducir que la NSA tiene conocimientos de algoritmos criptográficos con muchos años adelante de lo que se conoce en la actualidad.

La responsabilidad de la NSA es el continúo hacer y deshacer códigos. A principios de los años 70, matemáticos y científicos que trabajaban para las

fuerzas armadas norteamericanas empezaron a desarrollar el estándar de encriptamiento de datos denominado Data Encripytion Standard (DES).

En este tiempo la criptografía empezó a verse como un campo de investigación y desarrollo, pues la cantidad de datos transmitidos en redes abiertas era mayor, especialmente en grupos no armados. La NSA tiene a su disposición durante las 24 horas del día, dos mil millones de mensajes y cuenta con la ayuda de un potente sistema de inteligencia.

A través de un plan denominado “P-415 Echelon”, la NSA dispone de una red de alrededor de 120 satélites de comunicación (Intelsat), que envía los datos captados hacia unas 50 estaciones terrestres, esparcidas por todo el planeta, las cuales transmiten a la oficina central de la agencia. Echelon es un sistema de interceptación de comunicaciones a escala mundial en las que participan los departamentos de inteligencia de cinco países, bajo un acuerdo llamado “AKUSA”. En los últimos años el sistema se ha extendido a Internet captando los datos y mensajes que navegan en el ciberespacio.

La NSA emplea programas robotizados informáticos para recoger información y ficheros en función de parámetros preseleccionados como servidores, bases de datos y portales de internet. Además cuenta con computadoras especiales denominadas Diccionarios, que son capaces de almacenar un amplio registro de datos sobre objetivos específicos partiendo de un nombre, una dirección, un número de teléfono o ciertos datos seleccionados. También utiliza un moderno sistema de detección de voz.

La NSA depende del Departamento de Defensa, posee un Museo de Criptografía, donde se exhibe a la máquina Enigma utilizada por los alemanes en la última Guerra Mundial para escribir en forma cifrada. La NSA tiene estrecha relación con la NIST (National Institute of Standars and Technology), ambos regula el uso, control y exportación del software y hardware vinculado con la privacidad y seguridad.

2.1.3.- NCSC

El National Computer Security Center, forma parte de la Agencia de Seguridad Nacional (NSA), es responsable del programa de computación del Gobierno de los Estados Unidos, ésta institución evalúa productos de seguridad, es decir hardware y software comerciales, además efectúa trabajos de investigación y proporciona asesoría técnica.

El NCSC es famoso por la serie de libros que ha publicado referente a la seguridad informática, esta colección de libros se los conoce popularmente como los libros arcoiris, debido a que cada portada posee un color diferente. El libro más famoso de esta colección es el conocido Libro Naranja, oficialmente se lo llama Department of Defense Trusted Computer System Evaluation Criteria, este documento pretende definir los requisitos de seguridad, de tal modo que sea fácil para el desarrollador de sistemas medir objetivamente la seguridad de los mismos.

Este organismo se centra en la seguridad y poco trata sobre la criptografía, vale la pena mencionar que otro libro muy significativo es el Libro Rojo que oficialmente se lo denomina Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, que como su nombre lo dice interpreta los requisitos del Libro Naranja para redes.

2.1.4.- NIST

NIST es el acrónimo de National Institute of Standards and Technology, el cual pertenece al Departamento de Comercio de los Estados Unidos, anteriormente se lo conocía como NBS (National Bureau of Standards) y fue creado en el año de 1901.

El NIST promueve la interoperabilidad y la definición de estándares abiertos para conseguir el desarrollo de la industria informática, y para cumplir con esto publica una serie de estándares y recomendaciones con la finalidad de que sean aceptadas y adoptadas por las industrias. Los estándares oficiales son publicados como FIPS(Federal Information Processing Standards).

El NIST fue creado para apoyar a la industria en el desarrollo de la tecnología necesaria para mejorar la calidad de los productos, para modernizar los procesos de fabricación, para asegurar que los productos sean confiables y así facilitar la rápida comercialización de los productos basados en los recientes descubrimientos de las ciencias.

El programa del NIST en materia de tecnologías de la información y comunicación comprende varios proyectos que se clasifican en áreas como: Tecnologías de redes avanzadas, Sistemas y servicios de alto nivel de ejecución, Diagnósticos del software y pruebas de conformidad, Seguridad de los computadores, Acceso a la información e interfaces para usuarios

Un aporte importante de este organismo es el que haya convocado a un concurso para tener un sistema simétrico que sea seguro y pueda utilizarse en los próximos 20 años como un estándar. Se aceptaron 15 candidatos, de cuales el NIST seleccionó al algoritmo "RIJNDAEL" como futuro estándar AES. Para el año 2000, este algoritmo se hizo público, actualmente es el estándar de cifrado, se lo seleccionó por una excelente combinación de seguridad, sencillez, flexibilidad, velocidad y eficiencia tanto en memoria como en puertas lógicas.

2.1.5.- RSA Data Security, Inc

Fundada en 1982 por los creadores del algoritmo RSA, fundamentalmente se dedica a la comercialización, desarrollo y licenciamiento de la patente RSA, posee

licencias de RC2 y RC4, desarrolla los estándares criptográficos conocidos como PKCS en el laboratorio criptográfico, RSA Laboratories.

Esta compañía posee más de 9000 clientes alrededor del mundo, es reconocida como el socio estratégico en el e-security, las compañías más grandes y exitosas tienen su influencia en todo lo referente a los negocios en Internet.

Las soluciones que ofrece el RSA security's son de autenticación, manejo de acceso a la web, kit de herramientas para la seguridad. Estas herramientas ayudan a las organizaciones a obtener más oportunidades, así como obtener mejoras operacionales, mientras se está protegiendo la información crítica contra el acceso no autorizado y otras formas de acceso mal intencionado.

Todo los productos que ofrece RSA Data Security van a la vanguardia de la tecnología y proliferación del e-business. Hoy en día muchas redes privadas y públicas se han unido para redefinir a sus organizaciones y orientar sus aplicaciones hacia la Web, RSA Security's está evolucionando para cubrir estas necesidades.

Con una historia de más de 20 años de excelente innovación y actuación, las soluciones de autenticación de RSA security's siguen siendo para muchas compañías las mejores para proteger sus recursos informáticos, ofrece muchas opciones de autenticación para las empresas como acceso mediante tarjetas inteligentes o la emisión de certificados digitales, para la identificación de usuarios en aplicaciones a través de VPNs (Redes Privadas Virtuales), correo electrónico, intranets, extranets, servidores web y otros recursos de la red.

RSA Security's permite a las organizaciones mejorar sus relaciones comerciales con el acceso a aplicaciones web basado en múltiples servicios, la funcionalidad con que se diseñan los productos permite a los usuarios navegar en forma transparente por múltiples aplicaciones y dominios, con esto se logrará que las empresas cumplan sus objetivos comerciales.

Dentro de sus productos figura también la encriptación y la firma digital en muchas aplicaciones comerciales como navegadores web, dispositivos inalámbricos, servidores, correo electrónico, VPN (Redes Privadas Virtuales), etc., con la utilización de normas como SSL, S/MIME, Ipsec.

2.1.6.- VERISIGN,INC

Es una compañía de Estados Unidos fundada en 1995 como una parte de RSA Data Security, Inc. Es el principal proveedor mundial de certificados. Es una de las autoridades de certificación más importantes en cualquier navegador. Desarrolla soluciones integradas en lo que se refiere a comercio electrónico.

Provee de confianza digital a personas de cualquier parte del mundo mediante cuatro ofertas centrales que son: servicios de presencia web, servicio de telecomunicaciones, servicio de seguridad y servicio de pago, impulsado por una infraestructura global que maneja billones de conexiones de red y transacciones en el día. Verisign, Inc busca participar en el desarrollo de políticas alrededor del mundo que beneficien los intereses en el Internet y el comercio electrónico.

Verisign es una empresa certificadora especialmente para dar seguridad en el comercio electrónico y firma digital, por esta razón es que se han creado las Issuing Authorities o IA, que son las autorizadas por Verisign, Inc para que funcionen como terceras partes de confianza, emitiendo, gestionando o revocando certificados de acuerdo a las empresas. Existen también los LRA (Local Registration Authority) o autoridades de registro local que cumplen las mismas funciones.

En el proceso de certificación se encuentran los servicios de registro, autenticación, emisión, revocación y suspensión de los certificados. Verisign ofrece tres niveles de servicios de certificación y cada uno brinda funcionalidad y

seguridad. Cumplidos los requisitos que se exigen se emite el certificado o a su vez un borrador para la aceptación de interesado.

Los tipos de certificado de clase 1, son emitidos electrónicamente, relacionan el nombre de usuario y su e-mail con el registro que lleva Verisign, no autentican la identidad de la persona. Los certificados de clase 2, se emiten a personas físicas, confirman la veracidad de la información cuando sea ingresada en una aplicación, para ello acude a una base de datos de usuarios reconocida. Se utiliza para validación de software, suscripciones on-line. Los certificados de clase 3, son emitidos a personas físicas, organizaciones públicas y privadas, asegura la identidad física del suscriptor o la existencia de la organización ante un LRA o notario. Son utilizadas en comercio electrónico.

Verisign desarrolla y entrega soluciones de seguridad basadas en estándares que satisfagan los requerimientos de sus clientes, junto a IBM y Microsoft han desarrollado una especificación de seguridad denominada Web Services Security (WS-Security). Este es uno de los estándares para soportar, integrar y unificar múltiples modelos, mecanismos y tecnologías de seguridad.

Esta especificación presentada por estas tres organizaciones define un grupo estándar de extensiones SOAP (Simple Object Access Protocol) o de encabezados de mensajes, el que se puede utilizar para implantar integridad y confidencialidad en aplicaciones de servicios web.

2.1.7.- IETF

El Internet Engineering Task Force cuya principal preocupación es el desarrollo de nuevos estándares, arquitecturas y especificaciones que solucione los problemas técnicos que surgen del Internet. Esta organización es una gran comunidad abierta formada por grupos de diseñadores de red, operadores, vendedores, e investigadores que buscan la evolución y el buen funcionamiento del Internet.

El trabajo técnico real de IETF se lo hace en grupos que son organizados por tema en varias áreas como: seguridad, transporte, asignación de rutas, etc. Este trabajo es manejado por lista de correo y luego se celebran reuniones de dichos grupos tres veces por año.

Cada grupo de trabajo tiene un Area Director's (ADs), Estos directores son miembros del Internet Engineering Steering Group (IESG), este grupo es el que maneja todos los estándares y es el que se encarga de ratificar y corregir los Drafts o borradores de los grupos de trabajo de la IETF, es decir, da el visto bueno para que un draft se convierta en RFC (Request for Comments).

Existen otros organismos relacionados con el Internet Engineering Task Force (IETF) que se los menciona a continuación:

IAB (Internet Architecture Board), es la responsable de la supervisión y coordinación de las áreas de actividad de la IETF, este organismo busca una consistencia e integridad en las arquitecturas de las propuestas e investigaciones que realizan los grupos de la IETF.

IANA (Internet Assigned Numbers Authority) Su misión es mantener actualizado los servicios asociados a los puertos TCP y los tipo MIME. Se encarga de mantener el sistema de nombres principal (root domain name system) que actualmente está supervisado por la ICANN (Internet Corporation for Assigned Names and Numbers).

RFC-Editor se encarga de formatear, editar y publicar tanto los I-D (Internet Drafts) como RFCs trabajando en conjunto con la IESG. El trabajo de RFC-Editor es supervisado por la IAB.

2.2. ANÁLISIS DE LOS ESTÁNDARES PARA TRANSACCIONES EN INTERNET

2.2.1.- BREVE HISTORIA DE LA ESTANDARIZACIÓN

A comienzos del siglo XIX el continente Europeo vivía una etapa de agitación; los efectos de la revolución industrial se estaban haciendo evidentes más con el inicio la máquina de vapor y el ferrocarril. El primer problema de estandarización surgió con los rieles del ferrocarril; pues había que ponerse de acuerdo en las dimensiones, material y las demás características de las vías por donde se desplazaría. Con el surgimiento del telégrafo y sus evidentes beneficios se vio la imperiosa necesidad de difundir noticias y mensajes de manera rápida y eficiente. El ferrocarril y el telégrafo convirtieron de manera notable a la Europa del Siglo XIX.

Con la finalidad de encontrar una estructura y forma de funcionamiento que permita conocer los problemas de las nuevas tecnologías de comunicación, así como las demandas de los usuarios, en el año de 1865 se fundó la Unión Internacional de Telegrafía denominada, por sus siglas en inglés ITU. Esta fue la primera organización internacional e intergubernamental que se creó, siendo el primer paso y por ende el primer esfuerzo para estandarizar las comunicaciones en varios países.

En 1884 en Estados Unidos se fundó la IEEE (Institute of Electrical and Electronics Engineers), este organismo en la actualidad es el encargado de la promulgación de estándares para redes de comunicaciones. Unos pocos años más tarde, en 1906, en Europa se funda la IEC (International Electrotechnical Commission), ésta organización es la que define y divulga estándares para ingeniería eléctrica y electrónica.

En 1918 se crea el ANSI (American National Standards Institute), otro organismo de gran trascendencia en la estandarización estadounidense y desde

luego alrededor de todo el mundo. Para el año de 1932, se fusionaron dos entidades de la antigua ITU, con lo que se crea la Unión Internacional de Telecomunicaciones, que en la actualidad es una entidad de gran importancia debido a que es la encargada de promulgar y adoptar estándares de telecomunicaciones.

Siguiendo con la historia, en 1947, cuando había pasado la segunda guerra mundial, se funda la ISO (International Organization for Standardization), una organización que abarca ampliamente a los estándares de varias áreas del conocimiento.

Hoy por hoy existe una gran cantidad de organizaciones y entidades que definen nuevos estándares y que están a la vanguardia de las tecnologías de información y comunicación, para satisfacción y beneficio los usuarios de dichas tecnologías.

2.2.2.- CONCEPTO DE ESTÁNDAR Y SUS TIPOS

2.2.2.1.- Estándar

A un estándar, según como lo define la ISO "son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito".

Según lo anterior un estándar de seguridad para internet se lo puede definir como un conjunto de especificaciones, reglas y recomendaciones técnicas que regulan los procesos y servicios que ofrece internet. Los estándares deberán ser documentados y probados, con la finalidad de que sean difundidos y utilizados por organizaciones o personas que necesiten de una guía al momento de implementar e implantar uno de estos estándares.

2.2.2.2.- Tipos de Estándares

Los estándares pueden ser de tres tipos: de facto, de jure y los propietarios.

Los estándares de facto son los que tiene una alta aceptación e introducción en el mercado, pero todavía no son oficiales. Dichos estándares son promulgados por comités orientados por una organización o compañía que quiere sacar un producto o servicio nuevo, y si este tiene acogida y éxito muy probablemente una organización oficial lo adopte para que sea un estándar oficial o de jure.

Los estándares de jure u oficiales son los aprobados por grupos u organizaciones como la ISO, NSA, IETF entre otras. Estos estándares son promulgados por un grupo de personas provenientes de diferentes áreas de conocimiento y contribuyen con ideas u otros recursos para el desarrollo y la definición de un estándar específico.

Los estándares propietarios son de pertenencia absoluta de una organización y su utilización no es muy aceptada en el mercado. Muchas entidades trabajan con este tipo de estándar para atraer más clientes y vincularlos con los productos de dicha empresa. Sin embargo si un estándar propietario tiene éxito y logra introducirse bien el mercado puede convertirse en un estándar de facto e incluso puede ser adoptado por un organismo de estandarización y ser un estándar oficial

2.2.3.- RFC (REQUEST FOR COMMENTS)

Los Request For Comments son documentos que se publican de forma gratuita en servidores ftp, http, gopher o cualquier medio de transmisión de datos por la red, en los que entre otras cosas están los protocolos oficiales del IESG (Internet Engieneering Stering Group), la IAB (Internet Architecture Board) y la Internet Comunity.

En 1969 se empieza a publicar los RFC's, como parte del proyecto ARPA. En la actualidad el RFC Editor bajo la supervisión del IAB, es el encargado de publicar estos documentos. Los RFC's se numeran según el orden en que van apareciendo, se publican en código ASCII, pero pueden ser transformados a otros formatos, aunque el oficial es el Postscript. El autor del RFC debe presentar a la organización en texto ASCII con un formato de encabezado, paginación o incluir diagramas ASCII si fuera necesario, este formato está especificado en el RFC-2023.

Una gran cantidad de protocolos siguen evolucionando mediante los RFC, varios investigadores diseñan e implementan nuevos protocolos y los ponen a conocimiento de la comunidad de internet en forma de un RFC. La mayor fuente de RFCs es del Internet Engineering Task Force (IETF), organización subsidiada por Internet Architecture Board (IAB), pero cualquier persona puede enviar una propuesta de RCF al RFC Editor cumpliendo con los requisitos.

Cuando un RFC ha sido publicado, las versiones y sustituciones se publican como nuevos RFCs, esto quiere decir que si un RFC es actualizado el original no se eliminará de la lista de RFCs. Algunos RFCs son documentos informativos mientras que otros contienen protocolos y estándares para internet, los que están en uno de los siguientes estados:

1) Estándar, el IAB lo ha establecido como protocolo oficial de Internet y se dividen en dos grupos: Protocolos que se aplican a la totalidad de Internet y Protocolos específicos de redes, generalmente especificaciones del funcionamiento de IP en tipos concretos de redes.

2) Estándar provisional, el IAB considera que este protocolo es un posible protocolo estándar. Dispone de comentarios y pruebas exhaustivas cuantitativas y cualitativas. Los comentarios y los resultados de las pruebas deberían enviarse al IAB. Existe la posibilidad de que se efectúen cambios en un protocolo estándar provisional antes de que se convierta en estándar.

3) Propuesto como estándar, se trata de propuestas de protocolos que el IAB puede considerar para la estandarización en un futuro. Es necesario evaluar la implementación y es probable que el protocolo se someta a revisión.

4) Experimental, un sistema no debería implementar un protocolo experimental a menos que participe en el experimento y se haya coordinado el uso que va tener el protocolo desarrollado.

5) Informativo, Los protocolos desarrollados por otras organizaciones de estándares, o distribuidores, o aquellos que por otras razones son ajenos a los propósitos del IAB, pueden ser publicados a conveniencia de la comunidad de Internet como protocolos informativos. En algunos casos el IAB puede recomendar el uso de estos protocolos en Internet.

6) Histórico, son protocolos con pocas posibilidades de convertirse alguna vez en estándar en Internet, bien porque han quedado obsoletos por protocolos posteriores o debido a la falta de interés.

7) Estándares de Internet, cuando un protocolo alcanza el estado de estándar se le asigna un número estándar (STD). El objetivo del STD es indicar claramente que RFCs describen estándares de internet. Estos números hacen referencia a múltiples RFCs cuando la especificación de un estándar está repartida entre varios documentos.

Los STD no cambian cuando un estándar es actualizado y carecen de número de versión ya que todas las actualizaciones se hacen por medio de los RFCs. Para el seguimiento de algunos estándares, el estado del RFC no siempre contiene la suficiente información, por lo cual se le añade un descriptor de aplicabilidad que está dado por un STD, dicho descriptor está particularmente en los protocolos de encaminamiento.

8) For Your Information (FYI), un cierto número de RFCs tienen un amplio interés para los usuarios de internet y se clasifican como documentos For Your Information (FYI) o para su información, generalmente contienen información de ayuda o de carácter introductorio, un FYI no se cambia cuando se publica un RFC revisado y le corresponden a un único RFC.

2.2.4.- PROCESO DE ESTANDARIZACIÓN

Para que un protocolo llegue a convertirse en estándar, primero se debe ser un borrador para que se hagan implementaciones de este, y si estas implementaciones cumplieran con los requisitos técnicos pertinentes, se lo redactaría formalmente. Sin embargo existen dificultades para redactar un documento técnico de calidad, a continuación los requisitos técnicos que requiere un protocolo:

- Que sea un proyecto abierto, esto es que haya sido desarrollado mediante listas de correo públicas.
- Que sea flexible y portable para la mayoría de los sistemas.
- Que exista una prueba previa y haya tenido éxito.
- Que desde el punto de vista técnico que sea la solución más óptima al problema planteado.
- Que sea constante a través del tiempo

Existe todo un proceso antes de que un protocolo sea un estándar, pero sin la ayuda de los usuarios de internet que son los que hacen que un protocolo no se quede estancado. Mientras más lo utilicen e implementaciones hagan de acuerdo a los requisitos antes mencionados, más rápido podrá ser utilizado como estándar oficial.

Los pasos por los que un protocolo ha de pasar para llegar a ser estándar son los que se detallan a continuación:

1) Internet Draft (ID)

Es el Borrador de Internet, este es un documento publicado para todo el mundo, dicho documento puede ser analizado y mejorado. Si esta mejora es de calidad puede pasar a ser un RFC (Request For Comments). Un internet draft tiene un tiempo de vida de seis meses, y si durante este tiempo no es mejorado ni es recomendado por la IESG (Internet Engineering Steering Group) se lo eliminará de la lista de Internet Draft (ID).

2) Proposed Standard

Si un estándar llega al nivel de estándar propuesto, es porque la IESG (Internet Engineering Steering Group) le ha dado su confianza y ha comprobado que su uso por parte de usuarios de internet es alto, hay que subrayar que no es necesario que una implementación esté funcionado.

3) Draft Standard

Es el Estándar Borrador, para que una especificación tenga este nivel es necesario que exista por lo menos dos implementaciones que validen y den fiel testimonio del correcto funcionamiento de la especificación, además tiene que ser estable y ser probado para ser la base de múltiples implementaciones.

4) Internet Standard

El estándar de internet, una especificación tiene este nivel cuando ha logrado sus objetivos, se ha sometido a pruebas que la hacen totalmente segura de utilizar, para este nivel ya se han realizado los cambios necesarios para las implementaciones que con éxito que se hayan realizado, además demuestran una total estabilidad en ambientes de gran tamaño.

Hay que tomar en cuenta que no todas las especificaciones que se publican como RFC's llegan a ser un estándar, estos documentos pueden tener tres estados que son: Experimental, Informational o Historic.

Experimental, los documentos experimentales son en los que se da a conocer el esfuerzo para el desarrollo de la investigación y son publicados para tener una constancia del trabajo que se está realizando.

Informational, son textos que informan sobre algún tema de interés para los usuarios de internet.

Historic, este estado lo adquieren los documentos que son obsoletos y que continúan en la lista solo por la importancia que tuvieron en el pasado o por que sirven como antecedentes de trabajos.

2.2.5.- ESTÁDARES PARA TRANSACIONES EN INTERNET

Internet tiene problemas de autenticidad, integridad, confidencialidad y repudio que afectan los requerimientos de las transacciones electrónicas de la siguiente forma:

Robo de información, que se lo hace mediante escuchas de red, que consiguen los números de cuentas o de tarjetas de crédito, información de facturación o balances de usuarios ingenuos o no precavidos.

Suplantación de identidad, permite al atacante realizar operaciones en nombre del otro. En este tipo de situaciones el que alguien tenga varios números de tarjetas de crédito puede realizar pequeñas transacciones que le signifiquen una gran cantidad.

Sniffers, son herramientas informáticas que permiten obtener la lectura de información que se transmite por la red. Los sniffers permiten la terminación de un ataque de suplantación de identidad y/o robo de información.

Modificación de información, con este se puede alterar el contenido de ciertas transacciones como el pago de una orden de compra o la misma compra.

Repudio, es le rechazo o negación de una operación de una de las partes de un acuerdo previo. Esto puede ser causa de problemas de pago adicionales a una de las partes.

Denegación del servicio, un ataque de este tipo imposibilita al sistema para que pueda operar con normalidad y por lo tanto no es factible de realizar transacciones operacionales. Estos son tan sencillos y la identificación del atacante puede que sea imposible de saber.

Los estándares para transacciones en internet han ido evolucionando y lo a que a continuación se estudiará son los que están penetrando más en este mundo, donde la seguridad es el mayor objetivo de las grandes organizaciones que están involucradas con este tema.

2.2.5.1.- Protocolo Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) o Transacción Electrónica Segura, es un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales el pago de bienes y/o servicios con la utilización de tarjetas de crédito.

Fue desarrollado por Visa y MasterCard con la asesoría de IBM, Netscape, RSA, entre otras, con la finalidad de que los medios de pago clásicos sean trasladados al medio digital y cuenten con las misma seguridades y fortalezas.

El protocolo SET dispone de las técnicas necesarias para efectuar pagos y cobros con dinero digital sin la intervención de las instituciones financieras, aunque dichas instituciones prefieren cobrar las comisiones por emitir una tarjeta. SET provee integridad del mensaje, autentificación de los datos financieros, encriptación de datos, y proporciona medidas de seguridad para el comercio electrónico.

Los problemas que surgen con los cobros y pagos vía Internet con las tarjetas de crédito se van solucionado con los certificados digitales que validan la identidad de las partes que intervienen en una transacción, o a través de servidores seguros que van haciendo que la privacidad esté garantizada.

El protocolo SET protege la información de la siguiente manera:

1) Permite al titular de la tarjeta autenticar que el comerciante esté autorizado para aceptar tarjetas de pago y que utilice el protocolo de seguridad SET.

2) Permite al comerciante que utiliza el protocolo SET autenticar la tarjeta de pago que se utiliza en la transacción.

3) El protocolo SET utiliza un sistema de codificación avanzado que protege la información relacionada con el pago mientras se realiza la transferencia a través de Internet.

4) El protocolo SET asegura que la información relacionada con el pago sea leída por la persona que debería hacerlo. Dicha información solo puede ser decodificada por el comerciante e institución financiera que utilice el mismo protocolo.

Arquitectura del Protocolo SET

Este protocolo cuenta con tres entidades electrónicas. Entidad Merchant SET o Comerciante SET, es la encargada de gestionar el pago del producto y/o servicio que ha pedido el comprador. El pago siempre estará asociado con un acquirer o aceptador para la autorización del importe a pagar por el comprador. A ésta entidad se la llama Point Of Sale (POS) o Terminal Punto de Venta virtual, debido a que sus funciones simulan a los sistemas tradicionales.

Entidad Cardholder SET o Titular SET, es quién se encarga de realizar el pago en nombre del titular de la tarjeta. Por lo general a esta entidad se la conoce como Wallet o Cartera, pues su funcionalidad es similar a una cartera que almacena las tarjetas.

Entidad Gateway SET o Pasarela SET, su funcionalidad es hacer un puente entre el sistema aceptador SET y el sistema financiero. Esta entidad es de gran importancia ya que permite la conexión de los sistemas y las redes de autorización privados que se encuentran en Internet. Gráficamente las entidades funcionan de la siguiente forma.

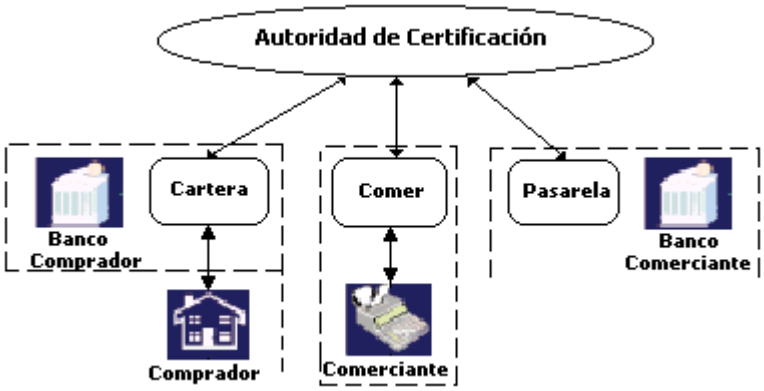

Figura 2.2

Todas las entidades implicadas en el protocolo SET deben estar en posesión de un certificado válido para que puedan intervenir en una transacción de pago. Las entidades de certificación en el SET se denominan CA SET (Certification

Authority SET)y por lo general son las instituciones financieras, que están facultadas para emitir tarjeta o las instituciones asociadas como los bancos que solicitan emisión de tarjetas.

Por lo general las Autoridades de Certificación se asocian a una marca de tarjeta particular, con esto los certificados de las entidades serán válidos para una marca determinada, esto es similar a los sistemas tradicionales ya que una tarjeta Visa no puede manejarse como MasterCard.

Funcionamiento de Protocolo SET

Define mensajes e interacciones entre las entidades SET para realizar una transacción de pago desde que el comprador acepta pagar hasta que este pago se realice mediante un abono en la cuenta del comerciante desde la cuenta del comprador. Existen tres fases que se detallan a continuación:

1) Fase de inicialización, es el mensaje inicial que el comprador realiza para contactarse con el comerciante, le informa la marca de la tarjeta para realizar el pago, el comerciante responde con el mensaje firmado.

2) Fase de pago, el comprador realiza la orden de pago, antes tendrá que verificar la identidad del comerciante y las condiciones para la transacción. La respuesta de este mensaje contiene la aceptación o denegación del pago.

3) Fase de autorización, el comerciante solicita a la pasarela de pago, y al sistema financiero tradicional, información sobre si el comprador tiene crédito o saldo en la tarjeta, o si no está revocada, etc. La respuesta a este mensaje lleva la aceptación o denegación del pago.

El protocolo SET implementa un sistema de firma dual en el que el comprador al realizar el mensaje inicial incluye datos protegidos para el comerciante y para la pasarela. De esta manera el comerciante nunca tendrá el número de la tarjeta del

comprador y la entidad financiera nunca tendrá los datos de compra. Con este esquema la fase de autorización ocurre durante la fase de pago, a ésta modalidad se la conoce como pago en línea inmediato y es la más utilizada, aunque SET permite diferentes modalidades.

Normas Básicas del Protocolo SET

Autentificación, que se realiza a través de certificados digitales que tanto el comerciante como el comprador tienen, y se los proporciona el CA SET, dicho certificado asegura la validez de una clave pública.

Privacidad, los datos transmitidos por la red son encriptados por algoritmos matemáticos que son casi indescifrables, están dotados de dos claves simétricas, una pública que es distribuida libremente y la privada que es conocida sólo por su propietario para descifrar los datos recibidos.

Integridad y autenticidad son la base para generar las firmas digitales. La firma se crea por las relaciones matemáticas entre la clave pública y privada. Usando una función irreversible se extraen los datos de la transacción que luego son cifrados con la clave privada del remitente, el resultado se adjunta al final del original y así se constituye la firma digital.

Todo lo que se ha mencionado sobre el protocolo SET conlleva muchas ventajas, sin embargo tiene algunos problemas, actualmente existen varias implantaciones del SET que han tenido que someter a modificaciones para lograr su funcionalidad. A continuación se mencionan algunos de estos inconvenientes:

- Debido a su alta seguridad, el SET es muy complejo, por eso es que sus fabricantes tardan mucho tiempo en tener un sistema completo y estable en el mercado.

- Las grandes inversiones por sus fabricantes impactado en el precio de los productos, pues son muy elevados, lo que termina en la poca adquisición de los usuarios. Además el ritmo del crecimiento del comercio electrónico es todavía lento.

2.2.5.2.- Protoloco Secure Socket Layer (SSL)

Secure Socket Layer (SSL), fue diseñado y propuesto por Netscape Comunications en 1994. Esta organización tiene la licencia de la tecnología criptográfica de llave pública RSA(Rivest, Shamir, Adelman) y la usó para desarrollar dicho protocolo.

SSL es soportado por aplicaciones comunes como Netscape Navigator, Microsoft Internet Explorer y la mayoría de aplicaciones de servidores como Netscape, Microsoft, Apache, Oracle, etc. y autoridades certificadoras como Verisign.

Estructura del Protocolo SSL

Existen dos partes el SSL Handshake y el SSL Record, el primero se encarga de realizar las funciones de autentificación entre el servidor y el cliente, el segundo realiza el envío y recepción de datos, cifrando y descifrando la información. A continuación se muestra un esquema de la estructura del SSL.

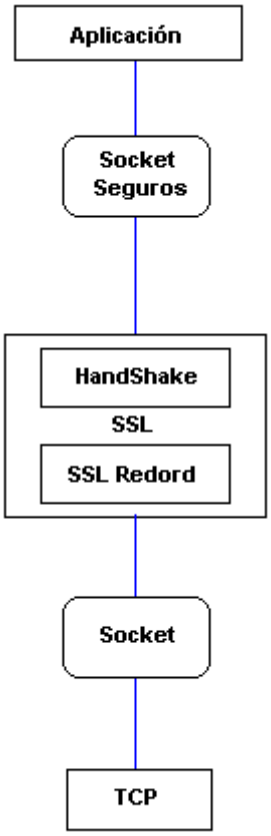

Figura 2.3

Para establecer una comunicación segura utilizando SSL se tiene que seguir los pasos que se detallan a continuación:

Primero se realiza una solicitud de seguridad, un cliente hace una solicitud de una URL a un servidor que soporte SSL, el servidor empieza a negociar la conexión, denominada SSL Handshake. SSL acepta solicitudes por un puerto diferente al utilizado normalmente por este servicio.

En segundo paso se establecen los parámetros que se utilizarán para el SSL, aquí se realiza la autenticación del servidor y opcionalmente la del cliente, se determinan los algoritmos criptográficos que se utilizarán y la generación de la llave secreta, esto para cuando se utilice el intercambio de mensajes en la comunicación SSL. El proceso del Handshake es como sigue:

Client Hello, o saludo de cliente es el que informa al servidor que algoritmos de criptografía puede utilizar y a la vez solicita la verificación de la identidad del servidor. El cliente envía un conjunto de algoritmos de criptografía que soporta y un número aleatorio, dicho número se utiliza en caso de que el servidor no posea un certificado para comprobar su identidad y seguir con una comunicación segura utilizando un conjunto diferente de algoritmos.

Server Hello, el servidor le contesta enviando su identificador digital que tiene su llave pública, también los algoritmos criptográficos y otro número aleatorio. El algoritmo que sea más fuerte tanto para el cliente como para el servidor será el que se utilice. En algunos casos el servidor puede solicitar al cliente un identificador digital.

Aprobación del cliente, el cliente verifica la validez del certificado enviado por el servidor, desencripta el certificado con la llave pública del emisor, con esto comprobará que el certificado es de una entidad certificadora de confianza. Luego se verifica información como fecha, URL del servidor, etc. Entonces el cliente genera una llave aleatoria encriptándola con la llave pública del servidor y el algoritmo criptográfico seleccionado, esta llave se la envía al servidor y si este handshake tiene éxito puede ser utilizado para el envío de futuros mensajes.

Verificación, es cuando ambas partes conocen la llave secreta, el cliente porque lo generó y el servidor porque la recibió a través de su llave pública. La única posibilidad de desencriptarla es con la llave privada del servidor. Se hace la última verificación de la información transmitida, enviando una copia de las anteriores transacciones encriptadas con la llave secreta. Si las dos partes validan las transacciones el handshake se completa y si no es así el proceso se reinicia.

El tercer paso es el intercambio de datos o SSL Record, donde ambas partes están listas para intercambiar información, a través del canal de transmisión seguro SSL y con la utilización de la llave secreta y algoritmos criptográficos acordados se intercambiarán los datos. Cuando el servidor o el cliente quieren

enviarse un mensaje, se genera un digest que utiliza un algoritmo de hash que hace que el tamaño del mensaje sea menor, entonces se encripta el mensaje, se envía el digest verificando cada mensaje.

El último paso es la terminación de la sesión SSL, cuando el cliente deja una sesión de este tipo la aplicación presenta un mensaje advirtiendo que la comunicación ya no es segura y pide la confirmación para terminar la comunicación SSL.

Servicios que ofrece el protocolo SSL

Privacidad, que se consigue con la encriptación de las llaves, la comunicación encriptada entre el servidor y el cliente SSL la hace no legible para aquellos como los hackers y crackers que logran interceptarla.

Integridad, para que la información transmitida llegue a su destino final sin modificaciones, SSL recurre a las combinaciones de funciones matemáticas secretas llamadas Funciones Hash.

Autenticación, en este proceso el servidor se convence de la identidad de cliente y viceversa, las identidades son codificadas en forma de Certificados de llave pública que son verificados por las Autoridades de Certificación.

Proporciona extensibilidad ya que es capaz de soportar nuevos protocolos en el futuro, también eficiencia porque utiliza la compresión para minimizar el tiempo necesario para establecer la conexión. Ofrece compatibilidad con productos de diferentes versiones SSL, pues pueden interoperar entre sí.

Netscape ha desarrollado una extensión del Protocolo HTTP para soportar SSL en servidores web, ésta se denomina https, una dirección de internet será mostrada como https en lugar de http, cuando se trate de una comunicación que utilice el protocolo SSL. El puerto por el que se comunica es el 443 en vez del

acostumbrado puerto 80 que utiliza el http. Una de las ventajas del SSL es la independencia de la aplicación, cuando un protocolo de alto nivel se coloca sobre el SSL lo hace de manera transparente.

2.2.5.3.- Secure HyperText Transfer Protocol (S-HTTP)

El protocolo Secure HyperText Transfer Protocol (S-HTTP) fue propuesto por Enterprise Integration Technologies (EIT), patrocinado por el Consorcio CommerceNet y actualmente desarrollado por Terisa System. El S-HTTP es una versión del HTTP con seguridad mejorada y está diseñado para enviar mensajes individuales de manera segura.

Aunque S-HTTP provee confidencialidad, integridad, no rechazo y autenticación no tiene el mismo éxito que SSL. La confidencialidad la proporciona mediante criptografía de clave pública como RSA y la criptografía de clave secreta. La integridad y la autenticación de los datos la consiguen mediante la firma digital.

S-HTTP propone el .shttp como nueva extensión para los documentos, además la creación del protocolo Secure-HTTP/1.1. Utiliza un sistema de cabeceras en cada transmisión para lograr que las comunicaciones sean seguras. El mecanismo de conexión en S-HTTP, en su versión 1.1, es el intercambio de datos formateados entre el cliente y servidor. Las líneas que se utilizan en las cabeceras comprenden:

- Dominios Privados S-HTTP, este especifica el tipo de algoritmo de cifrado y la forma de encapsulamiento de los datos.

- Tipo de Certificado S-HTTP, en esta parte se especifica el formato del certificado, que en la actualidad es el X.509.

- Algoritmos de intercambio de clave S-HTTP, se especifica los algoritmos que se utilizaran para el intercambio de claves.

- Algoritmos de firmas S-HTTP, en este se debe especificar el algoritmo para la firma digital.

- Algoritmos de resumen de mensajes S-HTTP, en este se deben identificar los algoritmos para proporcionar la integridad de los datos usando funciones Hash.

- Algoritmos de contenido simétrico S-HTTP, en el que se identifica el algoritmo simétrico de cifrado en bloque que se utiliza para cifrar los datos.

- Algoritmo de cabecera simétrica de S-http, en este se especifica una lista de cifrado de clave simétrica que se usa para cifrar las cabeceras.

- Mejoras de la intimidad de S-http, en el que se debe indicar las mejoras en la intimidad asociadas con los mensajes, esto es la forma de cifrar, firmar o autenticar.

Funcionamiento del Protocolo S-HTTP

La transacciones mediante el protocolo S-HTTP es relativamente sencillo y consta de cinco partes:

- El cliente se conecta con el sitio.

- El cliente envía su clave publica.

- El servidor verifica la clave, si acepta envía al siguiente paso, si no la acepta se corta la conexión.

- El servidor envía al cliente la clave de la transacción encriptada con la clave publica del cliente.

- Una vez que el cliente tiene la clave codifica cada dato que envía al servidor. Todo esto se puede complicar aun más con las firmas digitales, ya que el S-HTTP puede usar o codificar los datos, la firma digital, o incluso ambas a la vez. Por supuesto cada sesión que el cliente y el servidor lleven a cabo, se usará una clave diferente para no ser intercepta.

S-HTTP ofrece flexibilidad e integración dentro del HTML ya que Netscape introduce mejoras periódicamente en sus navegadores. Además S-HTTP está integrado con HTTP, actuando a nivel de aplicación, negociando los servicios de seguridad a través de cabeceras y atributos de página, por eso están disponible para el protocolo HTTP.

Entre las desventajas se puede señalar los efectos que se derivan de mantener la compatibilidad hacia atrás y la necesidad de implementar servidores que soporten las extensiones a HTML aportadas por el protocolo S-HTTP, y ante el protocolo SSL que sirve para cualquier comunicación, S-HTTP solo se utiliza para la web.

2.2.5.4.- Electronic Data Interchange (EDI)

Electronic Data Interchange o Intercambio Electrónico de Datos, se lo puede definir como un conjunto de datos estructurados de acuerdo a normas de mensajes definidas para la transmisión por medios electrónicos, puestos en un formato que puede ser leído por el ordenador y procesado automáticamente. En definitiva es un protocolo de comunicación para realizar transacciones entre organizaciones y personas. EDI, intercambian la información de negocios directamente entre sus sistemas de computación.

EDI cuenta con certificado ANSI (American National Stardards Institute) desde hace varios años, en la actualidad el formato utilizado es el X12-3040. Electronic Data Interchange se basa en la utilización de mensajes estándar, asegurando que todos los usuarios utilicen un lenguaje común. Un mensaje se fundamenta en

formatos uniformes adoptados para la transmisión electrónica de los documentos de negocios, también incluye elementos de seguridad, control y otras reglas referentes a la utilización de las transacciones.

Componentes del EDI

1) Centro de compensación, su función básica es recibir, almacenar y reenviar a sus destinatarios los documentos comerciales que sus usuarios intercambian, con esto se asegura la integridad y confidencialidad de la información. Cada empresa tiene asignado un buzón electrónico, mediante el cual cada usuario recibe y recupera la información que sus interlocutores comerciales les envían.

2) Red de telecomunicaciones, las empresas que son usuarias de éste servicio tienen acceso al centro de compensación a través de una red terrestre o satelital. El ingreso se hace por medio de accesos directos o por red telefónica conmutada al centro más cercano. La elección del vínculo se determina por la función del tráfico que las empresas necesitan para el servicio.

3) Estación del usuario, es la herramienta software que permite realizar la conexión del sistema informático de cada cliente con el centro de compensación, sus funciones son: comunicación, traducción de mensajes al formato estándar, interfase con aplicaciones del cliente, entrada manual de datos e impresión de documentos recibidos.

La contratación de una red de valor agregado (VAN), es también importante ya que será la encargada de administrar las comunicaciones de los socios, además proveerán facilidad para los buzones electrónicos y la interconectividad entre las diferentes redes para garantizar que los documentos de los negocios lleguen a su destino eficazmente.

Con el desarrollo del comercio electrónico e internet estas redes de valor agregado (VAN) se están transformando en proveedores de servicio de valor

agregado de internet o los denominado VAI's (Value Added Internet Service). Los VAI's están implementando servicios de transacciones sobre aplicaciones con tecnología que operan basándose en flujos de trabajos, servicios de capacitación, catalogación electrónica, hospedaje de contenido, servicios de traducción de formato en línea, etc.

Servicios del EDI

En esta solución las órdenes de compra son generadas por el personal y posteriormente enviadas al servidor departamental en el que se ejecuta las compras y facturación. Por lo tanto se hace necesario de los servicios de: comunicación externa, traductor para codificar / decodificar la información local en mensajes normalizados, comunicación interna para importar o exportar datos entre el traductor y la base de datos local, servicio de seguridad para garantizar la autenticidad e integridad en transacciones, servicio de gestión para mantener un histórico de los mensajes enviados o recibidos, informes de error, etc.

Existen dos soluciones básicas para integrar un paquete de software EDI:

1) Solución de Procesador Front-End-frontal de comunicaciones (FEP), en la que se mantienen tan separados como sea posible de las aplicaciones. La primera forma para implementar dicha solución el paquete EDI deberá residir en una máquina separada conectada con el sistema de información del contratista por medio de un paquete de comunicaciones.

La segunda es que el paquete software esté co-residente con las aplicaciones del sistema de información de la Administración Pública. Generalmente la solución FEP sobre una máquina separada es la mejor opción para introducir el EDI en grandes organizaciones durante proyectos de prueba, su costo es bajo, se implementa rápidamente y no enlaza el sistema del contratista con el mundo exterior.

2) La solución integrada, en la que las aplicaciones existentes se modifican para integrar en ellas la funcionalidad del EDI, además será posible maximizar los beneficios del EDI.

Identificados los mensajes EDIfact para el negocio se inicia un análisis cuidadoso de los sistemas internos por parte de las Administraciones Públicas, con el que se podrá evaluar los impactos y cambios necesarios para la introducción del EDI dentro del entorno, el análisis será relacionado con: disponibilidad de datos, contenido de los campos, longitudes de los campos y formato de contenido.

2.2.5.5.- Protocolo Trasport Layer Security (TSL)

El protocolo Trasport Layer Security (TLS) se basa en la especificación del protocolo SSL 3.0, las diferencias entre estos protocolos no son muy significativas, pues ambos se diseñaron de tal manera que puedan proporcionar integridad y privacidad de datos entre dos aplicaciones que se comunican.

Al igual que SSL su estructura muestra dos capas: el Record Protocol y al HandShake Protocol. El primero, para ambos protocolos se dedica a codificar y decodificar los mensajes que se transmiten y reciben. El HandShake Protocol consiste de un conjunto de subprotocolos que se utilizan para permitir a las partes involucradas en la comunicación ponerse de acuerdo con los parámetros de seguridad, autenticación y condiciones de informes de errores.

Componentes del TSL

1) El Record Protocol, se encuentra a un nivel más bajo sobre un protocolo de transporte fiable como el TCP, proporciona una conexión segura y privada, ésta capa usa criptografía simétrica para la encriptación de los datos pero puede utilizar también encriptación.

Para el transporte del mensaje utiliza un mensaje de chequeo de integridad que a su vez usa el MAC (Message Authentication Code) con clave, empleando opcionalmente funciones de hash seguras. Básicamente se encarga de tomar los mensajes a ser transmitidos, fragmenta los datos en bloques manejables, puede comprimir los datos opcionalmente, aplica una MAC, encripta y transmite el resultado. El dato recibido es desencriptado, verificado, descomprimido y reensamblado para ser entregado a los clientes en niveles más altos.

Este proceso se lleva a cabo a través de cuatro estados posibles de conexión: el estado de lectura actual, el estado de escritura actual, el estado pendiente de lectura y el estado pendiente de escritura. Cada uno de estos estados especifica el algoritmo de compresión, el algoritmo de encriptación y el algoritmo de MAC, el tamaño de las claves de encriptación y los IVs (Initialization Vector).

Los registros sólo se procesan bajo el estado actual, es posible pasar de un estado pendiente de conexión a un estado actual por medio del Handshake Protocol, cuando esto sucede el estado pendiente es reinicializado a un estado vacío. No es legal hacer que un estado no inicializado con los parámetros de seguridad pase a ser un estado actual. Cada estado de una conexión define los parámetros de seguridad.

Una vez que se ha definido la estructura, el Record Protocol genera el secreto MAC de escritura para el cliente (client_write_MAC_secret) y el servidor (server_write_MAC_secret), la clave de escritura para el cliente (client_write_key) y servidor (server_write_key) y los IVs en caso de que se trate de un algoritmo criptográfico por bloques (client_write_IV y server_write_IV).

Por cada registro procesado se deben actualizar los estados con los siguientes elementos:

- Estado de la Compresión, en este estado se encuentra el algoritmo de compresión.

- Estado del Encriptador, se encuentra el algoritmo de encriptación. Si es un encriptador por bloques en modo CBC, el único soportado por TLS, el estado inicial tendrá el IV actualizado con el último bloque de cipherText (texto del algoritmo criptográfico) que se haya generado, según se procesen los registros.

- El secreto del MAC, se mantiene para la conexión conforme se generó anteriormente.

- Número de secuencia, cada estado de conexión contiene un número de secuencia que se mantiene independientemente para los estados de lectura y escritura, el número es seteado a cero cada vez que un estado de conexión pasa a estado activo.

Fragmentación

El Record Layer de TLS recibe los datos no interpretados de capas superiores en bloques no vacíos de tamaño arbitrario, y los fragmenta en bloques de información de hasta 2^14 bytes o menos. Múltiples mensajes del cliente del mismo ContentType pueden unirse en un solo TLS PlainText record, o un solo mensaje puede fragmentarse en varios registros.

Si un bloque de longitud menor a los 2^14 bytes definidos como tamaño máximo para un registro intenta ser enviado, y a la vez otro bloque del mismo ContentType necesita ser enviado, se hace una concatenación, superando los 2^14 bytes, entonces se enviarán en registros separados.

Una vez hecha la fragmentación, si es necesario se introduce la información en una estructura llamada TLSPlaintext, gráficamente se la puede observar así:

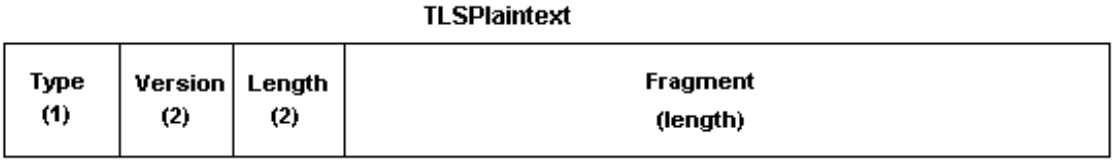

Figura 2.4

Type, es el protocolo de nivel superior usado para procesar el fragmento encapsulado.

Version, es la versión del protocolo que está siendo utilizado.

Length, es la longitud en bytes del TLSPlainText.

Fragment, el dato de aplicación, éste es transparente y tratado como un bloque independiente para ser distribuido al protocolo de nivel superior especificado por el campo Type.

Compresión y descompresión

Cuando se configura los parámetros de la conexión, se puede especificar un algoritmo de compresión y descompresión para comprimir los datos de un registro TLSPlainText. Esta es una etapa adicional antes de que los datos sean encriptados. Cuando se inicia el estado de sesión el algoritmo se define como CompressionMethod.null, esto se realiza por defecto, lo que significa que no va a haber ninguna compresión como resultado de esta etapa.

Independientemente de esto, se traslada la información a un registro tipo TLSCompressed como se muestra en el siguiente gráfico:

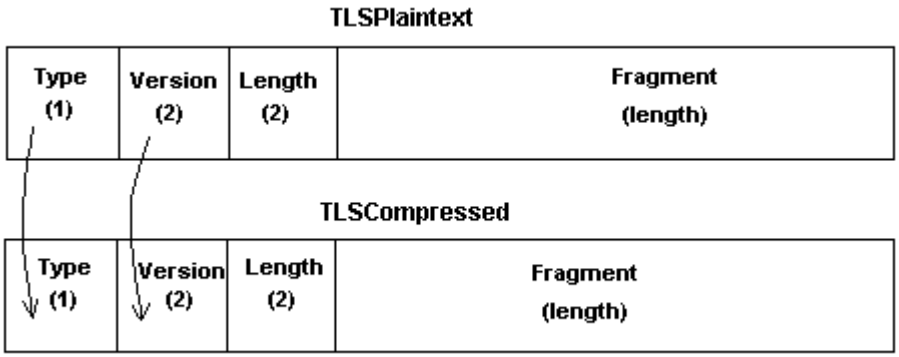

Figura 2.5

Type, es igual al TLSPlainText.
Version, como se definió en el TLSPlainText.
Length, es la longitud en bytes del TLSCompressed.fragment, donde los 1024 bytes son la máxima cantidad de información que agrega el algoritmo de compresión para poder efectuarse la descompresión.
Fragment, es el TLSPlainText.fragment comprimido.

Encriptación de Registros.

El último paso antes de la transmisión de los datos por el medio de transporte (TCP) es la encriptación y autenticación de datos. Las funciones de encriptación y MAC definidas al comienzo del estado de lectura y escritura de una conexión traducen la estructura TLSCompressed a TLSCipherText. Las funciones de desencriptación realizan el proceso inverso, además el MAC del registro incluye un número de secuencia para que los mensajes perdidos, extra o repetidos sean detectados.

2) Handshake Protocol, este protocolo involucra el uso del Record Protocol de TLS para intercambiar una serie de mensajes entre un servidor TLS-enabled y un cliente TLS-enabled al iniciar una conexión TLS. Este intercambio de mensajes se diseñó para proporcionar la autenticación del servidor por parte del cliente, permitir que el cliente y el servidor seleccionen los algoritmos criptográficos, establecer una conexión TLS encriptada.

El Handshake Protocol se encarga principalmente de establecer y terminar las conexiones TLS. Las aplicaciones lo usan para abrir y cerrar conexiones seguras, y se requiere que las aplicaciones estén diseñadas para soportar TLS. Este protocolo es responsable de la negociación de una sesión.

Entonces, para que un cliente y un servidor puedan empezar a comunicarse, primero se deberán poner de acuerdo en la versión del protocolo, seleccionar los algoritmos criptográficos para la privacidad de sus datos, autenticarse uno con el

otro, aunque esto es opcional, y las técnicas de criptografía de clave pública para generar secretos compartidos.

Varias operaciones en el Record Protocol y el HandShake Protocol requieren de un MAC con clave, el intento de falsificar un MAC es casi imposible, lo que le añade un grado más de seguridad.

Alertas de Error

Cuando se detecta un error, se envía un mensaje a la otra parte como una alerta fatal, las partes involucradas inmediatamente cierran la conexión. Servidores y clientes requieren que se desechen cualquier session_identifiers, claves y secretos asociados a la conexión fallada. A continuación algunas alertas de errores:

- unexpected_message o mensaje inesperado, esta alerta es siempre fatal y nunca debe ser vista en comunicaciones entre implementaciones apropiadas.

- bad_record_mac, este mensaje es retornado si el registro es recibido con un MAC incorrecto, siempre es fatal.

- decryption_failed, el TLSCipherText ha sido desencriptado en forma invalida, la longitud del bloque no ha sido múltiplo par, es siempre fatal.

- record_overflow, el registro TLSCipherText ha sido recibido con una longitud mayor a 2^14 + 2048 bytes, o el registro TLSCompressed desencriptado con mas de 2^14 + 1024 bytes, es fatal.

- handshake_failure, este mensaje indica que el transmisor no está capacitado para negociar un conjunto aceptable de parámetros de seguridad dados por las opciones disponibles, es un error fatal.

Mensajes

Algunos de los mensajes utilizados por el TSL son:

Mensaje HelloRequest, puede ser enviado por un servidor en cualquier momento y consiste en una simple notificación para que el cliente comience otra vez el proceso de negociación enviado un mensaje ClientHello. Si el servidor envía un mensaje HelloRequest pero no recibe un mensaje HelloClient en contestación puede cerrar la conexión con un error fatal. Este mensaje es opcional.

Mensaje ClientHello, cuando un cliente se conecta a un servidor, el cliente deberá enviar un ClientHello como iniciativa para negociar los parámetros de seguridad, este mensaje no es opcional.

Mensaje ServerHello, el servidor envía este mensaje en contestación al ClientHello cuando se ha encontrado un conjunto aceptable de algoritmos. Este mensaje es obligatorio.

Mensaje Finished, este mensaje no es opcional y se utiliza para verificar que el intercambio de claves y el proceso de autenticación se llevaron a cabo satisfactoriamente. Los destinatarios de los mensajes de finalización deben verificar que los contenidos sean correctos. Una vez que una parte envía el mensaje de finalización y recibe con la validación del mensaje de finalización de la otra parte, pueden comenzar a enviar y recibir los datos de la aplicación sobre la conexión.

2.3. ESTÁNDARES UTILIZADOS EN PKI

2.3.1.- PUBLIC KEY CRYPTOGRAPHY STANDARDS (PKCS)

Los Estándares Criptográficos de Clave Pública fueron introducidos por la RSA Data Security para las entidades que desean una interfaz estándar con la criptografía de clave pública. A diferencia con otros estándares que son apoyados por otros organismos internacionales los PKCS son una aproximación a un estándar al mundo de la criptografía.

Muchas organizaciones como Apple, Microsoft, Digital, Lotus, Sun y Massachussets Institute of Technology han participado en su desarrollo pero solo la RSA Data Security toma la última decisión en su promulgación y revisión. Actualmente está constituido por doce normas:

1) PKCS#1 (RSA Encryption Standard) en esta norma se describe un método para utilizar el algoritmo RSA, su finalidad es producir firmas digitales de mensajes y mensajes cifrados, utilizando la sintaxis definida por la norma PKCS#7. Las firmas digitales se producen aplicando la función Hash al mensaje y cifrado de la huella digital que resulta de la clave privada del firmante.

Para conseguir la encriptación de mensajes se cifra primero con una clave simétrica y luego ésta clave es cifrada con la clave pública del destinatario del mensaje. PKCS#2 y PKCS#4 se han incorporado a la PKCS#1

2) PKCS#3 (Diffie-Hellman Key-Agreement Standard) en éste se describe un método para implementar el intercambio de claves Diffie-Hellman.

3) PKCS#5 (Password-Based Encryption Standard) en esta norma se describe un método para cifrar los mensajes con la clave secreta. Su objetivo es permitir la transmisión cifrada de claves privadas entre dos ordenadores como se describe en el PKCS#8.

4) PKCS#6 (Extended-Certificate Syntax Standard), ésta describe una sintaxis para certificados extendidos, esto es que se pueden extraer certificados X.509 de un superconjunto. Además se incluyen atributos como la dirección electrónica.

5) PKCS#7 (Cryptographic Message Syntax Standard) proporciona una sintaxis general para los datos que tengan una operación criptográfica asociada ya sea cifrado o firmado. La sintaxis es recursiva de tal modo que se puede anidar mensajes cifrados, también proporciona un método para distribuir certificados o listas de revocación de certificados, con esto se puede decir que el PKCS#7 es compatible con varias arquitecturas de gestión de claves basadas en certificados.

6) PKCS#8 (Private-Key Information Syntax Standard) ésta indica una sintaxis para la información de la clave privada, la que incluye una clave privada, una serie de atributos y una sintaxis para las claves que se utilizarán.

7) PKCS#9 (Selected Attribute Types) en éste se describe algunos atributos para el uso de los certificados extendidos, para los mensajes que son firmados digitalmente, para la información de la clave privada y para las peticiones de firmado de certificados.

8) PKCS#10 (Certification Request Syntax Standard) describe la sintaxis para las peticiones de certificados, ésta petición de certificado consiste en un nombre distinguido o distinguished name, una clave pública y otros atributos que son opcionales, todo esto firmado con la clave privada de la persona que hace la petición. Esta petición se envía a una Autoridad Certificadora, esta autoridad transforma la petición en un certificado X.509 v3 o en un certificado extendido.

9) PKCS#11(Cryptographic Token Interface Standard) especifica una interfaz de programación llamada Cryptoki para utilizarlo con dispositivos criptográficos de cualquier tipo. Cryptoki tiene un enfoque basado en objetos lo que hace que las

aplicaciones realicen operaciones criptográficas sin saber la tecnología de los dispositivos.

10) PKCS#12 (Personal Information Exchange Syntax Standard) se describe la sintaxis para almacenar en software las claves públicas del usuario, para proteger sus claves privadas, los certificados y cualquier tipo de información relacionada con la criptografía. Su finalidad es la utilización de un único fichero de claves que se pueden ser accesibles desde cualquier aplicación.

11) PKCS#13 (Elliptic Curve Cryptography Standard) que describe un método de utilización de algoritmos de curva elíptica, la manera de generar y validar los parámetros, las claves, el procedimiento de firmado y cifrado, etc. Esta es muy similar a la PKCS#1

12) PKCS#15 (Smart Card File Format), surge como una necesidad de cubrir ciertos aspectos que no se contemplan en el PKCS#11. Trata de uniformizar la estructura de directorios y ficheros de las tarjetas inteligentes.

2.3.2.- ESTÁNDAR ITU-T X.509

2.3.2.1.- Origen y Definición

X.509 fue diseñado a mediados de los años 80, por la ISO (International Organization for Standardization), esto se desarrolló antes del enorme crecimiento de usuarios en Internet. Por lo que diseñó para operar en un ambiente donde sólo los computadores se interconectaban intermitentemente entre ellos. En las versiones 1 y 2 de X.509 se utilizan CRLs (Certificate Revocation List) muy simples que no solucionan los problemas actuales.

En la versión 3 el cambio fundamental es el formato de los certificados y los CRLs pues son extensibles. Ahora los que implementen X.509 pueden definir el contenido de los certificados como crean conveniente, se permite que una

organización pueda definir sus propias extensiones para contener información específica dentro de su entorno de operación

Éste estándar en su versión 3 es el más difundido en cuanto a certificados. Esta recomendación es la norma generalmente aceptada por numerosos entornos y permite economías de alto nivel gracias a las cuales las transacciones y comunicaciones de comercio electrónico son extremadamente seguras, desde las transacciones entre consumidor que tenga un riesgo limitado, hasta transacciones importantes entre empresas.

La industria de la tecnología de la información y comunicación en general considera que el estándar X.509 es la mejor referencia para las aplicaciones que se relacionan con Infraestructuras de Clave Pública (PKI).

Un certificado X.509 es comúnmente un archivo pequeño que contiene información como: nombre distintivo de la entidad, nombre Distintivo de la Autoridad Certificadora, período de Validez e información adicional.

2.3.2.2.- Formato del Certificado

De acuerdo a la versión del certificado han ido variando y actualmente existen tres versiones del certificado, la estructura de éstos se muestran a continuación:

1) Formato del certificado X.509 v1

```
Certificate ::= SIGNED SEQUENCE{
version                 [0] Version DEFAULT 0,
serialNumber            CertificateSerialNumber,
signature               AlgorithmIdentifier,
issuer                  Name,
validity                Validity,
subject                 Name,
```

SubjectPublicInfo SubjectPublicInfo}

version, indica la versión del certificado
serialNumber, es el número de identificación y es único para el certificado.
signature, es la firma digital de la Autoridad Certificadora (CA), se utiliza para firma el certificado y probar su autenticidad.
Issuer, es el nombre de la CA emisora.
validity, indica la fecha de inicio y validez del certificado.
subject, es el nombre del propietario de la clave privada.
SubjectPublicInfo, contiene el valor de la clave pública del propietario.

2) Para la versión del certificado X.509 v2 se añadieron los siguientes campos:

issuerUniqueId [1] IMPLICIT BIT STRING PTIONAL,
SUBJECTUniqueId [1] IMPLICIT BIT STRING OPTIONAL }

IssuerUniqueId, este es un campo opcional que se usa para identificar aún más a la Autoridad Certificadora que emite el certificado.
SUBJECTUniqueId, también es opcional y se utiliza para identificar de manera única al propietario del certificado.

3) Luego aparece la versión 3 del X.509, a este se agregaron las denominadas extensiones X.509 que permitían se incluyera información adicional en el certificado.

Certificate ::= SEQUENCE {
tbsCertificate TBSCertificate,
signatureAlgorithm AlgorithmIdentifier,
signatureValue BIT STRING}

TBSCertificate ::= SEQUENCE {

```
version                 [0]  EXPLICIT Version DEFAULT v1,
serialNumber            CertificateSerialNumbesignature,
signature               AlgorithmIdentifier,
issuer                  Name,
validity                Validity,
subject                 Name,
subjectPublicKeyInfo    SubjectPublicKeyInfo,
issuerUniqueID          [1]  IMPLICIT UniqueIdentifier OPTIONAL,
-- If present, version shall be v2 or v3
subjectUniqueID         [2]  IMPLICIT UniqueIdentifier OPTIONAL,
-- If present, version shall be v2 or v3
extensions              [3]  EXPLICIT Extensions OPTIONAL
-- If present, version shall be v3
}
```

tbsCertificate, contiene la información que se explicó en las versiones anteriores.
SignatureAlgorithm, indica el tipo de algoritmo que será utilizado por la Autoridad Certificadora para firmar el certificado.
SignatureValue, contiene la firma del certificado.

Gráficamente los campos que componen el Certificado X.509 v3 sería:

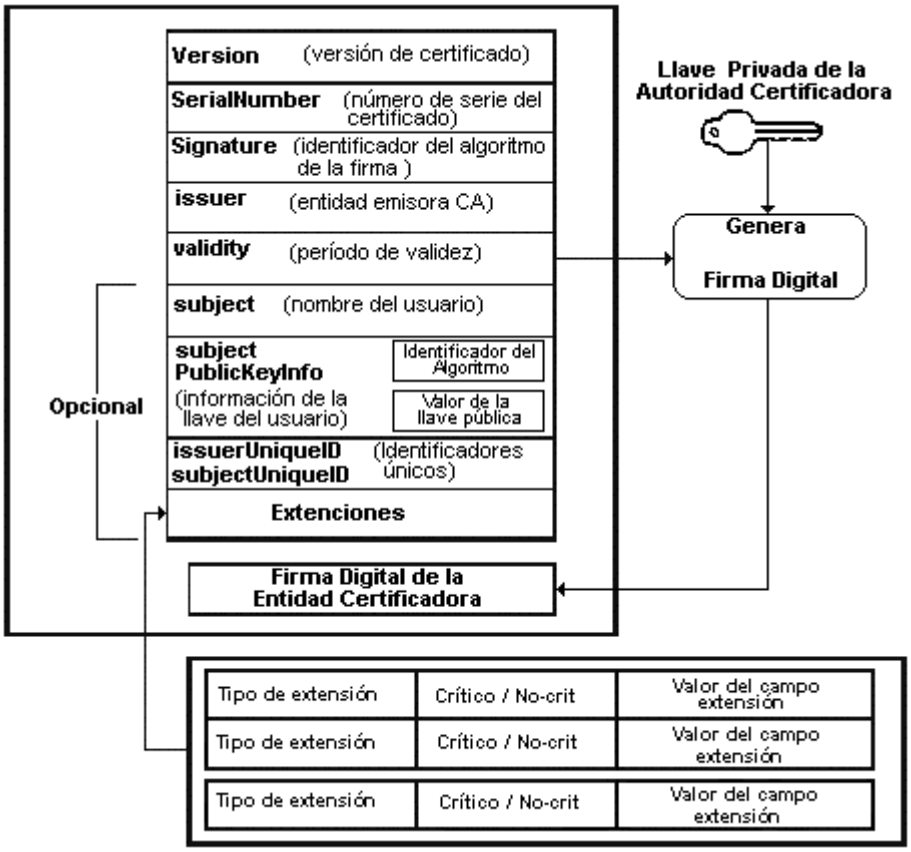

Figura 2.6

2.3.2.3.- Extensiones del certificado

Las extensiones del certificado X.509 v3 suministran los métodos para la asociación adicional de atributos con usuarios y llaves públicas, para gestionar la jerarquía de los certificadores y gestionar la distribución del CRL (Certificate Revocation List).

Pueden existir extensiones privadas, pero deben ser definidas en el certificado como crítica o no crítica. Es decir un sistema que usa los certificados y se encuentra uno crítico y que no lo reconoce, éste debe ser desechado, y en el caso que sea no crítico, entonces ignorado. Existen también extensiones estándar y son los que a continuación se especifican:

1) Identificador de la llave de la Autoridad, da un significado sobre la identificación de una llave pública particular para signar un certificado. La identificación se puede basar tanto con el identificador de llave o el nombre publicado y el número de serie. Esta extensión se debe incluir en los certificados.

2) Identificador de la llave del sujeto, identifica la llave pública particular en una aplicación, en donde la referencia a un identificador de llave pública es necesario, además se incluye un certificado asociado, que es usado con el sujeto de la llave pública. Esta extensión debe marcarse como no crítica.

3) Uso de la llave, la restricción de uso debe ser empleada cuando una llave para muchos propósitos, debe ser estricta, se considera una extensión crítica.

4) Período de uso de la llave privada, no se recomienda el uso de esta extensión. Autoridades de Certificación con este perfil no generan certificados con llaves privadas.

5) Políticas de Certificados, contiene una secuencia de políticas con términos de información, donde cada uno consiste en un identificador de objeto y calificadores opcionales. Estas políticas de términos de información indican la política bajo la cual los certificados son nombrados y para qué vamos a utilizar el certificado.

2.3.3.- ADVANCED ENCRYPTION STANDARD (AES)

2.3.3.1.- Origen y Definición

Un antecesor del AES es el Data Encryption Standard (DES), que en el año de 1973 el National Bureau of Standard (NBS) lo adoptó como el estándar de cifrado para la seguridad de documentos oficiales. La norma del DES exige se implemente un circuito integrado electrónico. El chip de DES es un producto estratégico estadounidense. El ANSI (American National Standards Institute,

USA) adopta el DES con el nombre de DEA (Data Encryption Algorithm) el cual no exige la implementación del algoritmo en un chip, pudiendo ser programado mediante software.

Luego de más de 25 años, en octubre del 2000 el Instituto Nacional de Estándares y Tecnología (NIST) anunció que el Advanced Encryption Standard (AES) sería el estándar de encriptación capaz de proteger la información más sensible de los usuarios así como del gobierno estadounidense.

Fue desde 1997 en que el NIST convocó a propuestas para un nuevo sistema de cifrado estándar. En 1998 se seleccionó a 15 candidatos posibles para alcanzar el estándar, un año después la lista se depura a tan sólo cinco candidatos el MARS de IBM, el RC6TM de RSA Laboratories, el Rijndael de Joan Daemen y Vincent Rijmen, el Serpent de Ross Anderson, Eli Biham, Lars Knudsen y el Twofish de Bruce Schneier, John Ke sey, Doug Whiting, David Wagner, Chris Ha , Niel Ferguson. Es cuando en el 2000 se adopta como estándar al AES o más conocido como Rijndael.

Rijndael es un cifrador que opera con bloques y claves de longitudes variables que pueden ser especificadas independientemente a 128, 192 ó 256 bits. Se lo puede aplicar a una amplia variedad de transacciones electrónicas: desde cajeros automáticos, comercio electrónico, e-mails confidenciales, etc. Por esto se afirma que, el AES ayudará a proteger las infraestructuras de información crítica y asegurar la privacidad de la información personal de todos los usuarios.

Los motivos para seleccionar a Rijndael, según el web del NIST son su buena combinación de seguridad, velocidad, eficiencia tanto en memoria y puertas lógicas, así como sencillez y flexibilidad.

2.3.3.2.- Funcionamiento del Rijndael.

El fundamento teórico se basa en el álgebra de cuerpos finitos GF (2^8) a nivel de byte. La estructura del estándar es:

1) Iteración inicial de aplicación de la clave.

2) N iteraciones secuenciales (donde N = 10, dependiendo de los tamaños del bloque). Estas iteraciones tienen tres etapas invisibles que son: etapa de mezcla lineal, etapa no lineal y etapa de aplicación de la clave.

3) Iteración final.

El estado puede representarse como un array rectangular de bytes de cuatro filas y la transformación u operaciones sobre los bloques que tiene lugar en cada vuelta de cifrado a su vez está compuesta de cuatro transformaciones diferentes.

Las operaciones sobre los bloques son:

- Bytesub o sustitución de bytes, se compone de dos operaciones y actúa sobre cada uno de los bytes del estado.

- ShiftRow o desplazamiento de filas, traslada cíclicamente cada fila a un número de bytes independientes.

- MixColumn o mezcla de columnas, equivale a una multiplicación de matrices por polinomios.

- AddRoundKey o adición de la clave de vuelta, se realiza una operación XOR entre el estado que es el resultado intermedio del cifrado y la clave. La clave de cada vuelta se deriva de la clave de cifrado mediante el esquema de clave. El esquema de clave consiste en dos operaciones: expansión de clave y selección de clave de vuelta de cifrado

Gráficamente la estructura de texto o denominado estado y la clave en un array bidimensional de bytes es:

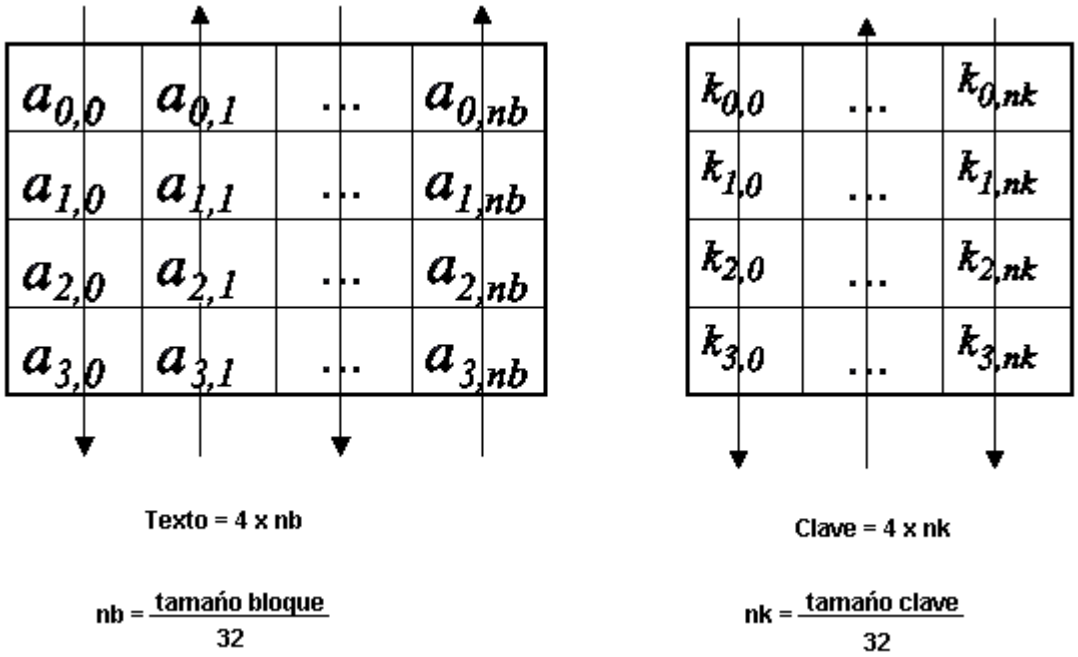

Figura 2.7

Todas las aplicaciones y comunicaciones en Internet, especialmente las bancarias, que hacían uso del DES, están siendo actualizadas paulatinamente a Rijndael, de manera que se espera que del DES no quede rastro más que en los libros de texto.

Como el AES es un algoritmo público y no necesita ser licenciado, cualquier otro país distinto de los EEUU podrá adoptarlo igualmente como estándar en sus propias aplicaciones si así lo desea.

2.3.4.- DIGITAL SIGNATURE STANDARD (DSS)

2.3.4.1.-Origen y Definición

El Digital Signature Standard (DSS) fue especificado por el National Institute of Standards and Technology (NIST) con la colaboración de la National Security

Agency (NSA), propuesto en el año de 1991 y fue adoptado como estándar en el año de 1994.

El DSS es un sistema de firma digital adoptado como estándar por las organizaciones estadounidenses, utiliza el algoritmo asimétrico Digital Signature Algorithm (DSA).

2.3.4.2.- Digital Signature Algorithm

El Digital Signature Algorithm (DSA), produce una firma digital en forma de un par de números grandes; se calcula con reglas y parámetros, verifica la identidad del firmante y la integridad de los datos firmados, los parámetros son:

- KG claves públicas de grupo, comunes y públicas en un grupo de usuarios.
- KU clave pública, generada por un usuario a partir de la KG, es pública.
- KP clave privada, es del usuario, se genera a partir de las anteriores.
- k número aleatorio, éste número se genera uno para cada firma.
- s y r, son dos palabras de 160 bits que forman la firma de un texto.

El número k permite que el texto del un mismo usuario no genere siempre la misma firma. El siguiente esquema resume el funcionamiento de este algoritmo:

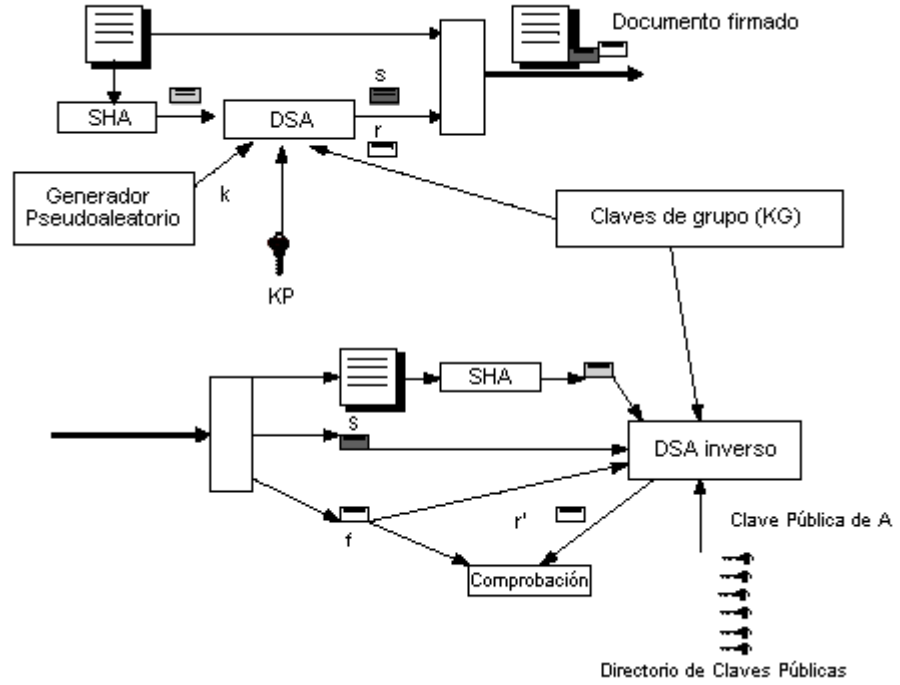

Figura 2.8

2.3.4.3.- Funcionamiento

Generación de las claves, en donde cada usuario realiza los siguientes pasos:

- Elige q primo, $2^{159} < q < 2^{160}$ (160 bits).
- Elige p primo de 1024 bits tal que q | (p - 1).
- Elige $x \in Z_P$ y calcula $g = x^{\frac{p-1}{q}} \bmod p$. Si g = 1 se toma otro x. g es el generador de un grupo cíclico.
- Elige $r \in [2, q - 1]$ aleatorio.
- Calcula $u = g^r \bmod p$.
- La clave pública es { p, q, g, u }, la clave privada es r.

Firma, para firmar el mensaje m se realiza los siguientes pasos:

- Se elige $k \in [2, q - 1]$ aleatorio.
- Se calcula $f^1 = (g^k \bmod p) \bmod q$.

- Se calcula k^{-1} mod q.
- Se calcula $f_2 = k^{-1} (SHA1(m) + rf_1)$ mod q. Si $f_2 = 0$ se toma otro k.
- La firma es el par (f_1, f_2).

Verificación de la firma, para comprobar la firma (f_1, f_2) del mensaje m es de A se realiza los siguientes pasos:

- Se busca la clave pública de A, { p, q, g, u }.
- Se calcula $w = f_2^{-1}$ mod q.
- Se calcula $\alpha_1 = SHA1(m)\ w \mod q$ y $\alpha_2 = f_1 w \mod q$.
- Se calcula $v = (g^{\alpha 1}\ u^{\alpha 2} \mod p)$.
- La firma es válida si $v \equiv f_1 \mod q$.

2.3.5.- LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

2.3.5.1.- Definición

El Lightweight Directory Access Protocol (LDAP) o Protocolo Ligero de Acceso a Directorios es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio, es el estándar para almacenar y recuperar certificados de la Lista de Certificados Revocados. Fue desarrollado por el IETF como una simplificación para acceso a directorios X.500, para un entorno PKI los servidores LDAP son la mejor opción para almacenar certificados.

Un servicio de directorio es como una base de datos, aunque no lo es, ya que procesa miles de cambios por minuto, contiene información descriptiva y basada en atributos. Su función básica es la de proporcionar una respuesta rápida cuando se hagan búsquedas o consultas.

La IETF trabaja para estandarizar esquemas LDAP que pertenezcan a certificados y CRLs, como es el caso de servidores de certificados y productos de

autenticación que se basan en el contenido de certificado y la estructura del directorio, lo que incrementa la interoperabilidad entre productos LDAP.

2.3.5.2.- Funcionamiento

Un servicio de directorio LDAP consta de uno o más servidores que contienen datos, con el que se forma un árbol de directorio LDAP o base de datos troncal.

Básicamente el cliente LDAP se conecta con el servidor LDAP para realizar cualquier consulta o búsqueda, el servidor le contesta con una respuesta a la consulta o un indicativo donde puede encontrar más información que es otro servidor LDAP.

2.3.5.3.- Estructura de un árbol de directorios LDAP

Los servidores de directorios LDAP almacenan los datos jerárquicamente como los árboles DNS. Muchas compañías utilizan este esquema el que consta de unidades organizacionales (OU), que representan una organización funcional, es decir ventas, administración, finanzas, etc. Los niveles inferiores a las OUs se utilizan para separar categorías.

2.3.5.4.- Registros LDAP

Las entradas que almacena un directorio LDAP tienen un Distinguished Name (DN), este a su vez tiene dos partes: el Nombre Distinguido Relativo o Relative Distinguished Name (RDN) y la localización del registro dentro del directorio LDAP.

El RDN es una porción del Distinguished Name no relacionada con la estructura del árbol de directorio. Para almacenar un objeto en un directorio LDAP se utiliza el atributo cn o Common Name, dicho cn es la base para el RDN.

2.4. ESTÁNDARES PARA PROTOCOLOS DE SEGURIDAD EN COMUNICACIONES

2.4.1.- PRIVATE COMUNICATIONS TECHNOLOGY (PCT)

2.4.1.1.- Definición

El protocolo Private Communication Technology (PCT) o Tecnología Privada de Comunicaciones, es un mecanismo general de acceso seguro. Se lo utiliza para comunicaciones de negocios y personales a través de Internet. PCT incluye posibilidades de autentificación e identificación mutua. Fue desarrollado por Microsoft, creado sobre los primeros logros del Secure Sockets Layer (SSL).

Básicamente el protocolo PCT se creó para evitar la escucha electrónica en aplicaciones cliente / servidor. El objetivo de PCT es proporcionar una vía de acceso de comunicación privada entre un cliente y un servidor. Al igual que SSL, PCT requiere un protocolo de transmisión fiable, como TCP, asimismo PCT es un protocolo independiente del protocolo de aplicaciones, por lo que protocolos de aplicaciones de nivel más alto como HTTP o FTP pueden superponerse y operar de forma transparente.

2.4.1.2.- Funcionamiento

El protocolo PCT inicia las conexiones estableciendo una comunicación para negociar el algoritmo y la clave de encriptación simétrica. PCT emplea claves públicas asimétricas certificadas. Esta regla ayuda a PCT a resolver uno de los problemas de seguridad de SSL potenciales.

PCT no especifica detalles en relación con la verificación del certificado, espera que el programador aporte una función que decida la validez de los certificados recibidos. Aplicar sus propias normas de validación en realidad es una ventaja, ya

que se puede elegir un sistema de certificación en función de las necesidades y no las de un protocolo de transferencia seguro.

Establecida la comunicación, PCT encripta todas las transmisiones de datos empleando la clave de sesión negociada durante el proceso de establecimiento de la comunicación.

2.4.1.3.- Diferencias entre PCT y SSL

1) La estructura del mensaje de PCT es bastante más corta que la del protocolo SSL. En una sesión reconectada sin autentificación de cliente sólo precisa un mensaje en cada dirección.

2) PCT ofrece una gama más amplia de características de protocolo en los algoritmos y los formatos criptográficos negociados, el tipo de cifrado y de certificado del servidor. También negocia el tipo de función hash e intercambio de claves. Si se necesita la autentificación de cliente, PCT negocia el tipo de firma y certificado del cliente.

3) Para la autentificación de mensajes se emplean claves distintas a las de encriptación. Esto posibilita claves de autentificación de mayor longitud, para que el proceso de autentificación sea mucho más seguro.

4) En la secuencia interrogación / respuesta de la autentificación de cliente de PCT se emplea el tipo de cifrado que se ha negociado para la sesión. En la autentificación de cliente de SSL se emplea un cifrado más débil que es independiente del tipo que se haya negociado para la sesión.

2.4.2.- INTERNET PROTOCOL SECURITY (IPSEC)

2.4.2.1.- Definición

Son un conjunto de protocolos que sirven para cifrar tanto el establecimiento de la conexión como el tráfico entre dos computadoras. IPsec proporciona seguridad en el nivel IP facilitando un sistema de selección que necesita protocolos de seguridad, que determinen los algoritmos para cada servicio.

IPsec puede ser utilizado para proteger uno o más caminos entre un par de servidores, pasarelas de seguridad o entre una pasarela y un servidor. La pasarela se refiere a un sistema intermediario que implementa el protocolo IPsec, como un router o un firewalls.

Los servicios que ofrece Ipsec son confidencialidad asegurando que nadie pueda comprender los datos excepto el receptor. Integridad garantizando que los datos no puedan ser cambiados en el camino. Autenticidad a través de la firma de datos para verificar al remitente. Además protección a la replica que asegura que una transacción sólo se la puede realizar una vez.

De un modo lógico, IPsec funciona en cualquiera de estos tres modos: Anfitrión-a-Anfitrión, Anfitrión-a-Red y Red-a-Red.

2.4.2.2.- Funcionamiento del IPsec

1) Authentication Header (AH) o Cabecera de Autenticación, provee autentificación a los datos originales, integridad en la conexión y protección a la replica en mensajes de respuesta. Asegura las partes de la cabecera IP del paquete como pueden ser las direcciones de origen y destino.

2) Encapsulating Security Payload (ESP) o Carga Útil de Seguridad Encapsulada, provee confidencialidad de los datos mediante la encriptación,

además de limitar el flujo del tráfico confidencial. Proporciona también integridad en la conexión y un servicio antirepetición de mensajes. ESP es utilizada en la mayoría de las aplicaciones.

3) Internet Key Exchange (IKE) o Intercambio de Claves Internet, es un protocolo que maneja las claves entre dos dispositivos que se comunican estableciendo varias conexiones conocidas como Asociación de Seguridad o SA

IPsec incorpora facilidades para la especificación de qué servicios de seguridad se quieren usar y en qué combinaciones. Estos protocolos controlan el acceso y son los que distribuyen las claves criptográficas de la seguridad de flujo de tráfico. IP sec es la manera más general de proveer servicios de autenticación y encriptación para internet, así lo demuestra el siguiente gráfico:

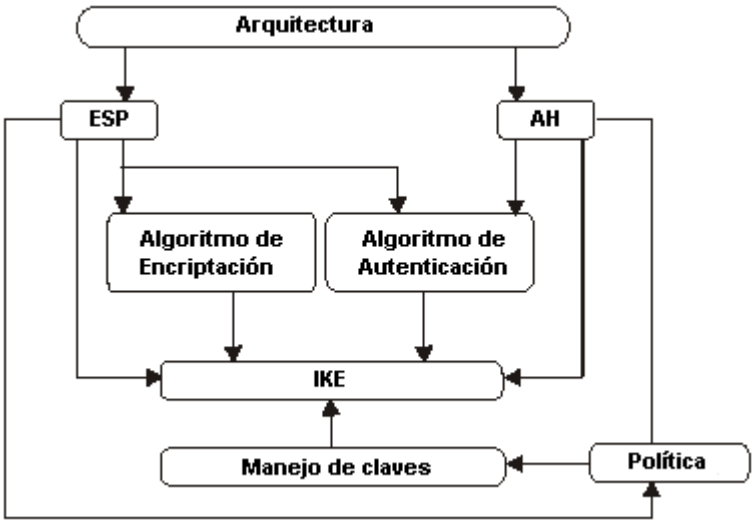

Figura 2.9

2.4.2.3.- Asociación de Seguridad

Una SA es una conexión IP entre dos host, entre dos gateways o entre un host y un gateway. Generalmente un SA se identifica por medio de un número de 32 bits elegido aleatoriamente denominado SPI y por la dirección de destino correspondiente. Dicho número se inserta en el encabezamiento del IPsec

Luego una base de datos relaciona los SPI con parámetros que caractericen a la conexión. Básicamente la información de la base de datos son: el algoritmo identificador de autenticación (AH), el algoritmo identificador de encriptado (ESP), los tiempos de vida de las claves y el vector de inicialización (VI) para establecer el estado inicial de los algoritmos.

En cuanto a los servicios de seguridad las SAs pueden estar orientadas al host o al usuario. La primera trabaja con la misma clave de sesión para todos los usuarios del host y la segunda cada usuario tendrá una clave de sesión diferente.

2.4.2.4.- Modos de Operación

Una asociación de seguridad (SA) detalla los servicios de seguridad que se aplicarán en el tráfico entre dos dispositivos que se conectan. Cada extremo que se comunica establece una SA intercambiando las claves de seguridad correspondientes. Varios enrutadores, firewalls y servidores de acceso soportan Ipsec en modo túnel, mientras que hay aplicaciones en las que se implementa el modo transporte.

Modo Túnel

Se usan gateways entre las redes que se comunican. En este modo los paquetes que van del host al gateway o viceversa viajan en texto plano sin encriptar, se establece un túnel por cada computadora que se conecte, por lo tanto en varias redes podría haber varios túneles en paralelo.

Para instalar un túnel Ipsec cada gateway se configura definiendo las subredes que se comunican, los algoritmos de autenticado y encriptado e incluso el secreto precompartido que permite identificar a los extremos que se comunican. Este modo es usual entre firewalls que operan como gateways de seguridad entre redes a través de Internet

Modo Transporte

Cumple sus funciones básicas de encriptado y autenticado a lo largo de una comunicación. En este modo el encabezamiento IPSec se inserta entre el encabezamiento IP y el encabezamiento siguiente, generalmente de Capa 4, TCP o UDP.

El modo de transporte puede ser útil especialmente para evitar accesos indebidos dentro de las propias redes donde se encuentra cada una de las máquinas que se comunican. En este caso los datos de los paquetes bajo IPSec viajan encriptados no sólo a través de Internet sino dentro de las propias LANs o intranets de los extremos.

2.4.2.5.- Configuración de Ipsec

Existen dos entidades administrativas que controlan al paquete. Una es la Base de Datos de Asociación de la Seguridad o Security Association Database (SAD), llamado TDB o tabla TDB, y el otro es la Base de Datos de Política de la Seguridad o Security Policy Database (SPD).

SPD se usa para paquetes salientes, para decidir qué entradas SAD se deben usar, y qué entradas SAD describen el proceso y sus parámetros. Las entradas SPD especifican las entradas SAD existentes a usar, pero si no hay una que se pueda usar, entonces se usa para crear nuevas.

SPD puede especificar qué tráfico debería bordear IPsec, y cuál se debería dejar caer, así que también debe ser consultado para tráfico no IPsec entrante. Las entradas SPD se deben ordenar de forma explícita, ya que varias podrían coincidir con un paquete particular, y el proceso debe ser reproducible.

Cada SA puede definir una cabecera ESP y una cabecera AH. Una sesión de IPsec debe tener una de las dos o ambas, pero no se puede definir sin ninguna de las dos.

2.4.3.- SECURE SHELL (SSH)

2.4.3.1.- Definición

Secure Shell (SSH), es un protocolo diseñado para dar seguridad entres dos computadoras que están accediendo en forma remota. SSH utiliza un canal de comunicación encriptado y mecanismos de validación de usuarios bastante sofisticados. SSH utiliza el puerto 22 para la comunicación, además se necesita que en el servidor exista un demonio que mantenga continuamente dicho puerto al servicio de la comunicación.

Toda la comunicación se lleva a cabo utilizando un canal encriptado, este canal se establece con un servidor que tiene una clave RSA (algoritmo de encriptación asimétrica) de 1024 bits y cada vez que se levanta el sshd o a cada hora se genera una clave RSA de 768 bits.

SSH provee autenticación y comunicación segura sobre un canal inseguro y nace como un reemplazo a los comandos telnet, ftp, rlogin, rsh, y rcp, los cuales proporcionan gran flexibilidad en la administración de una red, sin embargo, presenta grandes riesgos en la seguridad de un sistema.

2.4.3.2.- Protocolos de SSH

1) SSH1, este protocolo ssh cliente / servidor es utilizado libremente para propósitos no comerciales, es ampliamente usado en ambientes académicos.

2) SSH2, provee licencias más estrictas que SSH1 ya que es de carácter comercial. La ultima versión de ssh cliente / servidor para Unix con este protocolo es utilizado libremente respetando la licencia.

2.4.3.3.- Funcionamiento

SSH tiene una arquitectura cliente-servidor, cuando el usuario desea conectarse, la aplicación cliente intercambia una clave de sesión que es aleatoria con el servidor. El resto de la conexión va cifrada utilizando dicha clave.

- Primero el cliente envía una señal al servidor pidiéndole comunicación por el puerto 22.

- El servidor acepta la comunicación en el caso de poder mantenerla bajo encriptación mediante un algoritmo definido, le envía la llave publica al cliente para que pueda descifrar los mensajes.

- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

SSH usa el mecanismo RSA (algoritmo de encriptación asimétrica). Básicamente cada usuario crea dos claves, una es la pública que puede darse a y la otra es la privada que tiene que ser protegida. Esta clave se genera usando el comando ssh-keygen, se generan passwords en forma aleatoria, la pública es almacenada en texto plano y la privada se encripta y guarda en forma binaria. El largo de la clave es 1024 bits por defecto lo cual es bastante seguro.

La clave se encripta usando 3DES, Blowfish u otro mecanismo de encriptado que sea en una sola dirección. Para proteger la clave privada se usa una passphrase de entre 10 y 30 caracteres, esa frase pasa por una hash para obtener la cantidad de bits necesarios. Un problema que aparece con SSH es el

ingreso de la passphrase cada vez que se quiera validar, esto puede volverse bastante tedioso si se está compilando un programa en forma local.

2.4.3.5.- Utilidad del SSH

Para utilizar SSH, primero se debe obtener la herramienta, que la podemos bajar desde internet. Luego se deberá desempaquetarla y ejecutar setup.exe para instalará. Entre las ventajas del SSH son que protege contra:

IP spoofing: en la que una máquina remota envía paquetes que pretenden venir desde otra. SSH protege contra un spoofer en la red local, el cual puede engañar haciendo creer que es el router de salida al exterior.

IP source routing: en al que una máquina pretende que un paquete IP viene desde otra máquina conocida.

DNS spoofing: un atacante falsifica los registros del servidor de nombres.

Intercepción de passwords en texto plano y otros datos en máquinas intermedias.

Manipulación de datos por personas en control de máquinas intermedias.

Ataques basados en escuchar las autentificaciones de aplicaciones remotas y "spoofed conections" al servidor. Es decir que, SSH nunca confía en la red. Un extraño que pueda haber tomado control de la red lo único que puede hacer es forzar una desconexión de SSH pero no puede desencriptar el tráfico.

Sin embargo SSH no ayuda con nada que comprometa la seguridad de la máquina de alguna otra forma distinta de las mencionadas. Una vez que un atacante a ganado acceso de root a la máquina, puede hacer cualquier cosa.

2.5. ESTÁNDARES PARA CORREO ELECTRÓNICO

La seguridad en el correo electrónico es primordial en la actualidad, se supone que el correo es confidencial, pero en Internet, esto no es implícito, es decir, en una comunicación entre dos usuarios el mensaje de correo enviado por el emisor pasa por un gran número de máquinas hasta llegar al receptor y el mensaje puede haber sido leído, registrado o modificado, etc.

Por lo tanto se hace necesario utilizar herramientas basadas en criptografía para poder enviar y recibir correo electrónico seguro. Seguidamente se estudiarán algunas de las normas de seguridad para el correo electrónico más extendidas en Internet.

2.5.1.- PRETTY GOOD PRIVACITY (PGP)

2.5.1.1.- Origen y Definición

El protocolo Pretty Good Privacity (PGP) fue creado por Philip Zimmermann en 1991y la intención de su creador era ofrecerlo gratuitamente por medio de Internet, pero esto le trajo problemas judiciales con el gobierno de Estados Unidos, ya que violaba las leyes de ese país. Ventajosamente el problema se solucionó creando dos versiones, una americana que es la 2.6.2 con la librería RSAREF, válida solo para ese país y otra internacional la 2.6.3.i con la librería MPILIB, válida para el resto del mundo.

El PGP es un sistema de encriptación por llave pública y se creó para proporcionar una forma segura de intercambio de correo electrónico. Es un paquete completo de seguridad freeware para comprimir, cifrar y/o firmar ficheros para su intercambio, presta servicios de encriptación, autenticación, firmas digitales y compresión de datos.

Su fácil utilización, calidad y más que todo disponibilidad en diversas plataformas a hecho que se convierta en el protocolo freeware más utilizado, desplazando a otros estándares de Internet. Las restricciones impuestas por el gobierno estadounidense a la exportación de sistemas de encriptación han creado conflictos con relación a las patentes de los algoritmos, especialmente el RSA, que ha sido utilizado por el PGP.

2.5.1.2.- Características

El PGP provee de un envoltorio digital, que es un mecanismo que aprovecha las ventajas de los métodos de criptografía de clave secreta y clave pública para que el mensaje sea cifrado mediante un algoritmo simétrico, para lo cual utiliza una clave temporal, que a su vez cifra asimétricamente con la clave pública del usuario destino, de ésta forma se emplea la rapidez del cifrado simétrico y la gestión de claves del cifrado asimétrico.

Los algoritmos criptográficos que emplea PGP son RSA (algoritmo de encriptación asimétrica) para la generación de claves y firma del mensaje, IDEA o DES para el cifrado del mensaje y MD5 para la generación de un resumen del mensaje. Para utilizar PGP primero se genera un par de claves una privada y otra publica, PGP solicita se introduzca el tamaño de las claves que están en un rango de 348 a 2048 bits.

La clave pública es entregada a los destinatarios para establecer comunicaciones seguras. Esta clave es almacenada en fichero especial tipo ASCII denominado certificado de clave, éste incluye el identificador del propietario un sello de la hora en que se generó las claves e información propia de la clave. El manejo de claves en PGP se realiza mediante llaveros, un usuario puede tener varios pares de llaves para él, y utilizarlas en caso de que sospeche que alguna ya no sea segura. El usuario también puede tener un llavero con claves públicas.

El éxito del PGP entre otras está en que el paquete freeware incluye el código fuente y documentación, con esto se pueden incorporar mejoras, no está bajo el control de ningún gobierno o empresa, está basado en algoritmos seguros y extensamente probados.

2.5.1.3.- Niveles de Confianza y Gestión de Claves

La gestión de claves en PGP se fundamenta en niveles de confianza dados por una tercera parte o por el mismo usuario. Cada usuario mantiene dos bases de datos: un anillo de claves privadas o secring y otro anillo de claves públicas o pubring. El primero contiene pares de claves una privada y otra pública personales, que están asociadas a un identificador de 64 bits y a una o varias direcciones de correo electrónico.

De la misma forma en el anillo de claves públicas se encuentran todas las entradas de destinatarios del usuario, permitiéndole cifrar el mensaje mediante la clave pública. En este anillo se indica para cada entrada el nivel de confianza depositado en el usuario de la clave, de ésta forma la clave estará sin certificar, autocertificada o certificada por otro usuario.

Por consiguiente PGP ofrece tres niveles de confianza: ninguno, parcial y completo. Además existe un cuarto nivel denominado no definido, que no aporta nada a la entrada del anillo de claves públicas.

PGP no utiliza autoridades de certificación, en su lugar existen bases de datos con claves públicas que no son tan fiables, a esto se añade que no adopta una estructura jerárquica, la ambigüedad cuando se revoca alguna clave y su invalidez jurídica. Sin embargo es una opción para las comunicaciones seguras entre usuarios que intercambian proyectos, ideas, etc.

2.5.1.4.- Funcionamiento.

Para que PGP inicie se necesita de dos usuarios, que para el caso son X, Y. Los pasos que se siguen para el envío son:

1) PGP utiliza MD5 para dispersar el mensaje, con lo que se obtiene un resumen de dicho mensaje.

2) El resumen del mensaje se cifra mediante la clave privada RSA del usuario X, con lo que se obtiene la firma digital del mensaje

3) Después PGP concatena la firma con el mensaje original y lo comprime.

4) La salida comprimida es cifrada simétricamente a través de IDEA con una clave denominada de sesión(K), ésta es generada en tiempo de ejecución.

5) La clave de sesión o sea K se cifra mediante la clave pública del usuario Y.

6) Luego la clave cifrada IDEA y el mensaje comprimido cifrado se concatenan obteniéndose la salida cifrada y firmada que sólo podrá conocer el usuario Y.

7) El usuario Y mediante su clave privada RSA, descifra la clave de sesión o K, con ésta clave descifrará el mensaje.

8) Para verificar el origen, mediante la clave pública del usuario X, el usuario Y sabrá que viene firmado por el usuario antes mencionado descifrando el resumen.

Hay que mencionar que RSA (algoritmo de encriptación asimétrica) se emplea dos veces, para firmar el mensaje y para cifrar la clave de sesión. Aunque RSA es un algoritmo lento solamente debe cifrar 256 bits, que corresponden a los 128

bits del resumen MD5 y 128 de la clave IDEA. En realidad el que realiza el cifrado de mayor volumen de datos es IDEA.

2.5.2.- SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

2.5.2.1.- Definición

El Protocolo de Transferencia de Correo Simple (SMTP) es un protocolo TCP/IP utilizado en el envío y recepción de e-mails, define el mecanismo para mover correo entre diferentes máquinas, debido a que su capacidad es limitada para fijar los mensajes que va recibiendo, con frecuencia utiliza los protocolos Post Office Protocol (POP3) o Internet Message Access Protocol (IMAP).

Utiliza estos protocolos para que los usuarios almacenen sus mensajes en el buzón del servidor y puedan descargarlos periódicamente desde el servidor. Esto quiere decir que los usuarios utilizan programas con SMTP para enviar su e-mail y utilizan POP e IMAP para recibirlo.

Durante la sesión SMTP el origen y destino intercambian una secuencia de comandos y respuestas que siguen los siguientes pasos: Identificación de los hosts, Identificación del remitente del mensaje, Identificación del destinatario del mensaje, Transmisión de los datos, es decir el mensaje y Transmisión de un código que indica el fin de la transacción

Los códigos de respuesta del protocolo SMTP están estructurados de un modo muy similar al FTP, pues son números decimales de tres dígitos, el primero indica el status del comando y los dos siguientes información más detallada, generalmente el 1, 2 o 3 indican la realización de un comando con éxito y los que comienzan por 4 o 5 indican algún tipo de problema.

2.5.2.2.- Funcionamiento

El protocolo SMTP se basa en la entrega punto-a-punto en la que un cliente SMTP se contactará con el servidor SMTP de destino para entregarle directamente el correo, el que se guardará hasta que se haya copiado con éxito en el receptor.

En varias implementaciones, existe la posibilidad de intercambiar correo entre los sistemas de correo locales y SMTP, dichas aplicaciones se denominan pasarelas o puentes de correo. El enviar correo a través de una pasarela puede alterar la entrega punto-a-punto, debido a que el protocolo SMTP sólo garantiza la entrega fiable a la pasarela y no al host de destino. La transmisión punto SMTP en estos casos es host-pasarela, pasarela-host o pasarela-pasarela; SMTP no define lo que ocurre más allá de la pasarela.

Cada mensaje esta compuesto por:

- Una cabecera o sobre, la cabecera termina con una línea nula, todo lo que hay tras la línea nula es el cuerpo del mensaje, que es una secuencia de líneas con caracteres ASCII.

- Contents, El cliente SMTP es el que inicia la sesión (emisor) y el servidor el que responde a la solicitud de sesión (receptor). Sin embargo, como el cliente suele actuar como servidor para un programa de correo del usuario, es más sencillo referirse a él como emisor SMTP, y al servidor como receptor SMTP.

El modelo del Simple Mail Transfer Protocol (SMTP) se puede representar gráficamente de la siguiente forma:

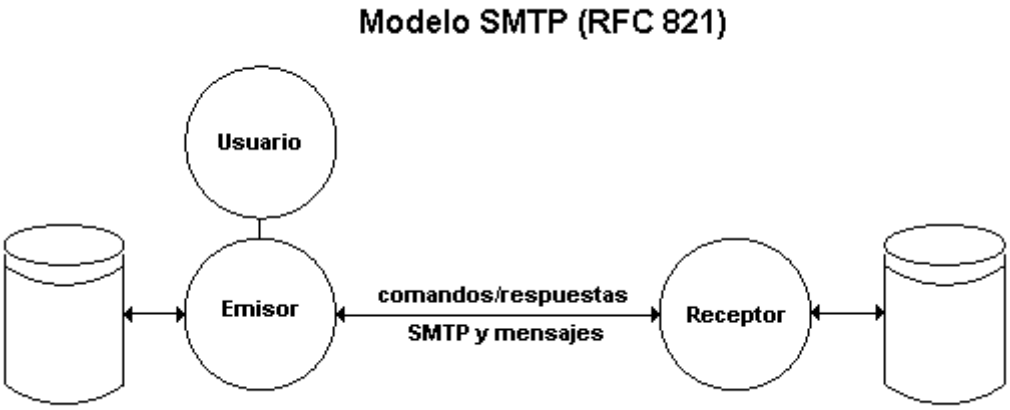

Figura 2.10

2.5.2.3.- Formato de la Cabecera

La cabecera es una sintaxis poderosa pero relativamente difícil de analizar. Los campos comienzan en la columna 1. Las líneas que comienzan con caracteres en blanco(SPACE o TAB) son de continuación que se unen para crear una sola línea para cada campo. Las cadenas entre comillas ASCII señalan que los caracteres especiales que limitan no son significativos sintácticamente.

2.5.2.4.- Intercambio de correo

Como resultado de la solicitud de correo de un usuario, el emisor SMTP establece una conexión en los dos sentidos con el receptor SMTP. El receptor puede ser el destinatario final o un intermediario éste es la pasarela de correo. El emisor generará comandos a los que replicará el receptor. El diseño de SMTP se basa en el modelo de comunicación mostrado en la siguiente figura:

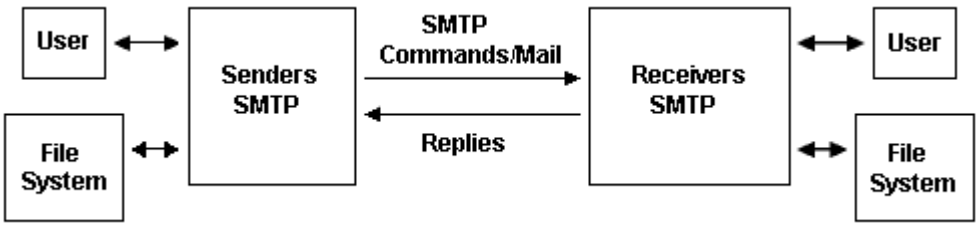

Figura 2.11

2.5.3.- SECURE MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME)

2.5.3.1.- Origen y definición

Primero aparece el protocolo MIME (Extensiones Multipropósito para Correo en Internet), en 1992 por el Internet Engineering Task Force (IETF), fue desarrollado para transmitir mensajes multimedia a través de las redes IP. Convierte en texto cualquier tipo de información y la regenera en formato original para su destino. Sin MIME no era posible crear ni leer mensajes que no fueran de texto.

S/MIME fue impulsado por la RSA Data Security, con el tiempo se convirtió en un estándar de internet. Es una extensión del estándar MIME, se utiliza para hacer seguros los mensajes y transacciones electrónicas, incluye firma digital y cifrado basado el algoritmo de clave pública RSA, además de las partes convencionales del formato MIME.

Este es el formato de intercambio de información firmada y/o cifrada a través de Internet que ha ganado gran aceptación en la mayor parte de las empresas, puesto que fue diseñado para que sea interoperable, esto es, que dos o más paquetes de software que implementen S/MIME podrán comunicarse de forma protegida.

2.5.3.2.- Estructura

Su estructura se basa en tipos de mensajes:

TIPO DE MENSAJE	SERVICIO	ALGORITMOS UTILIZADOS
Data	Datos originales	
Signed-Data	Firma digital	DSA, RSA, SHA-1,MD5
Enveloped-Data	Confidencialidad	Triple DES, RC2, Diffie-Hellman

Digested-Data	Integridad	SHA-1,MD5
Encrypted-Data	Confidencialidad	Triple DES, RC2
Authenticated-Data	Autenticación	SHA-1

Tabla 2.1

Para generar un mensaje se parte de otro con cualquiera de los tipos definidos anteriormente, se actúa sobre él añadiendo cabeceras y colas con información. La estructura del mensaje permite recursividad y paralelismo.

Recursividad, indica que cualquier tipo de mensaje puede servir como contenido de otros, y de esta forma establecer estructuras donde se unen varias firmas con encriptaciones.

Paralelismo, establece que se puede actuar sobre un contenido aplicando varias firmas. Cuando se quiera enviar un mensaje encriptado a varios usuarios se puede encriptar la clave de sesión con varias claves públicas y añadirlas al mensaje final.

2.5.3.3.- Funcionamiento

El sistema S/MIME utiliza certificados X.509, autoridades de certificación y lista de revocación de certificados lo que permite confidencialidad, autenticación e integridad y firma digital.

Confidencialidad, se la puede realizar mediante dos mensajes:

- Enveloped-data, que utiliza claves de sesión encriptadas con las claves públicas de los receptores, como se observa en el gráfico:

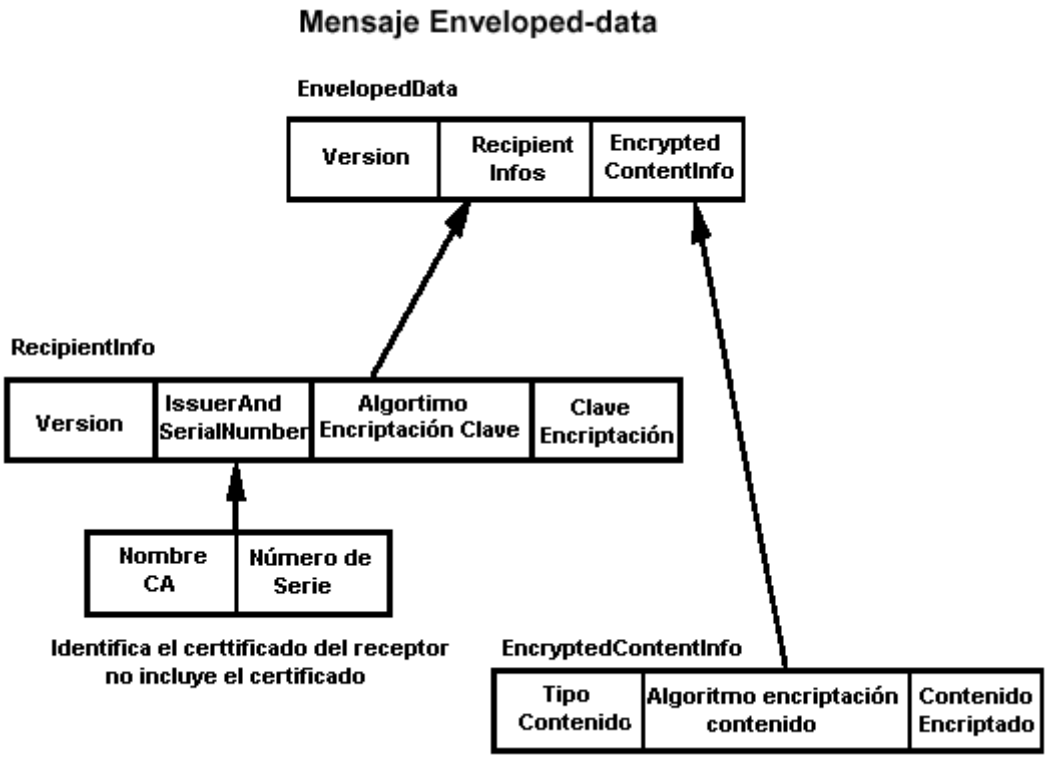

Figura 2.12

El proceso que se sigue para elaborar un mensaje Enveloped-data es:

1) Se genera una clave de sesión K_S aleatoria.

2) K_S se encripta para cada receptor, utilizando el algoritmo RSA con una clave pública, Diffie-Hellman con una clave pública y otra privada o el RC2 con una clave simétrica transmitida antes entre el receptor y emisor.

3) Se encripta el contenido con Triple DES o RC2

4) Se envía a cada receptor la clave de sesión encriptada y el contenido encriptado.

- Encrypted-data, en ésta se utiliza una clave simétrica que antes traspasó el receptor. En un mensaje Encrypted-data no se usan claves de sesión y el

contenido se encripta con una clave simétrica conocida tanto por el receptor como el emisor. Encrypted-data se muestra en el gráfico:

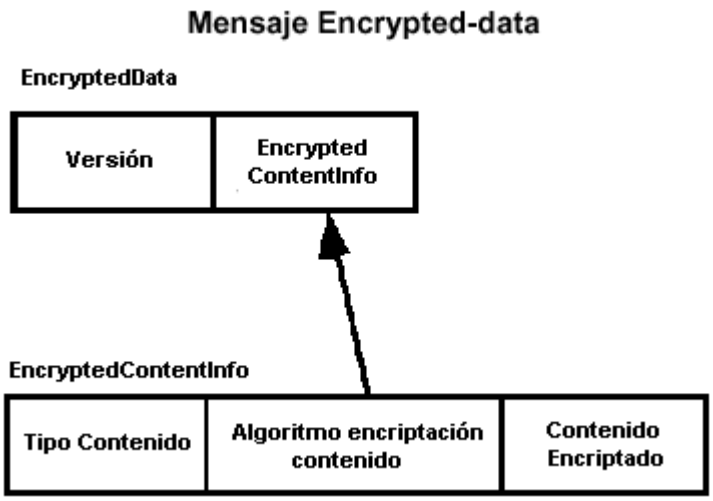

Figura 2.13

Firma Digital, se utiliza mensajes Signed-data con el siguiente proceso:

1) Primero se calcula un resumen del contenido, a través de una función hash. Para varios firmantes se calcula un resumen para cada algoritmo

2) El resumen se encripta con la clave pública de cada firmante.

3) Luego se adiciona al contenido las firmas, certificados y CRLs si fuere necesario.

Mensaje Digested-Data, éste realiza el cálculo de la función hash del contenido, comprueba la integridad y no la autenticación del correo. Gráficamente se puede observar así:

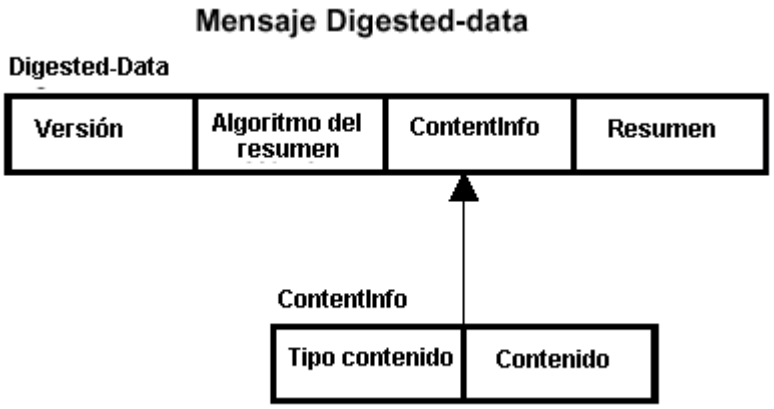

Figura 2.14

Mensaje Authenticated-Data, sirve para autenticar contenidos, las claves de sesión se generan y envían mediante el mismo sistema que enveloped-data.

2.5.4.- POST OFFICE PROTOCOL VERSIÓN 3 (POP3)

2.5.4.1.- Definición

El Post Office Protocol 3 (POP3) es la versión más reciente del protocolo estándar para recibir e-mails, éste es un protocolo cliente / servidor por el que un e-mail es recibido y administrado por el servidor de internet, sus usuarios periódicamente revisan su buzón en el servidor y los descarga. Este protocolo está incluido dentro de las aplicaciones cliente más utilizadas como el Eudora, Netscape Message y Outlook, provee extensas operaciones de manipulación de correo sobre el servidor, generalmente el correo es transmitido y luego borrado.

Un mail tipo POP3 tiene las características de:

1) Cuando un usuario pide un e-mail el servidor descarga toda la información en el disco duro de la computadora, con esto el servidor no se queda con ninguna copia del e-mail.

2) POP3 se puede configurar para que el servidor se quede con el e-mail y mande todas las copias que se solicite, se realiza esto con la finalidad de descargar el e-mail en todas las computadoras en las que se tenga configurado una cuenta.

Un servidor de POP3 puede disponer de un temporizador de inactividad o autologout inactivity timer. Este temporizador debe ser de por lo menos 10 minutos de duración. La recepción de cualquier comando desde el cliente durante este intervalo reinicia la cuenta de este temporizador. Cuando el temporizador llega a los diez minutos, la sesión no entra en el estado de actualización, entonces, el servidor debería cerrar la conexión TCP sin eliminar ningún mensaje y sin enviar ninguna respuesta al cliente.

2.5.4.2.- Comandos de POP3

Los comandos en POP3 consisten en un Keyword o palabra clave de una longitud de tres o cuatro caracteres, que puede estar seguida de uno más argumentos que llegan hasta los 40 caracteres de longitud. Las palabras clave y argumentos consisten en caracteres ASCII imprimibles separadas por un espacio. Los usuales son:

User Nombre, se autentifica con la combinación de los comandos USER y PASS, el cliente emite el comando USER, si el servidor responde afirmativamente, entonces el cliente responde con el comando PASS para completar la autentificación, o con el comando QUIT para finalizar con la conexión.

QUIT, cuando el cliente usa el comando PASS, el servidor utiliza el par de argumentos de los comandos USER y PASS para determinar si al cliente se le debe dar acceso al mail apropiado.

AUTH mecanismo, este comando hace referencia a un mecanismo de autenticación al servidor por parte del cliente. Si el servidor soporta este mecanismo, lleva a cabo el protocolo para la identificación del usuario. Si falla, la sesión permanece en el estado de autorización y el cliente puede probar con otro AUTH o bien con otro mecanismo como USER/PASS, o APOP.

UIDL [mensaje], si se da un argumento, el servidor emite una respuesta afirmativa con una línea que contiene información del mensaje. Esta línea se llama unique-id listing.

El protocolo POP3 es simple, no necesita una dirección IP fija y cualquier proveedor de Internet puede soportarlo, éstas son algunas de las ventajas que ofrece éste protocolo. Pero habría que tomar en cuenta algunas desventajas como que los mensajes con copia oculta no son enrutados en una determinada organización o si usa un buzón POP3 para cada usuario, se tiene que crear el buzón en el proveedor de Internet y en el Exchange Server(servidor de correo).

2.5.5.- INTERNET MESSAGING ACCESS PROTOCOL VERSIÓN 4(IMAP4)

2.5.5.1.- Definición

El Internet Messaging Access Protocol (IMAP), es un protocolo de correo que aporta funciones de almacenamiento y envío. Con IMAP los usuarios acceden a sus buzones desde cualquier estación de trabajo, además una gestión muy eficiente del correo, con la opción de moverse entre varios terminales y optimizar el ancho de banda en situaciones críticas. Trabaja tanto on-line como off-line.

Por las capacidades más avanzadas, se puede pensar que IMAP sería utilizado por todos, pero esto no es así ya que la sobrecarga del servidor de correo sería grande, debido a que los mensajes se mantienen en distintas carpetas. Además hace que las carpetas de correo a largo plazo de los usuarios se hagan cada vez

más grandes, con lo que se agotaría el espacio en el disco. En cambio con POP, los mensajes recuperados son eliminados del servidor de correo.

2.5.5.2.- Módulo Imaplib

En éste módulo se define una clase que encapsula la conexión a un servidor IMAP4 e implementa el protocolo del cliente IMAP4rev1. El módulo imaplib proporciona una sola clase que es:

IMAP4 ([host[, port]]), esta clase implementa el protocolo IMAP4 real. Se crea la conexión y se determina la versión del protocolo que puede ser IMAP4 o IMAP4rev1. Además si no se especifica el host, se utiliza el nodo local. Si se omite port, se utiliza el puerto IMAP4 estándar que es el 143.

Además se definen dos excepciones como atributos de la clase IMAP4 que son:

IMAP4.error, se emite esta excepción en cualquier error. El motivo para la excepción se la pasa como cadena al constructor.

IMAP4.abort, los errores del servidor IMAP4 emiten en esta excepción. Es una subclase de IMAP4.error. Cabe destacar que al cerrar la instancia o instanciar una nueva puede permitir que este estado de excepción se recupere.

IMAP4.readonly, esta excepción se emite cuando un servidor cambia el estado de un mailbox. Esta también es una subclase de IMAP4.error. Este proceso se da cuando un cliente ha obtenido permiso de escritura, por lo que habrá que volver a abrir el mailbox para retomar el permiso de escritura.

2.5.5.3.- Métodos IMAP4

Una instancia de IMAP4 cuenta con métodos, a continuación se describe algunos:

append (mailbox, flags, date_time, message), agregar el mensaje al apartado dado.

authenticate (func), orden de autentificación, requiere procesado de la respuesta y lanza una excepción.

close (), cierra el apartado actual. Se eliminan los mensajes borrados del apartado escrito, ésta orden que se recomienda hacerla antes de "LOGOUT".

copy (message_set, new_mailbox), copia los mensajes message_set al final de new_mailbox.

create (mailbox*),* crea un nuevo apartado mailbox.

delete (mailbox), elimina un apartado existente llamado mailbox*.*

list ([directory[, pattern]]), enumera los nombres de apartados del directory que concuerdan con pattern, directory es la carpeta de correo del nivel superior y pattern concuerda por omisión con cualquier cosa. Los datos devueltos contienen una lista de respuestas "LIST".

login (user, password), identifica al cliente mediante una contraseña en texto legible*.*

III. LOS ELEMENTOS INVOLUCRADOS CON LA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

3.1.- ESTUDIO DE LA CRIPTOGRAFIA DE CLAVE PÚBLICA

3.1.1.- INTRODUCCIÓN

La información tiene gran importancia en cualquier actividad, pues ésta es indispensable en la comunicación, puede tener varios niveles dependiendo del grado de valor, así, existe información confidencial en actividades militares, financieras, comerciales, etc.

Pero otro problema que surge con los sistemas informáticos es el controlar el acceso a las computadoras y recursos para evitar el uso indebido y garantizar por lo tanto la información que en ellas se encuentra almacenada. Cuando las computadoras y los sistemas están conectados a través de una red la protección se hace más necesaria y difícil de proveer.

La existencia de una red de área local con información que se tiene que proteger nos lleva a implementar sistemas de seguridad. Pero cuando estas redes están conectadas a otra gran red como es Internet el implementar la seguridad se vuelve más difícil. Con la intervención del mundo empresarial a la red, viaja por ella información confidencial que requiere de grandes medidas de seguridad. La manipulación de la información privada y los sabotajes han causado grandes pérdidas de dinero.

Los organismos interesados en este tema han propuesto una serie de soluciones para evitar ataques y operaciones ilegales, dichas soluciones proporcionan a las redes servicios de seguridad que utilizan técnicas criptográficas como herramienta base.

La criptografía ha tenido varias etapas de desarrollo. La primera se puede limitar hasta antes de la segunda guerra mundial en la que se utilizaba técnicas manuales, la segunda etapa se da al inicio de la segunda guerra mundial hasta la intervención de las computadoras en las que se utilizaba técnicas mecánicas y la

tercera etapa que utiliza técnicas con toda la tecnología que hasta hoy es conocida.

3.1.2.- LA CRIPTOGRAFÍA COMO BASE DE LA SEGURIDAD

El principal objetivo de la criptografía es brindar comunicaciones seguras sobre canales inseguros, además de permitir a dos entidades, sean personas o aplicaciones, enviarse mensajes en los que sólo los destinatarios autorizados puedan leer dichos mensajes. La criptografía es la herramienta básica que se vale de otros mecanismos más complejos para proporcionar servicios de seguridad.

Desde tiempos antiguos la criptografía se ha venido utilizando, pues los hombres han visto necesario cifrar sus mensajes para que sean enviados. La historia ha dejado ejemplos de sistemas criptográficos utilizados por personas muy importantes, pero que todos han sido fáciles de romper.

Pero con la intervención de las computadoras han hecho que aparezcan sistemas criptográficos modernos que han venido solucionando los problemas de identificación, autenticación y privacidad, con la implementación de algoritmos y estándares que fortalecen a redes especialmente a la de Internet.

En redes pequeñas la protección de la privacidad se la puede realizar utilizando un algoritmo simétrico como el AES (Advanced Encryption Standard), en lo que se requiere el intercambio de claves secretas entre cada una de las partes. Para las redes de comunicación de tamaño significativo ésta solución es impracticable e inadecuada.

Con la aparición de la criptografía de clave pública y el sistema RSA que utiliza un par combinado de claves, las grandes redes de comunicación ha encontrado una solución factible de implementar. Además con la influencia de factores que han destruido cualquier esquema criptográfico antes utilizado, debido a la

dificultad que se presentaba en relación con la complejidad – longitud de la clave y el tiempo necesario para encriptar – desencriptar los mensajes.

Los factores que han intervenido son primero, la velocidad de cálculo, especialmente con la introducción de la computadora, pues la potencia de cálculo se elevó. Además del avance de las matemáticas, con las que se pudo encontrar y definir claramente sistemas criptográficos seguros y estables. Y por último la necesidad de seguridad, debido al aparecimiento de actividades nuevas que necesitaban de la ocultación de información.

Los componentes de un sistema criptográfico o criptosistema son cinco:

1) El espacio de caracteres del texto original O.

2) El espacio de caracteres del texto cifrado C.

3) El espacio de la clave de cifrado K.

4) Una familia de transformaciones de cifrado $E_k = O \longrightarrow C$

5) Una familia de transformaciones de descifrado $D_k = C \longrightarrow O$

Cada transformación de cifrado (E_k) está definida por un algoritmo de cifrado E y la clave K que la diferencia de las demás trasformaciones. Para las transformaciones de descifrado (D_k), debe cumplirse que D_k sea inverso de E_k y por lo tanto que $D_k (E_k (M)) = M$ para cualquier texto original.

Todo sistema criptográfico debe cumplir tres requisitos básicos:

1) Las trasformaciones de cifrado y descifrado tienen que ser eficientes para cualquier clave.

2) El sistema tiene que ser fácil de usar.

3) La seguridad del sistema sólo debe depender de lo bien guardada que esté la clave, y no de lo bien preservado que se encuentre el algoritmo, que además tiene que ser público.

3.1.3.- SISTEMAS DE CLAVE PÚBLICA

3.1.3.1.- Breve reseña histórica

En 1976, dos ingenieros electrónicos de la Universidad de Stanford, Whitfield Diffie y Martin Hellman describieron el primer sistema criptográfico de clave pública conocido como “el cambio de clave Diffie-Hellman”, en éste sistema se utilizaba dos claves compuestas por un componente público y otro privado.

Ellos sugieren utilizar funciones matemáticas en lugar de sustituciones y permutaciones. Básicamente consiste en encontrar un sistema de cifrado que no sea tan difícil y que por el contrario el descifrado sea computacionalmente irresoluble, a no ser que se conozca la clave.

La primera realización del modelo propuesto por Diffie-Hellman fue desarrollado en 1978 por Ronal Rivest, Adi Shamir y Len Adleman, en aquel entonces profesores del Instituto de Tecnología de Massachusetts (M.I.T.), a ésta invención se la conoce como criptosistema RSA. La clave pública y privada están compuestas por un exponente y un módulo que es producto de dos números primos grandes.

La fiabilidad de éste sistema se basa en que si los primos se escogen lo más grandes posibles, el proceso de factorización del producto es inaccesible en un tiempo razonable, con lo que la divulgación de la clave pública no pone en peligro a la clave privada.

Para que el sistema criptográfico funcione se utiliza una función denominada de una vía o función trampa, ésta consiste en utilizar una transformación criptográfica (T_k) de fácil aplicación, de modo que sea difícil hallar su inversa sin la clave de descifrado.

En estos esquemas se utiliza una clave de cifrado o clave pública k que determina una función trampa Tk y una clave de descifrado o clave secreta que permite calcular la inversa de la función trampa Tk. Cualquier usuario puede cifrar con la clave pública, pero sólo los que tengan la clave secreta podrán descifrar correctamente el mensaje.

A partir de mediados de los años 80 se empezaron a buscar nuevos sistemas criptográficos de clave pública que utilizaran menos recursos para la generación de clave, así como para cifrar y descifrar. Así es como en el año de 1985 se propuso el Gamal, y en la primera mitad de los años 90 se introduce al estudio de los criptosistemas de curvas elípticas.

3.1.3.2.- Modo de funcionamiento

Como ya se ha explicado se basa en el uso de dos claves, generalmente la clave privada es usada por el propietario para encriptar los mensajes, mientras que la clave pública se utiliza para desencriptar el mensaje cifrado.

Las claves públicas y privadas tienen características matemáticas especiales, de forma que siempre se generan a la vez, estando cada una ligada intrínsicamente a la otra, de tal forma que si dos claves públicas son diferentes, entonces sus claves privadas también lo serán y viceversa.

Ambas claves están relacionadas matemáticamente, pero ésta relación debe ser lo suficientemente compleja para que resulte difícil obtener una partir de la otra, por tal motivo es que el usuario no las elige, sino que lo realiza un algoritmo

específico. Mientras que la clave privada se debe mantener en secreto por su dueño, ya que ésta es la base de la seguridad de este sistema.

El modo de funcionamiento es el siguiente:

1) Confidencialidad:

- Para cada usuario USR1 y USR2 se generan un par de claves, de las que una es la clave pública que se la almacena en fichero o registro público y la clave privada se la mantiene en secreto por el propietario.

- Para encriptar el mensaje se utiliza la clave pública y para desencriptar se utiliza la clave privada.

- Si el USR1 desea enviar un mensaje al USR2, encripta el mensaje con la clave pública del USR2.

- Cuando el USR2 recibe el mensaje lo desencripta con su clave privada, nadie más puede hacerlo ya que sólo dicho usuario tiene la clave privada.

- El sistema es seguro siempre y cuando cada usuario controle su clave privada, además que periódicamente se puede generar un nuevo par de claves.

2) Autenticidad:

- Para esto el USR1 prepara un mensaje para el USR2 y lo encripta con su clave privada.

- Cuando el USR2 lo recibe, lo desencripta con la clave pública del USR1. La autenticidad se fortalece con el hecho de que sólo el USR1 puede encriptar el mensaje.

- El mensaje entero encriptado sirve como una firma digital y requiere gran cantidad de almacenamiento tanto para el mensaje original sin cifrar y para el mensaje original cifrado que se lo utiliza para verificar el origen y el contenido.

- Para reducir el almacenamiento y conseguir el mismo resultado de la firma digital, se encripta un pequeño bloque de bits, que generalmente es una función hash, este bloque de bits se denomina autentificador. Para la encriptación se utiliza la clave privada del emisor por lo que se utiliza como firma digital. Con este mecanismo se garantiza la integridad y autenticidad.

Este sistema gráficamente se puede observar así:

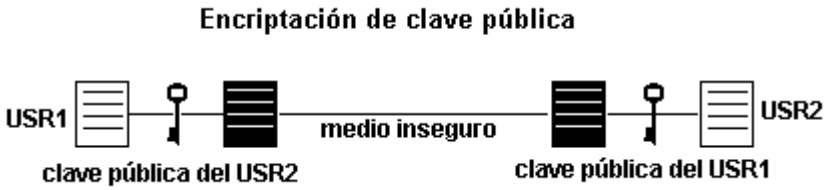

Figura 3.15

3.1.3.3.- Características de los algoritmos de clave pública.

Según Diffie y Hellman un algoritmo de clave pública debe cumplir con las siguientes características:

- Los usuarios pueden calcular sus propias claves públicas y privadas en tiempo polinomial.

- El usuario que emite el mensaje puede cifrar con la clave pública del receptor en tiempo polinomial.

- El receptor puede descifrar el sistema criptograma con la clave privada en tiempo polinomial.

- El criptoanalista que intente conocer la clave privada a través de la clave pública se encontrará con un problema que no podrá tratar.

- El criptoanalista que quiera descifrar un criptograma teniendo la clave pública también se encontrará con el mismo problema antes mencionado.

Un esquema para obtener un criptosistema de clave pública es el siguiente:

1) Escoger un problema que tenga un grado de dificultad alto.

2) Escoger un subproblema del antes mencionado y que sea fácil de resolver en tiempo polinomial.

3) Transformar el problema fácil de manera que el resultado del problema fácil sea parecido al inicial.

4) Hacer público el problema difícil y la forma de usarlo, éste sería el proceso para la clave pública de cifrado, en cambio la información de cómo recuperar el problema fácil a partir del difícil se mantendrá en secreto, éste sería el proceso que constituye la clave secreta de descifrado.

Los verdaderos usuarios que poseen la clave secreta pueden descifrar convirtiendo el problema difícil en el problema fácil, pero si un criptoanalista trata de romper este proceso se enfrentará inevitablemente al problema difícil. Con lo que se puede decir que es más dificultoso crear un sistema de clave pública seguro que un sistema de clave secreta.

3.1.3.4.- Gestión de claves

Para que un algoritmo de cifrado en un sistema de clave pública sea válido es necesario la protección de las claves y por lo tanto de procedimientos para la gestión de las mismas. La gestión de claves básicamente son técnicas para generar, almacenar, distribuir y mantener información que es almacenada y transmitida en las redes.

- Generación de claves, para generara claves el método más general sería el que proporciona claves de forma equiprobable, esto es que los algoritmos generan claves pseudoaleatorias de difícil predicción. Los procedimientos más utilizados son los generadores aleatorios de bits, por desplazamiento de registros o mediante algoritmos matemáticos.

- Almacenamiento de claves, en los sistemas de clave publica, como ya se mencionó, tienen un par de claves para cada usuario, la privada que debe ser secreta, la pública que debe ser accesible para todo el mundo y por lo tanto es que debe encontrarse en un lugar en donde exista mayor acceso posible. Pero surge el inconveniente que es el que una clave pública pertenezca a quién dice ser, esto se soluciona con una entidad certificadora que almacena las claves públicas y se comporta como un notario que asegura la identidad de los dueños de la clave pública.

- Distribución de claves, en los sistemas de clave pública el emisor tiene una clave privada secreta y la pública que la envía a la autoridad certificadora, entonces la autoridad determina por un procedimiento la identificación personal, en este proceso se crea la firma digital que hace que la clave pública del emisor sea auténtica.

- Mantenimiento de claves, es el cambio periódico de claves y las acciones que se deben hacer cuando son robadas. El cambio de claves se lo debe realizar con cierta frecuencia y dar a conocer el cambio a la autoridad certificadora para que valide la nueva clave pública. La pérdida, revelación o robo de claves se debe comunicar inmediatamente a la entidad

certificadora que hará no válida la clave pública, con lo que se procederá a crear un nuevo par de claves.

3.1.4.- ALGORITMOS UTILIZADOS EN SISTEMAS DE CLAVE PÚBLICA

3.1.4.1.- Algoritmo Diffie-Hellman

Este algoritmo fue propuesto por Whitfield Diffie y Martin Hellman, el mismo que fue una verdadera revolución en el mundo de la criptografía, ya que este fue la pauta para el desarrollo de los sistemas asimétricos, se lo dio a conocer en el artículo “New Directions in Cryptography”.

Este algoritmo es importante debido a que es el inicio de los sistemas asimétricos, ya que en la práctica es válido sólo para el intercambio de claves simétricas y con ésta funcionalidad se lo utiliza en sistemas seguros para Internet como es el caso de SSL (Secure Socket Layer) y VPN (Virtual Private Network).

Funcionamiento

Matemáticamente se basa en las potencias de números y la función mod (módulo discreto), con estos conceptos se define a la potencia discreta de un número como: $Y = X^a \bmod q$. Sin bien es cierto que el cálculo es fácil, la obtención de su inversa, el logaritmo discreto, no tiene una solución analítica para números grandes. El procedimiento es el siguiente:

1) Se busca un número primo muy grande q.

2) Se obtiene un número B, raíz primitiva de q, esto quiere decir que cumple con:

$B \bmod q, B^2 \bmod q, \ldots, B^{q-1} \bmod q$ son números diferentes.

3) B y q son claves públicas.

4) Para generar una clave simétrica compartida entre dos usuarios A y B, los dos parten de un generador de números pseudoaleatorios, estos números X_a , X_b son diferentes uno de otro y son las claves privadas de A y B.

5) Con estos números (Xa, Xb) y las claves públicas (B y q) que ambos conocen, cada uno genera un número intermedio Y_a , Y_b con las siguientes fórmulas:

$$Y_a = B^{Xa} \bmod q$$
$$Y_b = B^{Xb} \bmod q$$

6) Estos números son intercambiados entre los dos y después cada uno opera con el que recibe obteniendo:

$$K = Y_b^{Xa} \bmod q$$
$$K = Y_a^{Xb} \bmod q$$

El número K es la clave simétrica que a partir de ese momento ambos comparten y poder establecer una comunicación cifrada.

3.1.4.2.- Algoritmo RSA (Rivest-Shamir-Adleman)

Este algoritmo fue desarrollado en 1978 por Ronal Rivest, Adi Shamir y Len Adleman se basaron en el artículo de Diffie-Hellman sobre sistemas de llave pública, con el que el algoritmo y fundaron la empresa RSA Data Security Inc., que es actualmente una de las más prestigiosas en el mundo la seguridad de los datos.

El algoritmo RSA se basa en la dificultad matemática de factorizar números muy grandes. Generalmente para factorizar un número se empieza a dividir sucesivamente para 2, 3, 4, ...n, buscando que el resultado de la división sea exacto, esto es que tenga de residuo 0, con este proceso se encontrará el divisor del número.

Si se continúa con el proceso al decir que si el número antes encontrado es un número primo, el que es divisible para sí mismo y la unidad, se tendrá que para factorizar se empezará por 1, 2, 3, 4, ... hasta llegar al número, y si es que el número primo es bastantemente grande el procedimiento para factorizarlo es complejo y por lo tanto llevará mucho tiempo.

Funcionamiento

1) Cada usuario (U) elige dos números primos (p, q), que estén entre 100 y 300 dígitos. Luego se calcula n conocida como módulo, con n = p * q. Entonces el grupo a usar por el usuario U es Z^*_n. El orden de este grupo es:

$$\varphi(n) = \varphi(p*q) = (p-1)(q-1)$$

2) Después el usuario U selecciona un entero positivo (e) definido por:

$$1 \leq e < \varphi(n)$$

de tal forma que sea primo con el orden del grupo.

3) El usuario U calcula el inverso (d) del entero positivo (e), esto quiere decir (e^{-1}) en $Z_{\varphi(n)}$, entonces:

$$e*d \equiv 1 (\text{mod } \varphi(n)); \text{ con } 1 \leq d < \varphi(n)$$

4) La clave pública del usuario U es la pareja (n, e), mientras que la clave privada es el número d, los números p, q y $\varphi(n)$ se destruyen y lo que se hace público es el entero positivo e, necesario para alimentar el algoritmo.

Si un usuario A desea enviar un mensaje m de Z_n a un usuario B, utiliza la clave pública de B (n_b, e_b) para calcular el valor de $m^{e}{}_{b} (\text{mod } n_b)$ = se envía a B. Para recuperar el mensaje original B calcula $c^{d}{}_{b} = (m^{e}{}_{b})^{d}{}_{b} = m^{e}{}_{b}{}^{d}{}_{b} \equiv m (\text{mod } n_b)$.

Cuando las claves se generan dentro de una computadora, es conveniente que la clave privada se proteja mediante un algoritmo criptográfico simétrico. En lo que

se refiere a las longitudes de la clave, el algoritmo RSA permite longitudes variables que sean no menos de 1024 bits.

El algoritmo RSA es el más utilizado en los sistemas de clave pública, debido a que presenta varias ventajas incluyendo firma digital

Características

- Existen mensajes no cifrables cuando $m^e = m \pmod n$.

- Generalmente el e puede ser el 3 o $2^{16} + 1$ que son números primos.

- Los algoritmos de clave simétrica son 100 veces más rápidos que el RSA y cuando es implementado en chip es de 1000 a 10000 más rápido.

- Se utiliza mucho el denominado envoltorio digital, que es un mecanismo que aprovecha la criptografía de clave secreta y pública, de tal forma que el mensaje se cifra mediante un algoritmo simétrico (AES) para el que se utiliza una clave temporal y luego se cifra asimétricamente con la clave pública. Con éste envoltorio el usuario A encripta el mensaje m con un criptosistema simétrico con la ayuda de la clave aleatoria, luego dicha clave se encripta con RSA. Para recuperar el mensaje, el usuario B desencripta la clave de AES a través de la clave privada de RSA con la clave obtenida se desencripta el mensaje m.

- Para quebrantar RSA se necesita saber $\varphi(n)$ del que se puede deducir d y sabiendo n no es fácil determinar $\varphi(n)$ debido a que $n = p * q$ y no se conoce ni p ni q.

- Como ya se mencionó p y q no tienen que ser revelados, esto implica que p y q sólo deben diferir en pocos dígitos, aunque no tienen que ser tan

cercanos. Además (p-1)(q-1) deben contener factores primos grandes. El numero e debe ser pequeño y algo importante es que p y q sean primos.

Técnicas para romper al RSA

Las técnicas usadas para inutilizar un algoritmo RSA son dos:

1) Fuerza bruta, consiste en probar todas las claves privadas posibles, que en la actualidad es realmente imposible debido al gran tamaño de las claves, ya que los números originales son de por lo menos 1024 bits.

2) Factorizar $\varphi(n)$ en un número primo con esto se obtendría $\varphi(n)$ y e. pero ésta tarea es actualmente imposible de realizar en un tiempo razonable para las claves mayores de 1024 bits.

3.1.4.3.- El Gamal

Es un algoritmo criptográfico patentado hasta el año de 1997, este fue el primer algoritmo de uso libre. Como se conoce, un algoritmo de clave pública es difícil de romper mediante la técnica de fuerza bruta, es decir, probar todas las claves posibles, así es como el Gamal basa su seguridad en la dificultad de calcular logaritmos discretos en un campo finito.

Funcionamiento

Fijado un cuerpo finito GF(p) y un elemento α, además los mensajes originales que se quieren cifrar corresponde a m, y este pertenece a GF(p).

Cada usuario U escoge un entero $r_{u\in}$ [2,p-1] que formará la clave secreta, la clave pública será el elemento $\alpha^{ru} \in$ GF(p). Si un usuario A desea transmitir el mensaje cifrado, que corresponda al mensaje original m $\in$ GF(p), al usuario B tendrá que las siguientes operaciones en GF(p):

1) Escoger un entero k al azar y calcular α^k.

2) Cifrar m como:

$$c = E\, d^B (m) = m * (d^B)^k$$

3) Transmitir el par (d^k, c), con esto el usuario podrá recuperar m a partir del par recibido con las siguientes operaciones en GF(p):

4) Calcular $\beta = (d^k)^{rB}$

5) Calcular c/β en que el resultado será m.

El que desee calcular $(d^k)^{rB}$ teniendo conocimiento de α^k y $^{\alpha rB}$, pero sin saber r_B tendrá que calcular logaritmo discreto $\log \alpha_{\alpha}{}^{rB}$.

Entre las desventajas del algoritmo el Gamal están que es muy lento debido a que cuando se escoge un número aleatorio para cada bloque de cifrado. Además el texto cifrado es de doble tamaño que el texto original. El tamaño del espacio de las claves ha de ser grande para evitar escoger el mismo valor en varios bloques, pues no se aconseja usar la misma clave en más de un bloque.

3.1.4.4.- Sistemas basados en curvas elípticas

En el año de 1985 se encontró que el sistema de curvas elípticas se podría aplicar a la criptografía. La razón principal por que se pensó en esto es que las curvas elípticas definidas sobre cuerpos finitos proporcionan grupos finitos abelianos, en donde los cálculos se realizan con la eficiencia que requiere un sistema criptográfico, además el cálculo de logaritmos se vuelve más fácil en dichos grupos que en los cuerpos finitos.

Otra ventaja es que existe mayor facilidad para escoger una curva elíptica que para encontrar un cuerpo finito, lo que le hace más conveniente que el algoritmo el Gamal.

Funcionamiento

1) Básicamente en este sistema se utiliza el logaritmo discreto elíptico. Por lo tanto se dice que la ecuación de una curva elíptica se expresa:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

en donde las constantes a, b, c, d, e pertenecen a un cierto conjunto llamado campo F, que en el caso de la criptografía es un campo primo (Zp), o un campo de característica 2, esto es que los elementos están formados de ceros y unos.

2) Se determina un punto racional, que es el que satisface la ecuación antes descrita. Si el campo es finito, por lo tanto el conjunto de puntos (x,y) que satisfacen la ecuación también lo es, y se lo denomina conjunto de puntos racionales de la curva E sobre e campo F. El conjunto de puntos racionales se lo puede expresar como:

$$E: O, P_1, P_2, P_3, \ldots, P_n$$

En donde E representa la ecuación, O es el punto al infinito que no tiene coordenadas. El conjunto de puntos puede sumarse y tener las mismas propiedades de los números enteros, este el grupo abeliano.

3) La explicación geométrica de la suma de dichos punto es que si la gráfica representa a todos los puntos que satisfagan la ecuación de la curva elíptica y si se quiere sumar los puntos P y Q, se traza una línea recta que pase por P y Q. La ecuación de la curva es de grado 3 y la de la línea es de grado 1, por lo que

siempre existirán tres soluciones. Gráficamente los puntos se pueden describir en la siguiente figura:

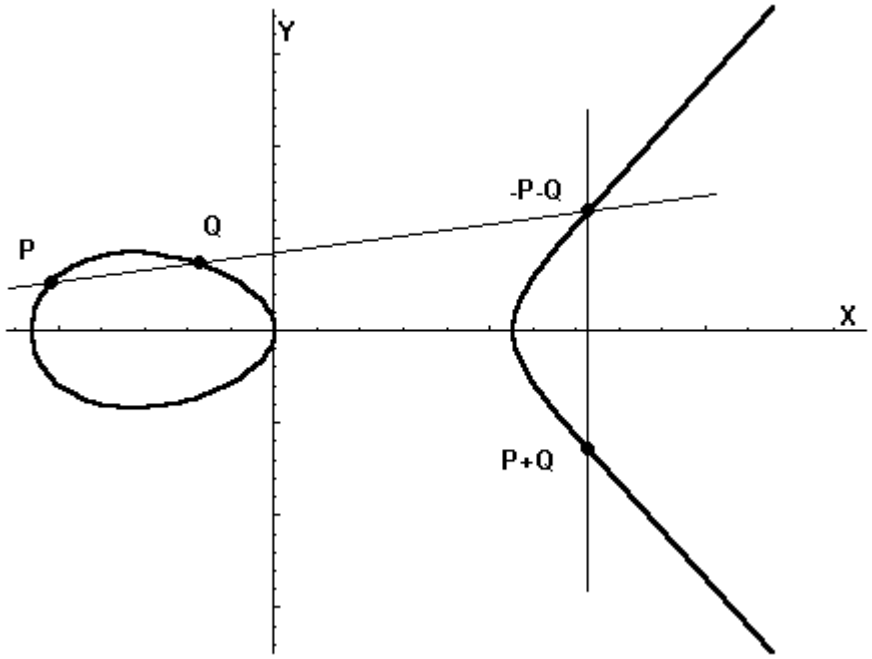

Figura 3.16

4) Para calcular las coordenadas del punto P+Q, se lo hace mediante las coordenadas del punto P y del Q. Si el campo de definición de la curva es un campo primo Zp las fórmulas son:

$$X_3 = \lambda 2 - X_1 - X_2$$

$$Y_3 = \lambda (X_1 - X_3) - Y_1$$

$$\lambda \begin{cases} \dfrac{Y_2 - Y_1}{X_2 - X_1} & P \neq Q \\ \dfrac{3X_1^2 + a}{2Y_1} & P = Q \end{cases}$$

5) Los sistemas basados en curvas elípticas fundamentan su seguridad en el Problema del Logaritmo Discreto Elíptico, esto es, que dados los puntos P y Q habría que encontrar un número entero x, tal que

$$xP = Q \ (xP = P + P + ... + P, \text{ x veces})$$

Características

La invención de un protocolo con criptografía de curvas elípticas requiere primero una alta seguridad y una buena implementación para la elección de una curva adecuada, es decir que no sea supersingular y el orden del grupo de puntos racionales tenga un factor primo de por lo menos 163 bits. Es importante también que si el campo Zp la curva no sea anómala, esto es, que no tenga p puntos racionales para evitar ataques conocidos.

En cuanto a la implementación es importante tener buenos programas que realicen la aritmética del campo finito, además contar con excelentes algoritmos que sumen los puntos racionales. La principal ventaja de este sistema ante el RSA es la longitud de la clave secreta pues sólo se necesitan 163 bits para ofrecer la misma seguridad del RSA.

Los elementos de los puntos racionales de este sistema pueden ser de característica 2, es decir arreglos de unos y ceros de longitud fija, con lo que se puede hacer una aritmética que optimice la rapidez y realizarle un circuito especial, a esto se lo denomina Base Normal Optima.

Este sistema es óptimo implementarlo el poder de cálculo y el espacio del circuito sea pequeño, en donde la memoria o el ancho de banda sea limitado, es decir nos permite utilizar smart cards, teléfonos celulares, fax, palms, etc.

3.1.4.5.- Sistema Probabilístico

El sistema probabilístico fue ideado por Golwaser y Micali y su propósito es cifrar mensajes de manera que no exista cálculo factible que proporcione información del texto original correspondiente. La criptografía de clave pública soluciona el problema de la distribución de claves, sin embargo presenta otro inconveniente que es el texto cifrado dado por: c = E (m), en la mayoría de los casos puede dar información sobre el texto original.

Esto puede suceder porque el criptoanalista tiene el conocimiento del algoritmo (E) que cifró al texto original o por lo puede calcular con la clave pública sobre algún texto. Cualquiera fuere el método para recuperar el mensaje (m) a partir de c, no se puede determinar la medida de información que se dejó escapar del mensaje original (m).

Cuando se introduce el sistema probabilístico se hace notar la diferencia con los cifrados de clave pública es que los algoritmos son más probabilísticos que determinístícos, esto es, el texto original puede dar lugar a varios textos cifrados, es por ésta razón que un criptoanalista no podrá verificar un algoritmo deducido por él, cifrando el texto original y comparándolo con el criptograma interceptado.

Funcionamiento

1) El sistema está formado por un conjunto de claves K, $k \in K$, un conjunto de mensajes en con texto original Mk, un conjunto de mensajes cifrados Ck, un conjunto de elementos de aleatorización Rk y las funciones definidas por:

$$Ek : Mk * Rk \longrightarrow Ck \qquad y \qquad Dk : Ck \longrightarrow Mk$$

en que Dk (Ek (m.r)) = m para cualquier mensaje con texto original Mk y $r \in Rk$

2) A partir de k tiene que ser fácil crear algoritmos eficientes para el cálculo de Ek y Dk, sin embargo tiene que ser considerablemente difícil diseñar un algoritmo eficiente para el cálculo de Dk con sólo conocer el algoritmo para calcular Ek.

3) Un sistema probabilístico cada usuario selecciona una clave y la utiliza para obtener Ek y Dk, para el primero el algoritmo se hace público y Dk se guarda en secreto.

En el sistema de cifrado probabilístico cuando un usuario desea enviar un mensaje (m), éste usuario tendrá que buscar Ek en un directorio público donde se encuentran alojadas las Ek de otros usuarios, luego aleatoriamente seleccionar r $\in$ Rk y calcular el texto cifrado con c = Ek (m, r).

3.1.4.6.- Diferencias entre algoritmos simétricos y de clave pública o asimétricos.

La principal diferencia entre estos algoritmos es que para un asimétrico existen mayores restricciones para el diseño, debido a que la clave pública representa información adicional que puede ser perjudicial en el caso de que se quiera hacer criptoanálisis.

En un algoritmo de clave pública la seguridad está basada en la dificultad de resolver un problema matemático conocido, en cambio un algoritmo simétrico está diseñado de tal manera que las ecuaciones matemáticas que utiliza son muy complejas que no son resolubles analíticamente.

Otra muy marcada diferencia es en la generación de claves, es así que en un algoritmo asimétrico la clave de cifrado y descifrado no es pública, en cambio en los algoritmos simétricos la clave de cifrado equivale a la de descifrado y viceversa. Además hay que notar que en un algoritmo de clave pública se hace necesario un proceso para calcular la clave pública basándose en la privada, de tal forma que sea computacionalmente eficiente, además que el cálculo inverso no sea posible de realizar.

3.2.- FIRMA DIGITAL

3.2.1.- INTRODUCCIÓN

La tecnología de la encriptación es el factor más importante dentro de la seguridad en el ciberespacio, pues se observa que todas las propuestas para trasmisión de datos, certificados digitales y estándares para los sitios web involucran el encriptado.

En el mundo de las redes como es Internet el procedimiento de obtener firmas así como las que se realizan en papel es una necesidad imperiosa para permitir la autorización de pagos on-line y para atestiguar la identidad.

Las firmas digitales son la mayor ventaja dentro de la seguridad, son utilizadas para firmar documentos digitales, para certificar códigos de aplicación y componentes, configurar topologías de redes públicas seguras y por supuesto encriptar datos.

Las firmas digitales son creadas y verificadas utilizando la criptografía, además de otros procesos como la denominada función hash, con dicha función es computacionalmente imposible que conociendo el valor de hash del mensaje pueda encontrarse el mensaje original.

El comercio electrónico no es el único campo que se favorece de la firma digital, pues, en la actualidad organizaciones públicas y privadas del país y del mundo tienen grandes cantidades de documentos en papel que ocupan gran parte del espacio de las oficinas lo que hace que la información sea lenta y costosa. Lo que les hace pensar el futuro y con la ayuda de las nuevas tecnologías de información y comunicación implementar esquemas que vayan de acuerdo a la web.

El Ecuador ha reconocido la firma digital al aprobar la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que dan el soporte legal y

confiable para la implantación de sistemas informáticos que requieran de este tipo de tecnología. Actualmente por Internet a diario se envían y reciben documentos con información confidencial, que necesitan ser firmados para evitar que la información sea modificada o no llegue a su destino.

3.2.2.- FUNCIÓN HASH

3.2.2.1.- Definición

A una función hash se define como una función computable de transformación, que como entrada es una cadena x de bits de longitud variable y como salida produce una cadena h de bits de longitud fija (h = H(x)). La entrada x puede tener una longitud de 1Mb, mientras que h se puede reducir a 64 o 128 bits.

Una función hash unidireccional es una función H de modo que para cualquier mensaje m' es muy difícil encontrar un mensaje m de modo que m' = H(m), en que H(m) es de tamaño fijo. Si una función hash es unidireccional, esto es que se hace difícil de invertir, a ésta se la denomina función resumen.

Para que una función hash pueda utilizarse con propósitos criptográficos debe cumplir con lo siguiente:

- La entrada puede tener cualquier longitud, con lo que se debe tomar en cuenta el desbordamiento u overflow.

- La salida debe ser de longitud fija, ésta es independiente de la longitud de la entrada.

- Para cualquier entrada su valor hash o resumen debe ser fácil de calcular.

- La función resumen o hash deber ser en un único sentido y ésta dada por f(x) y debe ser computacionalmente difícil de encontrar un valor y, tal que f(y) = f(x).

- Es difícil encontrar dos entradas x, y tales que H(x) = H(y)

3.2.2.2.- Características de la función hash

La función hash se utiliza para comprimir un texto en un bloque de longitud fija, se la usa en autenticación y firma digital en lo siguiente:

1) No necesita encriptar todo el texto para la autenticación y firma digital, puesto que este proceso es lento con los algoritmos asimétricos. La función resumen se la utiliza para comprobar si la clave privada del emisor es auténtica, no se hace necesario encriptar todo el texto si no se desea Confidencialidad. El siguiente gráfico muestra el proceso:

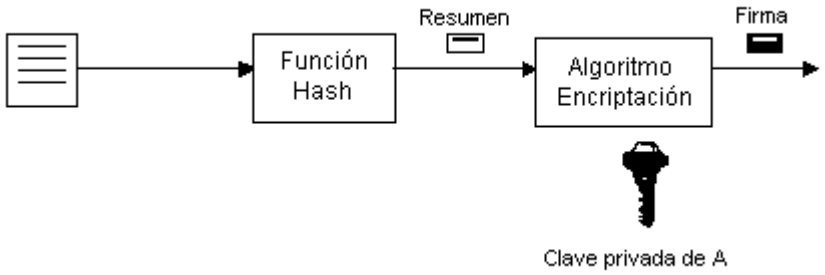

Figura 3.17

2) Si se encripta todo el texto cuando se quiera desencriptarlo y comprobar su autenticidad sólo se deberá observar si el resultado es inteligible, este es un proceso manual. Cuando se utiliza la función resumen para comprobar si es auténtico se compara el resumen del receptor con el desencriptado.

3) Si se quiere comprobar la integridad del texto se deberá comparar el resumen del texto recibido con la desencriptación.

Las funciones hash son públicas e irreversibles, no encriptan sólo comprimen los bloques de longitud fija. Tienen gran diferencia con las funciones comunes de compresión de textos como el Zip, Huffman, etc. ya que estas son funciones reversibles y eliminan la redundancia de los textos conservando su significado.

3.2.2.3.- Funciones hash más utilizadas

1) Message Digest (MD), son funciones resumen que se usan en criptografía, diseñados por Ron Rivest. Básicamente funciona con la generación de huellas digitales de documentos, mensajes de correo electrónico y similares. Los más conocidos son MD4 y MD5.

MD4 fue presentada en 1990 es una función muy rápida, genera una huella de 128 bits y divide el mensaje en cuatro bloques y hace cuatro vueltas con operaciones AND, OR o NOT. Pero en 1995 se demostró que es posible hallar colisiones con MD4 en menos de un minuto con una computadora común, con lo que ya no se considera seguro.

MD5 es una versión mejorada del MD4, aunque MD5 es más lenta. Se lo desarrolló en 1991 por el mismo Rivest, según su autor es fuerte por la longitud de salida que es de 128 bits, con lo que la probabilidad de obtener dos mensajes con el mismo resumen es de 2^{64} y la dificultad de obtener un mensaje cuyo resumen es de 2^{128}.

Estos algoritmos son de dominio público. El MD5 es considerado bastante seguro pero es recomendable actualizarse con algoritmos más modernos.

2) Secure Hash Algorithm (SHA), desarrollado en 1994 por el National Institute for Standards and Technology (NIST) conjuntamente con el National Security Agency (NSA). Se lo utiliza en firma digital, tiene una longitud de bloque de 160 bits con 200 operaciones y se necesita de un permiso especial para utilizarlo.

SHA-1, es una revisión del anterior y su funcionamiento es similar al MD5, de entrada utiliza mensajes de menos de 2^{64} bits y genera salidas de 160 bits, más largas que las producidas por cualquier otra función resumen. Es un algoritmo ligeramente más lento que MD5, pero mientras de más longitud sea el resumen es más seguro frente a colisiones usando la fuerza bruta, es decir probando todas las combinaciones posibles.

3.2.3.- FIRMA DIGITAL

La firma digital en cuanto se refiere a la seguridad informática, es el resultado de aplicar técnicas criptográficas específicas a una determinada información, para que simule con la misma validez de la firma manuscrita.

Una firma digital permite identificar a una persona en el ciberespacio, proporcionar certeza en cuanto a su participación en un proceso que requiera de dicha firma, así como vincular a una persona con un documento digital.

A la firma se la puede distinguir de la implícita, es decir contenida del texto, con la explícita que se la añade al texto como una marca inseparable, y la privada que es legible para aquel que comparte un secreto con el emisor, de la pública que es legible para todo el mundo.

La idea principal de la firma digital es que sólo el emisor la pueda generar, además demostrar que sólo él, es quién efectivamente la pudo producir. Se basa en la criptografía de clave pública, en la que la información es encriptada con una clave y desencriptada con la otra.

Características

- La firma digital es única y la genera un usuario legítimo.

- No puede ser falsificada, ya que el sólo intentarlo llevaría a una resolución de problema numérico que no podrá ser tratado.

- Es de fácil autenticación, pues el receptor podrá establecer su autenticidad después de pasado algún tiempo.

- La firma digital es irrevocable, ya que el autor de la firma no podrá negar su autoría.

- Es sencilla de generar, se lo hace a través de la clave pública y puede ser verificada por cualquier persona que conozca la clave pública.

- Las firmas digitales deben depender tanto del mensaje como del autor.

- Con las firmas se puede asegurar la integridad y no repudio de los documentos firmados.

3.2.4.- PROCESO DE GENERACIÓN

1) Primero se genera un resumen o hash con los algoritmos MD5 o SHA-1

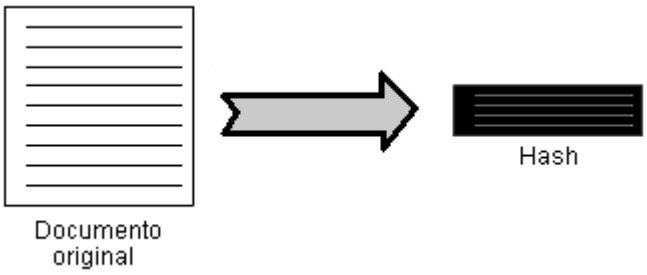

Figura 3.18

2) Luego se cifra el resumen o hash con la clave privada. Dicha encriptación se realiza con algoritmos asimétricos como RSA y se transmite el original y la firma.

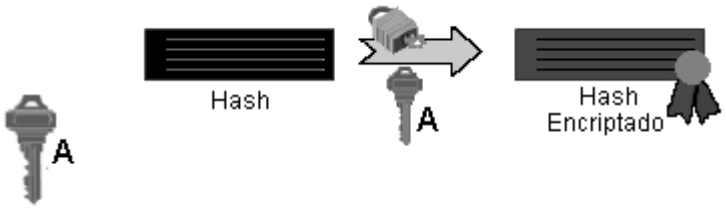

Figura 3.19

3.2.4.1.- Generación de la firma digital con RSA.

En el criptosistema RSA básicamente cuando un usuario A desea enviar la firma digital del mensaje m, con la clave pública (n_a, e_a) y la clave privada d_a, tiene que realizarse los siguientes pasos:

- Se obtiene el resumen H(m) del mensaje m.
- El usuario A encripta H(m) con su clave privada d_a, con lo que se obtiene una rúbrica de modo que $f = (H(m))^{da} \pmod{n_a}$.
- El usuario B podrá descifrar dicha rúbrica con: $f^{ea} \bmod (n_a) = h(m)$.

3.2.4.2.- Generación de la firma digital con El Gamal

El proceso para la generar la firma con el algoritmo el Gamal es con los siguientes pasos:

- El usuario A genera un número aleatorio h, de modo que sea primo con el orden del grupo (h, p-1) = 1.
- Luego el mismo usuario calcula el elemento $r \equiv \alpha h \pmod{p}$.
- El usuario A resuelve la congruencia $m \equiv a * r + h * s \pmod{p-1}$

Con lo que resulta la firma digital del usuario A para el mensaje m y es el par (r,s). Hay que recalcar que no interviene una función resumen o hash. Para que el receptor del mensaje compruebe la firma digital de A debe proceder de la siguiente manera:

- El usuario B calcula $r^s \equiv (\alpha^h)^s \pmod p$ y $(\alpha^a)^r \pmod p$.

- El usuario B tiene que calcular también $(\alpha^a)^r (\alpha^h)^s \pmod p$ y se comprueba que es igual a $\alpha^m \pmod p$.

3.2.5.- ATRIBUTOS DE LA FIRMA DIGITAL

En algunas sociedades se siguen utilizando documentos en papel pero sólo por satisfacer exigencias reconocidas legalmente, aunque la información que se almacena en una computadora puede ser o tener la misma legalidad que tiene su contraparte en papel.

Aunque las transacciones no han cambiado las leyes y las sociedades se han adaptado a los avances de la tecnología para superar los efectos esperados por las formas en papel. La firma digital ha contribuido con en el avance en el campo del comercio electrónico, infraestructura de clave pública, etc.

Una firma digital tiene los siguientes atributos:

- Autenticación del firmante, este indica quién firma el documento, con lo que se hace imposible que otra persona pueda falsificarla sin autorización.

- Autenticación del documento, con esto se puede identificar que está firmado y no se pueda alterar o falsificar. Los dos atributos antes mencionados son generalmente llamados Servicio de no Repudio.

- Acto afirmativo, sirve como función de aprobación de la firma y establece la seguridad de tener una transacción legalmente ejecutada.

- Eficiencia, en el sentido que se puede asegurar la autenticidad del firmante y del documento con la utilización muy baja de recursos.

La firma digital hoy en día resulta más fuerte que la firma manuscrita porque además de autenticar la firmante protege el contenido del documento, debido a que la firma se construye a partir de la clave privada del emisor y que sirve como una garantía de integridad del mensaje, sin embargo algunas organizaciones requieren de la presencia física para proporcionar una credencial de firma digital.

3.3.- CERTIFICADOS DIGITALES

3.3.1.- DEFINICIÓN

Un certificado digital es un documento emitido y firmado digitalmente por una autoridad certificadora (Certification Authority, CA), que acredita que una clave pública corresponde a una persona o entidad determinada y que es válida durante un período de tiempo.

Son documentos digitales utilizados para verificar la autenticidad de la clave pública de un usuario o entidad dueño de un certificado, con lo que se proporciona las más altas garantías de seguridad. Por lo tanto es realmente necesario estar seguros de que una clave pública que maneje una persona para firmar o cifrar un texto pertenezca a quien dice corresponder.

Sería desastroso manejar una clave pública de una persona que se hace pasar por otra y sin poderlo descubrir a tiempo, ya que se podría tomar una firma como válida sin serlo y tratar con una persona que realmente no lo es.

Un certificado digital no puede falsificarse siempre que esté firmado por una Autoridad Certificadora confiable, cuando un dato de la firma es modificado el correspondiente resumen o hash que se obtendría de dicha modificación no sería igual a la firma original y por lo tanto el software que gestiona esto emitiría un mensaje de error, invalidando la firma.

Gráficamente la forma en que un usuario A debería mantener sus claves es como se muestra a continuación:

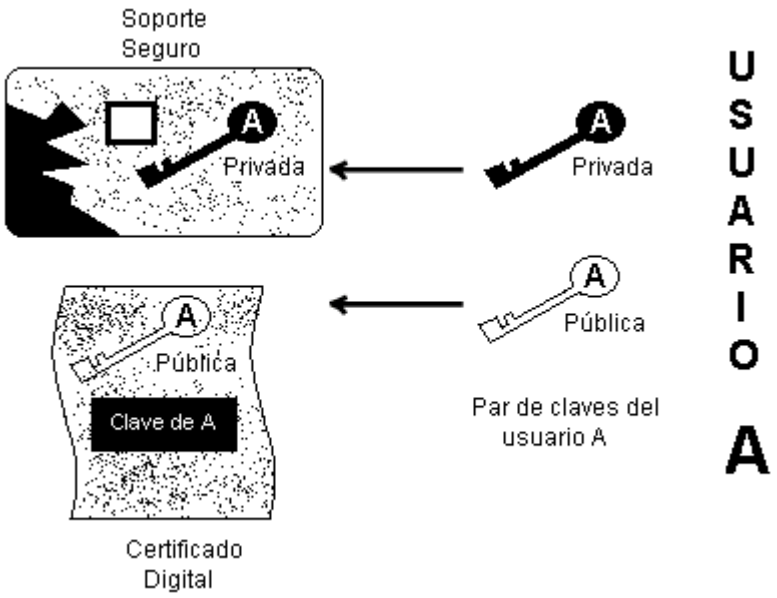

Figura 3.20

3.3.2.- CARACTERÍSTICAS

Un certificado digital contiene una clave pública y una firma digital, dicha firma en un certificado es su identidad electrónica que antes fue autentificada y registrada por una Autoridad de Registro, que es quien asegura a los destinatarios que los mensajes que provienen de quienes dicen ser realmente lo son y no han sido falsificados ni manipulados por alguien ajeno a este proceso.

Para que los certificados funcionen correctamente y cumplan con sus objetivos deberán contener la siguiente información:

- Un identificador del propietario del certificado, el que consta del nombre, apellidos, dirección e-mail, datos de la empresa a la que pertenece como nombre, localidad, país, provincia, etc.

- Un identificador de quién asegura la validez, es decir de una Certification Authority o CA (Autoridad de Certificación).

- Una fecha de inicio y otra de fin del período de validez del certificado, esto quiere decir cuándo un certificado empieza a ser válido y hasta cuando lo podrá ser, ésta es la fecha donde la clave pública no se podrá utilizar para firmar o cifrar.

- Un identificador del certificado, que es el número de serie único para cada certificado emitido por la Certification Authority o CA (Autoridad de Certificación).

- Una firma de la Autoridad de Certificación, ésta es la que asegura la autenticidad del certificado.

Existen varios formatos para un certificado, pero el más difundido es el X.509 v3, estos certificados permiten intercambiar información entre usuarios de forma segura. Generalmente los certificados son almacenados en un directorio, luego dichos certificados serán publicados y podrán ser consultados por otros usuarios que quieran enviar información cifrada o verificar firmas digitales.

El Ecuador cuenta con el marco legal necesario para manejar los certificados digitales aunque no están muy difundidos en el medio, pues la falta de una autoridad certificadora que promueva sus servicios hace que los usuarios no utilicen ésta tecnología.

En mundo existen varias Autoridades de Certificación que proveen certificados y muchas de las cuales lo hacen a través de una página web o por un software que

es proporcionado para generar las claves. Luego una Autoridad de Registro verificará la identidad de la persona solicitante mediante documentos. Asimismo se le puede otorgar un certificado a un servidor.

3.3.3.- TIPOS DE CERTIFICADOS

Dependiendo del uso, persona o entidad que solicite el certificado, se han divido a los certificados en varios tipos que se detallan a continuación:

1) Certificados Clase 1, son los certificados más fáciles de obtener, debido a que conllevan pocas verificaciones de datos, dichos datos son nombre y dirección de correo electrónico del solicitante.

2) Certificados Clase 2, en estos certificados la Autoridad Certificadora datos como licencia de conducir, fecha de nacimiento, numero de seguro social.

3) Certificados Clase 3, además de los datos del certificado de clase 2, se verifica el crédito de la persona o entidad que la solicita.

4) Certificados Clase 4, a las anteriores comprobaciones se le añade la verificación del cargo o la posición de una persona dentro de una organización

5) Certificados SSL para cliente, estos certificados se utilizan para identificar y autenticar a clientes ante servidores cuando se realizan comunicaciones con el protocolo Secure Soket Layer (SSL), se lo da a una persona particular o empleado de una empresa.

6) Certificados SSL para servidor, se utilizan para identificar un servidor ante un usuario cuando tienen una comunicación SSL, se lo expide a una empresa dueña de un servidor seguro.

7) Certificados S/MIME, se utiliza para correo electrónico firmado y cifrado, el mensaje lo firma digitalmente el remitente, además se puede cifrar el mensaje con la llave pública del destinatario.

8) Certificados de firma de objetos, se utilizan para identificar al autor de ficheros o partes de código en cualquier lenguaje de programación. Si un usuario A posee un certificado de este tipo, otro usuario B dejará que ejecute el código que el A requiera, de lo contrario el usuario A será rechazado.

9) Certificados para AC, que identifican a las Autoridades Certificadoras, son utilizados por el cliente para comprobar si la AC es de confianza.

3.3.4.- GESTIÓN DE LAS CLAVES

3.3.4.1.- Ciclo de vida de una clave

Las claves deberán tener una fecha de expiración, de tal forma que los algoritmos que las utilizan no podrán sufrir un ataque con facilidad. El ciclo de vida de una clave incluye los siguientes períodos:

1) Generación del par de claves, la clave o par de claves debe ser emitida por su propietario para proteger sus comunicaciones. Si se utiliza algoritmos de clave asimétrica la clave pública debería ser registrada lo que se genera en un certificado.

2) Distribución de claves, en el caso de la criptografía de clave simétrica debe ser entregada a su destinatario sin la intervención de terceros y para el caso de las claves asimétricas la distribución de la clave no tiene ningún problema pero se debe asegurar mediante un certificado identidad del propietario.

3) Emisión y expiración, la fecha de emisión da por válida la clave y la fecha de expiración puede darse al final de una comunicación o en una fecha

determinada, para el caso de la criptografía de clave pública debe verificarse en el certificado si la clave es aún válida.

4) Retirada, si existe un motivo o sospecha por la que la clave ha sido comprometida, se tiene que dar aviso a la autoridad certificadora para que anule la clave y emita una nueva.

5) Terminación, cuando una clave termina su ciclo de vida es almacenada y reemplaza por una clave nueva.

3.3.4.2.- Almacenamiento de las claves

El almacenamiento de las claves debe tener un grado de importancia mayor, ya que la seguridad de la clave es directamente proporcional al valor de los mensajes que serán cifrados con las claves.

En la actualidad existen métodos para salvaguardar las claves, uno de ellos son las smart cards o tarjetas inteligentes que contienen un circuito integrado que permite encriptar información, almacenar o leer datos a través de un computador.

Las tarjetas inteligentes son la mejor opción para almacenar las claves privadas y de acuerdo al estándar Cryptographic Token Interface en PKCS#11 publicado por la RSA Data Security, en el que se especifica un estándar de bajo nivel para acceder a dispositivos criptográficos desde cualquier plataforma.

3.3.4.3.- Recuperación de las claves

El gobierno de los Estados Unidos no permite la exportación de productos criptográficos debido a que pueden ser utilizados por gobiernos enemigos o terroristas que puedan atentar contra la seguridad de ese país. Pero la sociedad informática ha presionado para impedir esto, con lo que se ha permitido la recuperación de claves o Key Recovery que bajo un estricto mandato judicial

levantan las protecciones criptográficas de determinadas comunicaciones. Se han desarrollado para asegurar la gestión, almacenamiento y recuperación de claves:

1) Key escrow o custodia de claves, en este caso cada usuario u organización genera su clave o claves y las entrega a otra parte que las guarde. Una variante de este mecanismo consiste en fragmentar la clave y confiar cada fragmento a diferentes custodias, con lo que la protección de la clave queda en otras manos.

2) Trusted third party o tercera parte de confianza, en esta técnica aparece una tercera parte que genera la clave de acuerdo a los requerimientos del usuario, la distribuye a los destinatarios correctos y almacena una copia. La seguridad de la clave queda nuevamente en otras manos diferentes a la de los usuarios.

3.3.5- LISTA DE REVOCACIÓN DE CERTIFICADOS

La Certificate Revocation Lists (CRL) o Lista de Revocación de Certificados son listas publicadas por las Autoridades de Certificación donde se incluyen certificados que han sido revocados y por lo tanto no son válidos, esto ayuda para que los clientes puedan comprobar su veracidad.

Un CRL no es más que un archivo de una base de datos firmado por la Autoridad Certificadora, cada certificado tiene un número de identificación y la fecha en que ha sido revocado. Para llevar la lista de certificados revocados las CA deberán contar con servidores que contengan la base de datos con los certificados anulados y con una actualización constante de los mismos. Gráficamente el proceso para los CRLs es el siguiente:

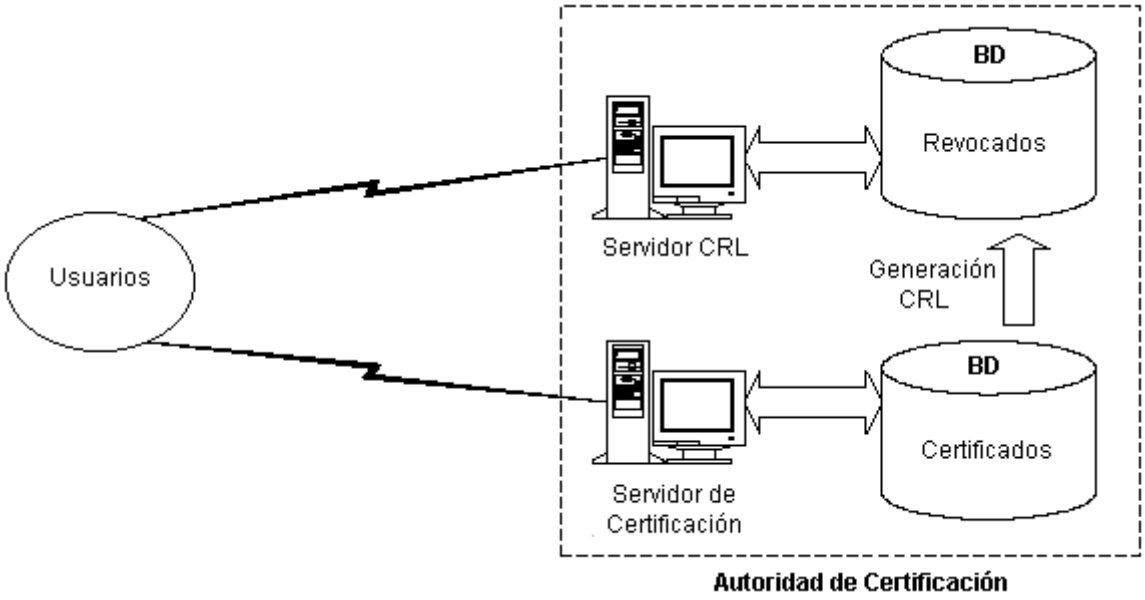

Figura 3.21

Las listas de revocación son totalmente necesarias para descongestionar los sistemas de generación de certificados dentro de una Infraestructura de Clave Pública, con esto se garantizará a los usuarios la calidad de seguridad.

3.4.- AUTORIDADES DE CERTIFICACIÓN

3.4.1.- INTRODUCCIÓN

La confianza es vital dentro de la Infraestructura de Clave Pública es por este motivo que surgen las autoridades de certificación que registran a las personas y a la vez emiten los certificados digitales son los que acreditan una relación entre una determinada clave y su propietario real. Al mismo tiempo surgen los niveles o jerarquías en las Autoridades de Certificación para mantener un ambiente seguro y así evitar falsificaciones en los certificados.

Actualmente existen varias autoridades de certificación en el mundo que son muy conocidas debido a la confianza que durante algún tiempo han dado a sus usuarios. Una Autoridad de Certificación debe cumplir con algunos requisitos y brindar los servicios que están contemplados en la ley, básicamente una

autoridad debe tener los conocimientos técnicos y experiencia necesaria de tal forma que pueda brindar confianza.

Además las autoridades de certificación se han convertido en la base fundamental para el comercio electrónico, puesto que ayuda a confiar en los emisores de una oferta, además de la aceptación de las partes involucradas en un contrato, también se evita el cometer fraudes por falsificación de identidad.

El creciente incremento de negocios electrónicos en el Ecuador hace necesaria la creación y reglamentación de Autoridades de Certificación que permita que estos negocios crezcan progresivamente. Pero para que esta entidad funcione adecuadamente se requiere de la voluntad gubernamental para incorporar ésta tecnología a la sociedad ecuatoriana.

3.4.2.- DEFINICIÓN

Una Autoridad de Certificación o Certification Authorities (CA), es un ente u organismo que de acuerdo a políticas y algoritmos genera certificados digitales utilizando la clave privada del usuario para firmarlos. Una CA tiene otras funciones como revocar los certificados mediante las CRLs.

Es decir una CA es la responsable de emitir los certificados, de verificarlos, así como de dar a conocer las claves públicas en los directorios destinados para ello, debe contar con medidas de seguridad que infundan confianza para el éxito de su gestión, así como altos niveles de calidad en la atención y disponibilidad para los usuarios.

Una Autoridad de Certificación puede hacer uso de las Autoridades de Registro que son las encargadas de verificar la identidad de las personas y así solicitar la emisión correspondiente del certificado bajo los procesos determinados por la CA

3.4.3.- CARACTERISTICAS

3.4.3.1.- Elementos de las CA

Una Autoridad de Certificación debe poseer un proceso de autenticación y a la vez éste debe contar con:

- Una política de certificación que permita regular los servicios de certificación, esto es las solicitudes para un certificado, la validación de la solicitud, la emisión, el uso, la suspensión, la revocación o renovación del certificado.

- Un certificado de la CA que dará una jerarquía de confianza, puesto que debe existir un Autoridad de Certificación raíz que avale y de fiabilidad a los usuarios que la CA que utilizan está legalmente establecida.

- Los certificados de los usuarios que deben estar bajo una estándar que puede ser el X.509 v3, con esto los usuarios podrán manejar sus certificados y tener conocimiento de la información que contienen dichos certificados.

- Los protocolos de autenticación, gestión y obtención de certificados deben estar bien definidos por las CA para que sus usuarios no tengan inconvenientes a la hora de obtener sus certificados.

3.4.3.2.- Obligaciones y responsabilidades de las CA

Una Autoridad de Certificación debe cumplir con las obligaciones estipuladas en la ley, en general tienen que cumplir con eficiencia los servicios para lo que fueron creadas, controlar su principal actividad, que es la comprobación de la identidad de los solicitantes de certificados, así como la gestión eficiente de los certificados

para que cumplan con los requisitos legales exigidos en las sociedades que reconocen a dichas autoridades.

Deben responder por los servicios de certificación que están ofreciendo, puesto que si causaren daños y perjuicios a sus clientes tendrán que compensarlos por el incumplimiento de sus obligaciones.

En el Ecuador las Autoridades o Entidades de Certificación son autorizadas por el Consejo Nacional de Telecomunicaciones (CONATEL) y sus obligaciones están bien definidas en el Art. 30 Capítulo III. En cuanto a las responsabilidades de la CA acreditadas están definidas en el Art. 31 del capítulo antes mencionado.

3.4.3.3.- Requisitos para crear una CA

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su reunión celebrada del 18 al 28 de febrero de 1997, debatió sobre la necesidad de establecer los requisitos para el establecimiento de una Autoridad Certificadora. Los requisitos que ha continuación se describen fueron tomados del párrafo 44 del documento denominado A/CN.9/WGIVo/WP.71, que es el resultado de la reunión de la comisión.

1.Independencia (ausencia de interés financiero o de otro tipo en las transacciones subyacentes).

2. Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de pérdida

3. Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados.

4. Longevidad (conservación de certificados).

5. Aprobación del equipo y los programas.

6. Mantenimiento de un registro de auditoria y realización de auditorias por una entidad independiente.

7. existencia de un plan para casos de emergencia.

8. Selección y administración del personal.

9. Disposiciones para proteger su propia clave privada

10. Seguridad interna.

11. Disposiciones para suspender las operaciones, incluida la notificación a los usuarios.

12. Garantías y representaciones.

13. Limitación de la responsabilidad.

14. Seguros.

15. Capacidad para intercambiar datos con otras autoridades certificadoras.

16. Procedimientos de revocación.

3.4.4.- FUNCIONES

Dentro de las funciones de las Autoridades de Certificación están las que a continuación se detallan:

1) Generación y registro de claves, existen muchos usuarios que tienen varias claves para usos distintos que puede ser para el trabajo, personal o para uso administrativo. De cualquier manera cuando se han generado el par de claves se debe registrar su clave pública ante una CA y de acuerdo a los procesos y políticas de certificación que tenga la autoridad se emitirá un certificado digital que de validez a la clave pública del usuario.

2) Identificación de solicitantes de certificados, para que una CA proporcione un Certificado de Identidad Personal se exige a los usuarios brindar los identificadores intrínsecos, que son características propias de los solicitantes como pueden ser la fotografía, firma manuscrita, huellas dactilares, timbre de voz, marcas de nacimiento, etc. Aunque no todas las Autoridades piden los mismos requisitos ya que depende de sus políticas y tipo de certificado que se solicite.

3) Emisión del certificado, como ya se ha mencionado las CA proporcionan certificados digitales pero también deben mantener un registro actual de los certificados que emite. Un certificado puede estar en estado activo o preactivo desde cuando se ha generado hasta que entre en vigencia. Un certificado está suspendido cuando la CA ha decido anularlo temporalmente hasta que se lo vuelva a poner en estado activo. Un certificado es revocado cuando las condiciones por las que fue emitido cambiaron antes de que expire, para lo cual se emite otro certificado que es de revocación. Un certificado está caducado cuando la fecha límite ha terminado, este cumplió con todas las operaciones válidas.

4) Almacenamiento en la CA de las claves privadas, es importante para la CA mantener completamente seguras las claves privadas por la reputación de la entidad. Para conseguir un nivel alto de seguridad se utiliza hardware con medidas de seguridad sofisticadas, a estas unidades son las Unidades de Firmado de Certificado, están diseñadas para que ante cualquier intromisión las claves y demás información relacionada se destruyan antes de que puedan ser obtenidas por intrusos.

5) Mantenimiento de las claves vigentes y revocadas, dentro de los servicios de las CA está almacenar los certificados emitidos durante un período de validez, de tal forma que si un usuario pierde su certificado podrá solicitar una copia a la autoridad emisora. Asimismo se deberá mantener una lista de certificados revocados o CRLs para que invalide cualquier operación que se haga con fecha posterior a la revocación del certificado.

6) Servicios de directorio, es una base de datos mediante la cual cualquier usuario puede obtener la clave pública certificada de otro. Estos directorios tienen las funciones de guías telefónicas de modo que los usuarios puedan obtener los certificados de las claves públicas que necesiten.

3.5.- AUTORIDADES DE REGISTRO

3.5.1.- INTRODUCCIÓN

Las Autoridades de Certificación son agentes confiables que firman digitalmente, por esto en las instalaciones de una CA no se deben escatimar gastos para proporcionar la más alta seguridad a los medios tecnológicos utilizados. Las instalaciones por lo tanto son costosas y es poco probable que las Autoridades de Certificación las asuman.

Es cuando aparecen las Agencias de Registro asociadas con las CAs, son una extensión lógica que publica y ejecutan las políticas de seguridad, son las que deciden sobre la emisión de los certificados digitales.

En estas agencias están las Autoridades de Registro que son intermediarios con las Autoridades de Certificación, son los que realmente verifican la identidad de los usuarios solicitantes de certificados. Asimismo se encargaran de la revocación de los certificados.

Las Autoridades de Registro son las encargadas de hacer llegar las peticiones de los usuarios remotos a la Autoridades de Certificación, de tal forma que los procedimientos para adquirir un certificado digital se vuelve más rápido y eficaz.

En una Infraestructura de Clave Pública (PKI), estas autoridades tienen funciones notariales, son de gran importancia porque es el enlace más directo que tiene una CA con los usuarios.

3.5.2.- DEFINICIÓN

Una Registration Authorities (RA) o Autoridad de Registro es la encargada de gestionar las peticiones de certificación y revocación de certificados digitales, así como de identificar o autenticar de manera única a los usuarios que solicitan dichos certificados, la calidad del proceso de autentificación establece el nivel de confianza que se puede otorgar a los certificados digitales.

Cualquier usuario de Internet que desee solicitar un certificado de clave pública debe primero dirigirse a una RA, ésta tendrá que cumplir con:

- Efectuar la autentificación única del usuario, mediante procedimientos apropiados a los niveles de seguridad que ofrece cada categoría de certificado.

- Enviar la información del usuario a la Autoridad de Certificación para generar el certificado correspondiente.

- Recibir y verificar los certificados emitidos por la Autoridad de Certificación.

- Entregar el certificado con su correspondiente clave pública al usuario.

- Recibir peticiones de revocación de certificados por parte del usuario, realizar la correspondiente validación y enviarla a la Autoridad de Certificación.

3.5.3.- AUTORIDADES DE FECHADO DIGITAL

Las Time Stamping Authorities (TSA) o Autoridades de Fechado Digital son la que relacionan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento electrónico.

Esta tercera autoridad afianza la seguridad para la firma, pues se compromete a registrar con la fecha y hora actual un resumen del documento que dará como resultado un certificado de tiempo que es la única prueba de que dicho documento exista en tal fecha.

La TSA no comprueba el contenido del documento ni la identidad del usuario que lo somete a este fechado. Es importante para las Autoridades de Certificación tener fechas convincentes para cuando se revoque los certificados, aunque esto no es necesario cuando se los emite.

Las Autoridades de Fechado digital permiten verifica si la firma digital fue ejecutada dentro del período de validez del certificado. Con esto se previenen fechados fraudulentos ya sea antes o después de la fecha asignada, a la vez impiden alterar el contenido del documento posterior al instante de la firma.

IV. METODOLOGÍA PARA EL DISEÑO DE UN PKI

4.1.- INTRODUCCIÓN A LA METODOLOGÍA

4.1.1.- METODOLOGÍA

Se la puede definir como un conjunto lógico de métodos y técnicas definidos como un modelo, aplicados de tal forma que los resultados permitan optimizar los procesos. Se dice que la metodología es un procedimiento porque definirá el Que y una técnica porque especificará el Cómo se la aplicará dentro de un entorno, éste es importante para aplicar una metodología pues depende de la organización, sus empleados y los objetivos que quiere alcanzar.

4.1.2.- COMPONENTES

Para crear una metodología que sea aceptada y cumpla con las expectativas de sus usuarios se debe pensar en los componentes:

1) Método de trabajo, es la forma en que se va a descomponer las actividades o etapas, definirá también que se tiene que hacer y que tecnologías se utilizarán para generar los documentos.

2) Técnicas utilizadas, en la que se dará una clara explicación de cómo llevar a cabo las actividades especificadas anteriormente.

3) Control del trabajo, en donde se definirá las responsabilidades de cada uno de los integrantes del grupo de trabajo, así como el control de etapas planificadas.

4) Documentación, que se genera a través del desarrollo de la metodología y que cuando sea aplicada permitirá el óptimo funcionamiento de la Infraestructura de Clave Pública.

4.1.3.- INTRODUCCIÓN A LA METODOLOGÍA

La implementación de una Infraestructura de Clave Pública (PKI) en una organización requiere de varias etapas que se someterán a pruebas de eficiencia y seguridad que proporcionará a la red, no sólo están los certificados y la Autoridades de Certificación como parte de la infraestructura sino también las políticas que la organización deberá definir para el desarrollo y mantenimiento de los elementos involucrados en una PKI. Se basa en la criptografía asimétrica, ya que proporciona los mecanismos necesarios para establecer comunicaciones seguras en la red. Además de los servicios, protocolos y tecnología para la gestión de un sistema de información seguro.

Uno a uno han ido surgiendo los problemas así como sus respectivas soluciones, desde cuando se pensó en la criptografía de clave pública como respuesta a la seguridad en Internet, luego con los certificados digitales se aumentó el grado de certeza, pero a ello se suman los Autoridades de Certificación para garantizar y validar la autenticidad de las claves, sin embargo la aparición la Infraestructura de Clave Pública (PKI) que reúne todo lo anterior y a otros servicios ofrece verdaderamente la fortalece y garantía a las comunicaciones en general.

Es recomendable pensar en las aplicaciones como correo y comercio electrónico seguro, comunicaciones seguras o software firmado, pues formarán parte de la Infraestructura de Clave Pública (PKI), y que en mayor o menor grado determinarán el rendimiento de dicha infraestructura. Actualmente es la solución más conveniente para una empresa, aunque no es mágica es apta para cualquier tipo de negocio y resulta ideal en una intranet, ya que provee mayor agilidad que los sistemas tradicionales basados en un nombre, una contraseña y un control de acceso. Pero cuando se trata de una extranet o de Internet el uso es casi obligado, pues hasta hoy es la única forma de brindar confianza a los usuarios que no se conocen entre ellos.

4.2.- ESTUDIO DE LOS REQUERIMIENTOS PARA EL DISEÑO DE UN PKI

4.2.1.- INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

PKI es el acrónimo de Public Key Infraestructure (Infraestructura de Clave Pública), es una tecnología que reúne protocolos servicios y normas que son la base de una aplicación que utiliza criptografía de clave pública con la finalidad de gestionar los certificados digitales, las claves públicas y privadas.

Generalmente una PKI es un sistema de certificados digitales, autoridades de certificación (CA) y otras entidades de registro que autentican y validan a cada parte involucrada especialmente en una transacción electrónica. Se compone de varios elementos pero los que son trascendentales son los que se muestran en la siguiente figura:

Figura 4.22

La Autoridad de Certificación, es la parte central y fundamental del PKI, está constituida por hardware, software y personas que proporcionan confianza.

Política de Certificación, son procedimientos operativos que rigen a la PKI, establecen las responsabilidades entre la CA y los usuarios finales a través de documentos técnico legales.

Aplicaciones PKI-Enabled, son aplicaciones software que operan con los certificados digitales.

Soporte de Clave Privada y Pública, se refiere a la gestión de claves, es decir la generación, recuperación y almacenamiento de clave.

Publicación de Certificados, es importante mantener un repositorio de certificados que permita operar entre sus usuarios, así como un buen mantenimiento de las listas de revocación de certificados (CRL).

4.2.2.- REQUERIMIENTOS PARA IMPLANTAR DE UNA PKI

El tiempo, el esfuerzo y el costo son considerables durante la implementación de una PKI, entonces habrá que pensar si la organización requiere los niveles de seguridad que ofrece y si resolverá los problemas de dicha organización. Para un bueno diseño de una PKI se requiere una compresión tanto tecnológica como funcional de todos y cada unos de sus componentes, pues, con esto se quiere proteger datos sensibles a través de la encriptación y la emisión de certificados, que es lo básico en una PKI.

Para la implementación de una PKI en una organización se debe empezar por crear un plan de trabajo que contemple lo siguiente:

1) Formación de un equipo, el que representará a todos los usuarios.

2) Evaluación del entorno, para saber lo que se puede utilizar para el diseño de la PKI como personal, hardware, etc.

3) Identificar requerimientos, que pueden ser estratégicos, comerciales y técnicos acorde a los objetivos del diseño.

4) Desarrollar un plan del proyecto, que será realizado sobre la base de la información antes obtenida.

5) Evaluar y probar, a través de un conjunto de criterios de evaluación al diseño inicial y luego con los productos finales.

6) Fase piloto, en la que se pondrá en marcha todo lo antes planificado y desarrollado, es donde se explicará a los usuarios de los servicios de la PKI, así como sus beneficios. También se informará al personal técnico.

7) Implementación, de la fase piloto se procederá a la implementación total de la PKI.

4.3.- DESARROLLO DE LA METODOLOGÍA

La Infraestructura de Clave Pública (PKI) y los certificados digitales dan el soporte de seguridad necesario para los negocios en internet o en la información que maneje. Con los conceptos bien definidos de la Infraestructura de Clave Pública (PKI) y los elementos que intervienen en ella, se puede empezar con el desarrollo de la metodología para el diseño de una PKI.

La metodología que se propone evitará tomar decisiones equivocadas provocando pérdida de tiempo y dinero para la organización, contiene varias etapas consecuentes que se irán describiendo con precisión para evitar confusiones por parte del usuario. Además cada etapa abarca procesos importantes para el diseño los que se analizarán con detalle.

4.3.1.- ETAPAS DE LA METODOLOGÍA

4.3.1.1.- Análisis de los requerimientos básicos

En ésta primera etapa el equipo de trabajo, que se ha de formar con la exclusiva finalidad del diseñar la Infraestructura de Clave Pública (PKI) detallará:

- Los motivos para el diseño.
- Se identificará los requerimientos para diseñar la PKI
- Se definirá los requerimientos de usuario.
- Requerimientos de seguridad de la PKI.

1) Motivos para el diseño, se definirá el para que del diseño de la PKI, esto para conocer el alcance dentro de la organización, basándose en las aplicaciones que se tiene que instalar y con las que se cuenta actualmente. Es importante conocer las directrices de los negocios, pues, de esto dependerá el éxito de la implementación, así como el grado de afectación de los usuarios. Los negocios electrónicos que en la actualidad toda organización tiene o quiere implementar, es una razón para que se opte por una PKI y que sus transacciones sean seguras y rentables ante la inversión de dicha implementación.

Privacidad, integridad y autenticidad de la información en comunicaciones a través de internet, debido a que ésta información es de estricta confidencialidad para la organización y sus usuarios. El lograr que las comunicaciones no sean alteradas es el principal motivo para el diseño de una PKI.

Disminución del trabajo en la organización debido a la utilización de los documentos firmados electrónicamente, pues se reduce los costos de almacenamiento de los documentos firmados físicamente y los procesos que conllevaría almacenar dichos documentos.

Soporte al usuario en cuanto al manejo de sus cuentas y contraseñas, pues se necesita que los recursos sean bien administrados y no utilicen espacio innecesario con información obsoleta. Además evitar que las contraseñas sean mal administradas, ya que se han dado incidentes en los que las contraseñas son de acceso fácil.

Aumento de Seguridad en los procesos de la organización, este es el principal motivo para la implementación de una PKI, aunque es conveniente describir de forma explícita las áreas de la organización que se beneficiarán de la seguridad de la PKI, así como las que necesitarán de mecanismos más fuertes de autenticación, autorización y control de acceso.

2) Requisitos para el diseño de la PKI, actualmente no existe un diseño estandarizado de una PKI, pues cada red presenta sus propias características así como las aplicaciones que se colocarán en la ella. Por lo tanto se debe iniciar con la planeación y definición de la arquitectura de la Infraestructura de Clave Pública especificadas según las necesidades de la organización, detallando de forma física y lógica la red que dispone para el diseño de la PKI. Esta arquitectura generalmente contiene los siguientes elementos:

Un servidor PKI que lo constituye la Autoridad Certificadora y un repositorio de certificados o directorio. La organización deberá decidir como se van a utilizar estos elementos, cuales serán sus funciones y objetivos. Hay que tomar en cuanta que la arquitectura PKI se acoplará a la que tiene la organización, es esencial ubicar a los servidores PKI así como las aplicaciones y usuarios que formarán parte de esta infraestructura.

Clientes PKI formados por un servidor web, un browser, aplicaciones que utilicen la clave pública. El usuario tendrá que adaptarse a las nuevas aplicaciones que le permitirán identificase y autenticarse a través de los certificados, pero antes deberá tener la preparación correspondiente para evitar

los fracasos en la implementación. Además se definirá los algoritmos y estándares criptográficos necesarios para el manejo de claves.

Certificados Digitales que serán emitidos por el servidor y luego utilizados por los clientes. Es recomendable que exista un grupo de administración de certificados que manejará el ciclo del certificado, es decir, la inscripción inicial, la aprobación, revocación, renovación y reemplazo del certificado.

3) Requisitos del usuario, es importante satisfacer las necesidades de los usuarios, estarán en diferentes categorías y sus conocimientos será para algunos limitado por lo que las aplicaciones tendrán que ser lo más transparentes posibles. El impacto del usuario interno o externo frente a esta tecnología estará de acuerdo al entrenamiento e información que le brinde la organización. Los usuarios de la PKI pueden ser personas, software o hardware geográficamente distantes, en el caso de que los usuarios estén físicamente lejos como se haría para identificarlos y registrarlos, es recomendable determinar el posible número de usuarios y su localización para evitar que el diseño de la PKI tenga cubrir inconvenientes no previstos.

4) Requisitos de seguridad de la PKI, es primordial en esta etapa establecer los requerimientos de seguridad, que como ya se mencionó son: confiabilidad, integridad, disponibilidad, seguridad. La disponibilidad en cuanto a las responsabilidades que adquiera la PKI y respecto a tiempo de recuperación en el caso de ataques o robos debe ser el menor posible, para lo cual se contará con un plan que permite mantener bajo control cualquier improvisto. La seguridad, esto aunque parece redundante no está por demás confirmarlo, ya que el diseño de una PKI principalmente ofrecerá un nivel alto de seguridad en lo que se definió como directrices de negocios. Es necesario tomar en cuenta a los sistemas que se enlazarán a la PKI para no perjudicar el rendimiento de los procesos de la organización.

4.3.1.2.- Descripción de los servicios

Para el diseño de una PKI se debe planificar los servicios, que generalmente se proporciona a sus usuarios que como se mencionó serán personas, hardware o software. Por tanto los servicios estarán en función de estos elementos que determinarán el desempeño de la Infraestructura de Clave Pública. Los servicios que se describen a continuación son una guía para el diseñador:

- Servicio de Administración del Ciclo de Vida de las Claves.
- Servicio de Administración de Certificados.
- Servicio de Lista de Revocación de Certificados (CRL).

1) Servicio de administración del ciclo de vida de claves, el tiempo que pueda mantenerse una clave en secreto es relativo ya que depende de factores como: los avances en los métodos de criptoanálisis, fallas en la implementación del software o hardware o por que simplemente el dueño de la clave no supo mantenerla en secreto. El diseño de la PKI debe contar principalmente con el servicio de claves para firmas digitales para lo cual es necesario crear una entidad firmadora / verificadora que se encargará de cifrar el valor hash con la clave privada y verificarla a través de la clave pública descifrando el hash firmado. En cuanto a esquemas de recuperación de claves para firmas digitales no es muy utilizado debido a los inconvenientes en la aceptación de documentos firmados, cuando se extravía la clave privada de la firma y para proporcionar seguridad la mejor solución es crear un nuevo par de claves y un certificado para generar la firma.

La administración de la clave se refiere a procesos de generación, distribución, protección, almacenamiento y recuperación de la misma. En la generación de la clave es recomendable tomar en cuenta el tamaño de las claves y el algoritmo pues determina directamente la dificultad para descifrarla, si el número de bits aumenta la cantidad de potencia para el procesamiento y el tiempo crece aceleradamente. Sin embargo los costos de generación pueden ser altos.

Iniciado el sistema de generación de claves es necesario decidirse por un sistema centralizado o distribuido. El centralizado simplifica el servicio de almacenamiento y recuperación de las claves, utilizado en claves de cifrado que usualmente están en un sistema de archivo, en cambio las claves de firmas digitales generadas localmente casi nunca se archivan. El sistema centralizado se vuelve un elemento de seguridad sensible para un ataque a la Infraestructura. En el sistema distribuido la generación de claves está dada por el lado del cliente, en estás condiciones la aceptación será legal y técnica. Pero se puede necesitar de elementos hardware adicional para el diseño de la PKI, este es el caso de las tarjetas inteligentes.

Con la experiencia de otras aplicaciones PKI se puede utilizar un sistema dividido que genere centralmente las claves de cifrado y que las firmas digitales se generen en una aplicación cliente a través de una tarjeta inteligente. Con los dos sistemas se requiere unidades de procesamiento centrales de calidad con un buen soporte de hardware para números aleatorios para que el sistema de generación de claves este disponible y sea altamente confiable.

Se inicia la distribución o transporte de claves mediante el estándar PKCS#12, el cual es un contenedor que puede transferir las claves con seguridad entres los almacenes, pero ésta no es una solución a largo plazo para soportar movilidad de las claves. La respuesta está en la smart card ya que permite que claves y certificados se transporten con seguridad entre las aplicaciones y ambientes de computación.

En cuanto a la protección de la clave privada debe ser fuerte en cada etapa de su ciclo de vida, por eso es recomendable generarla a nivel local a través de medios electrónicos probados. Dentro del diseño de una PKI el compartir claves y certificados entre aplicaciones es una característica muy ambicionada que permite a los usuarios disminuir la cantidad de claves y certificados que les dejará identificar estas aplicaciones, además de que las tarjetas inteligentes son la base fundamental para un esquema de protección de claves para el usuario.

El sistema de recuperación se lo implementa para las claves de cifrado y no para las firmas digitales, es importante también mantener un archivo con registros de auditoria o los denominados logs. Desde este punto existen claves actuales o activas, anteriores y antiguas que necesitan de un sistema de recuperación.

Una Clave Activa o actual se puede recuperar por la pérdida temporal debido a un descuido del usuario al extraviar el dispositivo donde estaba almacenada la clave, sin embargo lo más óptimo sería crear una nueva clave, en ese caso la clave pasaría a ser anterior. Una Clave Anterior de hecho será el siguiente estado de la clave actual, debido especialmente por tiempo de vida de las claves. El proceso de superposición de claves debe manejarse los más transparente posible para no afectar la PKI. Este proceso ocurre cuando se han cambiado las claves de un día a otro debido a que se han caducado. Una alternativa es mantener un servicio central de archivos y recuperación de claves para el usuario. A las claves antiguas probablemente será necesario acceder en un tiempo que sobrepase las claves actual y anterior que serán de uno a dos años. Aunque el sistema de recuperación sea costoso por los recursos que consuma es muy probable su implementación.

2) Servicio de Administración de Certificados, se refiere a una serie de operaciones en el certificado aplicables durante todo su ciclo de vida. Los certificados para claves públicas o firmas digitales son emitidos por las CA por tanto son responsables de todo el desarrollo de administración. Se incluyen procesos como:

Registro del certificado, es la fase inicial en donde el usuario deberá proporcionar la información necesaria para crear una solicitud que luego será analizada por la CA. Mucha de la información contenida afecta directamente la privacidad por lo que seria mejor revisarla antes de publicarla, pues se puede haber modificado o agregado información durante el proceso de expedición. Es apropiado también distribuir las anclas de confianza entre los usuarios, esto se lo puede realizar como respuesta a una solicitud.

Una vez hecha la solicitud se necesitará que los suscriptores se presenten físicamente ante una autoridad de registro (RA) para verificar con la documentación correspondiente la identidad del usuario. Cuando la CA y la RA verifiquen que la solicitud cumple los requisitos se expedirá el certificado. Una alternativa es crear un sitio central se establecería con un sistema de personalización de tarjetas inteligentes que enliste a los usuarios y tome la información necesaria para generar las solicitudes a la CA.

Ahora para comprobar que el usuario realmente posee la clave privada correspondiente a la pública se realiza la Proof of Possession (POP) o Prueba de Posesión. En las firmas digitales se verifica a través de la firma de la solicitud de registro y comprobando la firma con la clave pública correspondiente enviada en el mensaje de solicitud. En cuanto a las claves de cifrado es un poco más complicado, pero una solución sería que la RA plantee una pregunta aleatoria cifrándola con la clave pública si el suscriptor descifra la pregunta se comprueba que el usuario tiene la clave privada.

Renovación del Certificado, para expedir un nuevo certificado es necesario que este haya llegado al final de su vida útil o haber expirado y en algunos tendrá que hacerse necesario la actualización de los datos. Cuando la renovación sea de una CA las claves anteriores se utilizarán para firmar un nuevo certificado y las nuevas para firmar un viejo, de donde surgen cuatro certificados de la CA raíz. Un certificado viejo con viejo lo tienen todos los que dependen de la CA al momento de la actualización. Un certificado nuevo con viejo permite que la clave pública de la CA generada sea comprobada por la anterior. Terminado el proceso anterior se crea el certificado nuevo con nuevo en la que permite a todas las partes el reconocimiento de las nuevas claves. En tanto el certificado viejo con nuevo permite una transición suave del nuevo par de claves y sigan confiando en la CA con certificado antiguo.

Revocación del Certificado, se realiza cuando las condiciones exigen el término de su validez antes de la fecha establecida o por un desacuerdo en la identidad

del usuario con su clave privada. En circunstancias en las que haya cambiado el estado del usuario o por que la clave se encuentre seriamente comprometida. Es necesario que se comunique al usuario a partir de que fecha no será válido el certificado, así como publicarlo ante los usuarios de Internet para que puedan determinar cuales son las operaciones válidas del certificado.

Publicación de Certificados, la responsabilidad de la CA cuando se haya revocado un certificado es publicarlo, los usuarios requerirán que las publicaciones se realicen en un tiempo mínimo debido a que realizan transacciones financieras de alto valor, si el número de certificados es grande esto afectará la lista de revocación, o si el usuario tiene restricciones de recursos para procesar una lista larga. Por tanto el sistema de revocación debe tener en cuenta estos factores para el usuario reciba un servicio óptimo y la suficiente confianza de la lista de certificados.

Mecanismos de Auditoria, cualquiera que fuere la finalidad de una organización se deberá proporcionar los mecanismos necesarios para realizar una auditoria a cada uno de los procesos diseñados en la Infraestructura de Clave Pública. La auditoria es un examen cuya finalidad evaluar la eficacia y eficiencia de una entidad la cual será factible de realizarla en cualquier momento.

3) Servicio de Lista de Revocación de Certificados (CRL), las Listas de Revocación de Certificados (CRL) son un esquema que bajo un estándar notifican la revocación, en su forma más simple es una lista regulada por la CA que contiene todos los certificados no autorizados a funcionar. La CRL tiene un sentido de autoprotección porque el usuario puede identificar cuando un certificado ha sido modificado de la lista y se hace innecesaria la seguridad en el almacén de certificados.

Punto de Distribución de CRL en donde se clasificarán las CRL por categorías de acuerdo al tipo de certificado o de revocatoria, esto ayudará a la Autoridad de Certificación a manejar listas más pequeñas de certificados o por el contrario

generar una CRL indirecta en la que pueden participar varias CA, en esta contará un Expedidor de Certificado que identificará la CA que expidió la revocación.

CRL simples es un contenedor o archivo secuencial que va creciendo y que contiene una lista de certificados revocados identificados por un número de serie, sin embargo tiene otra información que podría hacer que la tasa de revocación de certificados crezca directamente y afecte el desempeño de la CRL simple.

CRL delta fue creada para reducir el tamaño de la CRL que se transmite hacia el usuario destino. La constituye un CRL base, que contiene una lista de revocaciones completa emita por una determinada CA, a partir de aquí se realizan deltas o actualizaciones que son como una CRL firmadas por una CA. Sin embargo tiene un Identificador CRL Delta que la marca como crítica para que los usuarios sepan que las lista no está con información completa. Los diseñadores son libres de escoger el tipo de CRL que más se ajuste a la organización tomando en cuenta los productos que se entregarán y si el diseño de la PKI será dirigido a usuarios internos o externos.

4.3.1.3.- Descripción de las herramientas y funciones para el desarrollo de los servicios de PKI

La tecnología por la que se ha optado contiene una variedad de características relacionadas principalmente con la autenticación, por lo tanto el diseño de la PKI es el principio de un proceso que en muchos de los casos cambiará la estructura de la organización. Este documento es una guía que se ajusta a los estándares que actualmente están siendo utilizados por otras empresas y que están funcionando y siendo de gran utilidad en sus procesos. Una organización deberá estar dotada de los siguientes servicios y funciones:

1) Manejo de claves, la generación y disponibilidad de un par de claves pública y privada dependerá de atributos como el tipo de algoritmo criptográfico que generará las claves que tendrá que dar soporte tanto operaciones de firma

como de cifrado. La longitud de las claves es una fortaleza para operaciones de cifrado. El grado de sensibilidad de la información incidirá en el nivel de seguridad para el almacenamiento de las claves. Se considerará los siguientes subservicios:

Claves de Cifrado, denominada así en el estándar X.509. Para el cifrado la clave pública de propietario de la información la usa para cifrar los datos y la privada para descifrar, como se ha venido mencionado. Cuando se cifran los datos surge la necesidad de implementar un mecanismo de recuperación de claves cuando se pierda o destruya, sin embargo este mecanismo puede debilitar la Infraestructura y poner en duda la privacidad de la información.

Claves de Firma Digital, el generar un par de claves pública y privada con fines de firma digital es para la CA una responsabilidad ya que pone en juego la seguridad que pretende proveer a sus usuarios. Una excelente alternativa es que la CA cree el mecanismo para generar las claves y que la primera vez que se entregue tiene que ser personalmente o a través de estándares de intercambio seguro y luego podrán comunicarse por la red con toda la seguridad y privacidad mediante las claves entregadas. Los estándares de intercambio seguro son aceptados por una PKI y consiste en que las claves privada y publica son transportadas en un contenedor de software protegido por una clave simétrica. De hecho este paquete es importante por lo que cuando cumpla su finalidad debería destruirse ya que sería un blanco perfecto para un pirata informático.

2) Actualización de las claves, las claves deben ser únicas para cada usuario y el tiempo de validez de la clave debe tener un tiempo mínimo de un año. El generar periódicamente nuevas claves hace una buena práctica de seguridad, razón para probar los períodos de validez de los certificados ya que su expiración está relacionada con la generación de una nueva clave.

3) Modelos de Confianza de Autoridades de Certificación (CA), la recomendación X.509 y el grupo de trabajo PKIX asumen un espacio global de nombre por lo que piensan en una CA centralizada o jerárquica. Pero existe otra

filosofía donde existe una multitud de espacios locales enlazados donde la jerarquía no existe. Sobre estas filosofías se ha hecho algunas variantes que por sus características se podrá pensar en una que sea objeto del diseño.

Modelos Jerárquicos Subordinados, permite relaciones de confianza unidireccionales. La Autoridad de Certificación raíz es al ancla de confianza común para todos los usuarios y las demás relaciones se formarán a partir de esta CA. La principal función es certificar a los niveles más bajos de CA que se hayan formado y que están subordinadas a través de las relaciones de confianza construidas en éste modelo. Gráficamente un modelo de este tipo es como sigue:

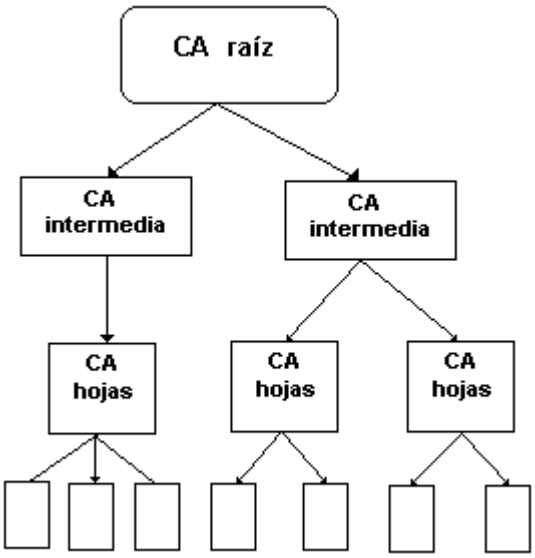

Figura 4.23

La CA raíz crea un certificado autofirmado por sí misma, la clave pública de este certificado corresponde a la clave privada utilizada para generar la firma en el certificado, de modo que la clave pública se utilizará para validar la firma en el certificado. En este modelo la CA subordinada no puede certificar a otras CA, lo que se denomina Restricciones de Nombre. Además todas las rutas incluirán el certificado de la CA raíz. Si existe el peligro de una clave comprometida la CA raíz y sus ramificaciones también lo estarán, entonces el modelo de confianza y sus

usuarios serán afectados. Se tendrá que revocar y generar nuevos certificados, reemplazar cualquier certificado y clave que estuviera dudosa.

Pero cuando se quiere crear una nueva comunidad de usuarios es sencillo pues se crea una relación de confianza entre ésta y la CA raíz. Además la búsqueda de la cadena de certificados es simple, puesto que nunca será mayor a la profundidad del árbol. Este modelo puede trabajar bien dentro de una empresa y mejor aún si se tiene una estructura organizacional fuertemente jerárquica.

Modelo Entre Iguales, este modelo asume la confianza entre dos Autoridades de Certificación que no son subordinadas entre sí. En este modelo se conoce a la certificación cruzada que se da cuando una CA certifica una clave pública de otra creando una confianza bilateral. Este modelo es sencillo pero le hace falta escalabilidad, pues cada CA debe certificar directamente a las demás CA que quieran incluirse en el modelo, por lo tanto la cantidad de relaciones que se establezcan es de aproximadamente el cuadrado del número de autoridades de certificación. Gráficamente el modelo sería así:

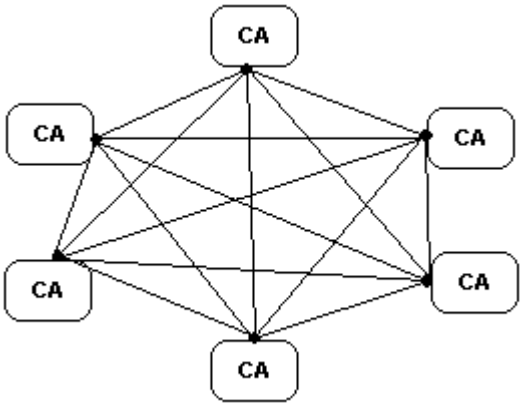

Figura 4.24

Cada CA establecerá una relación bidireccional lo que genera e intercambia dos certificados cruzados. Si una CA está comprometida no afectará el diseño de la PKI completamente, su recuperación significa revocar los certificados de la CA comprometida. Actualmente el impedimento más significativo es la falta de

soporte de aplicaciones para cadenas de certificados que contienen certificados cruzados

Modelo de Malla, el modelo entre iguales es muy útil pero tiene algunas restricciones que pueden ser mejoradas aplicando esta misma técnica dando como resultado el modelo de malla, en donde se construyen cadenas largas de certificados. Para crear las relaciones de confianza cada usuario tendrá certificaciones cruzadas con otros iguales, con lo que la ruta del certificado atraviesa múltiples CA. Gráficamente este modelo se vería así:

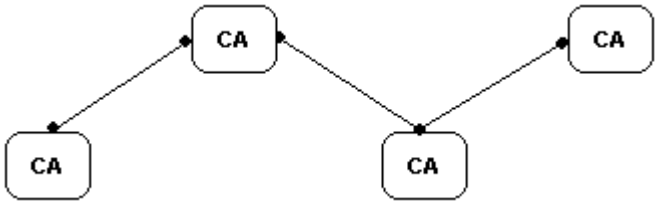

Figura 4.25

Cuando la longitud de las rutas aumenta es difícil mantener un nivel de aseguramiento a través de los dominios de confianza, las largas rutas de certificados incurren en operaciones de validación significativas. Por lo tanto es mejor mantener rutas tan cortas como sea posible, por esto se recomienda establecer una Relación Directa, que disminuirá los procesamientos y los recursos para la validación del certificado, el siguiente gráfico muestra esta relación:

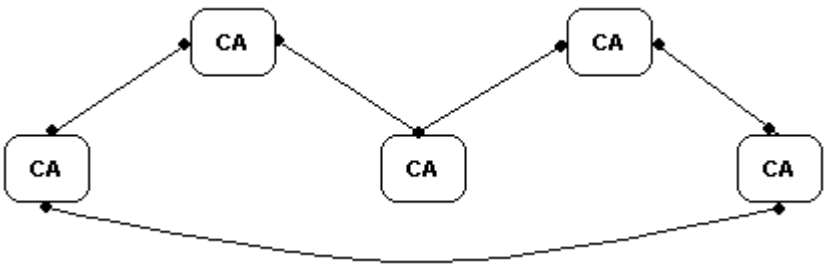

Figura 4.26

En este modelo puede requerir evaluar rutas alternas para determinar rutas de confianza además el tiempo será significativo para recorrer las rutas. La complejidad para encontrar la ruta válida aumenta con el número de relaciones de confianza y más si no estaban previstas. Un modelo de malla es válido siempre que se establezcan restricciones para mantener un control sobre las acciones de los usuarios, pues el éxito está en el acceso a los directorios para localizar los certificados cruzados que requerirán de un ancho de banda grande.

Modelo Híbrido en el que se tome lo mejor de cada modelo y se diseñe de acuerdo a las necesidades permitiendo que los dominios de confianza se mantengan ante las extensiones o fusiones con otras organizaciones. Esto puede facilitar las cadenas de certificados para que sean más cortas y directas. Las combinaciones de modelos jerárquicos con certificación cruzada entre iguales puede resultar óptimo en las organizaciones en donde no es posible que un modelo de confianza se subordine a otro, una conexión de múltiples jerarquías gráficamente se muestra así:

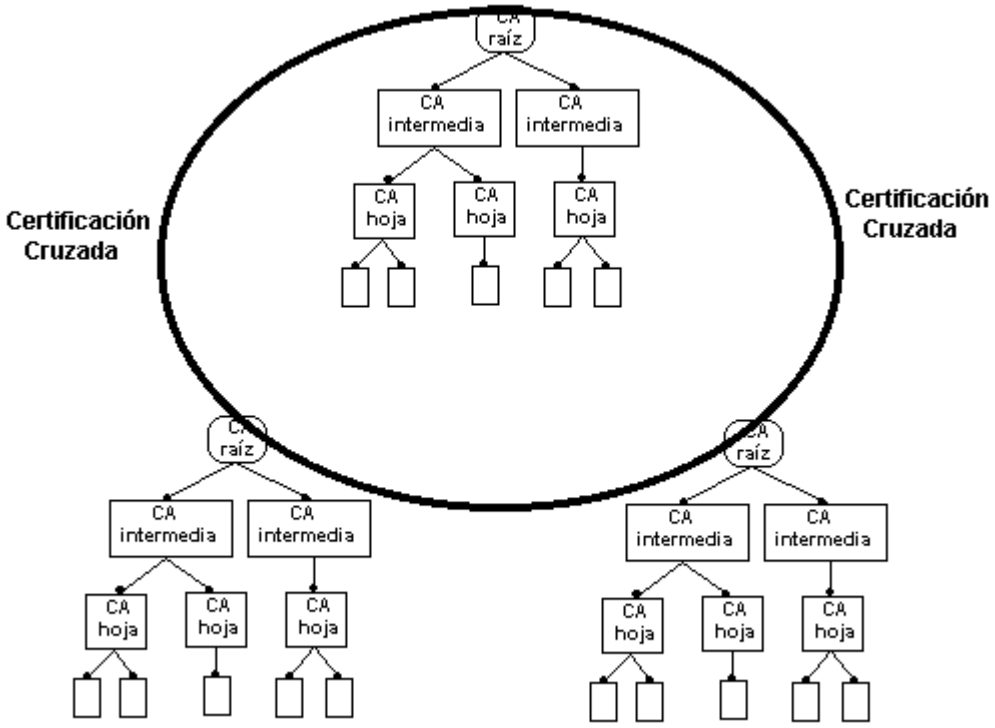

Figura 4.27

En este modelo cada Autoridad de Certificación raíz expide una certificación cruzada para formar un anillo. Esta es una opción cuando una organización tiene una modelo jerárquico y con el tiempo necesita de una certificación cruzada con otras organizaciones permitiendo unirse al modelo de confianza sin necesidad de una reestructuración. Existen otros modelos híbridos que básicamente se han desarrollan con los ya mencionados y que serán efectivos si se diseñan con los requerimientos de cada organización.

4) Manejo de Certificados, el ciclo de vida del certificado tiene varias etapas las que están primero bajo la responsabilidad de la Autoridad Certificadora (CA) que una vez emitida y en poder del usuario se será solamente su obligación mantenerlo. Para una buena gestión de los certificados se seguirán las siguientes etapas, pero se pueden incluir otras que el diseñador crea conveniente para su organización.

- El Formato del Certificado, se podrá emitir certificados para identidad personal, servidor, revocación o suspensión de clave, y de acuerdo a la organización y su ámbito de certificación podrá emitir certificados de autoridad de certificación y de participación en la jerarquía de autoridades de certificación.

  La solicitud de certificado de identidad personal básicamente contendrá datos: de la agencia de certificación, fecha de solicitud, datos del solicitante y de la clave pública. La solicitud de certificado de servidor tendrá: la fecha de solicitud, datos del servidor, de la clave pública y del solicitante. Para la revocación o suspensión de la clave los datos serán de la clave pública, fecha de expedición y validez de la clave, así como de la autoridad de certificación.

  La solicitud para certificados de autoridad de certificación contendrá la fecha de la solicitud, datos de la organización, datos del responsable técnico y de la clave pública. En la solicitud de participación jerárquica la

entidad interesada pondrá en conocimiento su interés de incluirse en su jerarquía, además de los datos del técnico responsable.

El certificado que se emita deberá contener datos del solicitante, de su clave pública e información adicional relacionada con la validez del certificado y de acuerdo a las políticas de certificación que cada organización establezca. Aunque cada organización podrá definir su formato de certificación el estándar X.509 v3 es una opción excelente y muy difundida en el entorno PKI permitiendo que cada organización defina sus propias extensiones con información específica necesaria para su ambiente de operación.

- La Generación del Certificado, está bajo la responsabilidad de la Autoridad de Certificación que a través de una entidad denominada Autoridad de Registro recepte y valide la solicitud. El proceso se inicia con el registro de la información que dependerá del solicitante que como ya se mencionó puede ser una persona, software o hardware que requiere de la certificación. La Autoridad de Registro se encargará recibir la solicitud y verificar físicamente la identidad del solicitante. Dicha solicitud será examinada por la CA y si todo está correcto se generará una clave pública y una privada que almacenada en un medio físico seguro se le entregará al solicitante. El certificado junto con la clave pública le será enviado mediante un e-mail.

- La Verificación del Certificado, para verificar que el certificado le pertenece a un determinado usuario es posible que exista una jerarquía de Autoridades de Certificación, de forma que la validación del certificado irá pasando de un nivel a otro hasta llegar a una CA que confirme que el certificado es válido. La CA verificará que el certificado no esté vencido o que se haya revocado.

Existen opciones para verificar un certificado pero la que cumple con los requerimientos de seguridad, autenticidad e integridad está dado por preguntar siempre a la CA a través de la última Lista de Certificados de Revocación (CRL) que dicho certificado es válido y de hecho se lo tomará así. Pero que sucede cuando al siguiente día el certificado que era válido aparece en la CRL, estas se situaciones se dan por lo que es conveniente que existan los documentos digitales llamados recibos. Este es un documento firmado digitalmente con la clave privada de una Autoridad de Fechado Digital que añade la fecha actual de los documentos que recibe para su certificación. Con esto los usuarios tienen un documento firmado con la hora y fecha exacta que envía o recibe un certificado digital.

- La Revocación del Certificado, anteriormente ya se mencionaron las razones por la que un certificado deber ser revocado pero es necesario recalcar que el usuario del certificado debe ser notificado ya sea off-line o por Internet (on-line) y luego publicarlo en la Listas de Certificados Revocados. Para la revocación se considerarán importantes dos fechas, la primera cuando el estado del usuario o el contenido del certificado ha cambiado, pues a partir de esa fecha el certificado se considera como no confiable, aunque la fecha en caso de una clave comprometida no se podrá determinar con seguridad. La segunda fecha identifica la última operación del certificado cuando era válido.

  Se deberá establecer el mecanismo de revocatoria para el certificado en caso de que un usuario lo solicite, generalmente se lo hace a través de una interfaz de la Autoridad de Certificación o de la Autoridad de Registro, tomando en cuenta que se necesita la autenticación del usuario que solicita la revocación, se pueden establecer formas de secreto compartido en el proceso de registro para que el usuario se autentique. Cuando un certificado es válido por seguridad el propietario puede pasarlo a un estado de suspendido en donde prevendrá su utilización. Entonces el certificado válido pasa a este estado cuando el propietario sabe que no va a utilizarlo

por un tiempo determinado y quiere garantizar que el certificado no se utilice por el lapso de ese tiempo

- Las Políticas de Certificación, contiene una secuencia de lineamientos definidos para el manejo de los certificados, es decir contendrá información acorde a la organización y al ámbito del diseño de la Infraestructura de Clave Pública. Se incluirá políticas de seguridad, definición de los períodos de validez de los certificados, la convención de nombres y el uso de las extensiones de los certificados. Todo esto conlleva un análisis de los recursos de la organización para garantizar a los usuarios el funcionamiento óptimo del diseño de la PKI.

  Las políticas de seguridad definidas para los certificados serán normas concretas que guiarán a los diferentes usuarios de la PKI para establecer el ciclo de vida del certificado, así como los tipos de certificados que se emitirá. En el período de validez de los certificados se definirá el tiempo por el cual será valido el certificado de acuerdo al tipo de usuario. Para la convención de nombres se establecerá los mecanismos para asegurar la unicidad de nombres necesarios para la certificación. En cuanto al uso de las extensiones de los certificados se presentarán como recomendaciones explicando cuales y como se utilizarán en los certificados.

  Este conjunto de normas tiene que prever todas las situaciones posibles y de cómo este evento ya sea crítico o no debe ser tratado y desde luego superado para normal operación de la PKI. A esto se lo denomina una Declaración de Prácticas de Certificados o Certificate Practice Statement (CPS). El CPS contiene una explicación detallada de cómo la Autoridad de Certificación gestionará los certificados que emite y otros servicios que relacionados con este. Además actúa como un acuerdo entre la CA y los usuarios describiendo obligaciones, limitaciones legales y los principios para verificaciones y auditorias posteriores. La política de certificados y la

CPS comúnmente se redactan con el personal del diseño de la PKI, el grupo de usuarios y personal jurídico

- La Cadena de Certificado, es el camino que recorre un certificado para ser verificado, es decir cuando un certificado llega a un usuario, éste deberá cerciorarse si conoce a la CA que la firmó, de no ser así se buscará hasta encontrar a una CA conocida o firmada por sí mismo. La cadena de certificado depende de los niveles de confianza entre las Autoridades de Certificación y la arquitectura que se haya implantado para la distribución del certificado. Para el diseño de esta arquitectura es necesario tener en cuenta las características tanto físicas como lógicas que posee la red, la distribución del personal necesario para el diseño de la PKI y el buen manejo de los certificados harán que las CA que se utilicen estén bien distribuidas y la organización esté acorde a sus funciones.

5) Protección de la PKI y almacenamiento de claves y certificados, es importante que la organización diseñe un mecanismo tanto de alarmas como de auditorias que prevenga y mantenga el trabajo de la Infraestructura de Clave Pública. Cada elemento de la PKI mantiene operaciones importantes que deben ser objeto de inspección a través de archivos logs, permitiendo indagar cualquier operación comprometedora para la seguridad de la PKI. La generación de pistas de auditoria mantiene un historial de los cambios en la información, permite saber que cambió, quién y cuando lo hizo, con el análisis de esta información se determinará el grado de afectación de la infraestructura.

La criptografía para PKI es fuerte, un certificado válido puede ser verificado ante una CRL, pero nada de esto es seguro si la clave privada es vulnerable a una copia o acceso. Entonces el usuario tiene que basarse en una autenticación fuerte para su clave privada. El diseñador tendrá que utilizar las principales técnicas de autenticación como: contraseñas, identificadores de prenda o tokens de autenticación, tarjetas inteligentes y la biometría. No existe una respuesta perfecta y única para cada organización, pues cada forma de autenticación tiene

niveles de seguridad, características propias de uso y diferentes costos de adquisición y administración. Se deberá considerar la mejor forma de autenticación que a cada organización le sea más factible de implementar y de acuerdo a los recursos que dispone.

4.3.1.4.- Protocolos de comunicación

Hasta la actualidad el área de estandarización de la tecnología PKI ha tenido grandes avances, el esfuerzo de organizaciones y grupos de gobierno por crear modelos operacionales que se acoplen con especificaciones PKI ha ida dando resultados, pues hoy tenemos varios estándares que facilitan los procesos de la PKI. El rendimiento de la Infraestructura de Clave Pública está directamente relacionado con los protocolos de comunicación que se utilice para los procedimientos que tendrá la PKI.

Una ves conocidos los servicios y funciones que se pretende otorgar, es oportuno definir los protocolos que se utilizarán para la comunicación y transportación de información valiosa para la PKI. El especificar el protocolo entre un usuario y la Autoridad de Certificación, en este caso para la generación de los nuevos certificados, la revocación, renovación y validación del certificado de la misma CA u otra diferente. El servicio de seguridad en la web requiere también de un protocolo que provea comunicación segura entre el cliente y servidor. Para la protección del correo electrónico también se requiere de un protocolo que proporcione confidencialidad, integridad, autenticación y no repudio de origen.

4.3.1.5.- Descripción de las Entidades

En este punto se debe tener claro las entidades que participan en la Infraestructura de Clave Pública, sin embargo definir las funciones de cada una ayuda a encontrar o reafirmar las operaciones que las entidades tendrán que cumplir. La funcionalidad de cada elemento permitirá conocer la interrelación de

los elementos y como se desempeñan en conjunto para principalmente gestionar el ciclo de vida de los certificados.

Una posibilidad es explicar las obligaciones de la Autoridad de Certificación, de la Autoridad de Registro y de los Propietarios de los diferentes certificados que se han expedido concretados en documentos escritos para la constancia de los compromisos que cada entidad aporta en el mantenimiento de la Infraestructura de Clave Pública. En el caso de que exista una CA firmada por la CA raíz se acoplará a las normas regidas por esta y principalmente deberá tener en cuenta las políticas de certificación de la Autoridad de Certificación raíz para ofertar sus servicios.

Así como se ha expuesto las obligaciones se tendrá que detallar las responsabilidades de cada una de las entidades mencionadas para garantizar el cumplimiento de las obligaciones expuestas y por lo tanto prevenir que las operaciones la PKI se vean afectadas por el mal uso especialmente de los certificados digitales emitidos por la CA.

4.3.1.6.- Interrelación con otras Infraestructuras de claves públicas externas

Interrelación con otras PKI, básicamente se refiere a las relaciones de confianza que establece una organización con otra similar en cuanto a los certificados que emite cada una. A esto se lo denomina modelo de confianza que son una directiva de seguridad, que incluso es más legal que técnico, si se decide confiar en los certificados de una CA externa necesitará de personal especializado que revise cuidadosamente los documentos de la CA y determine si la organización está en capacidad de soportar este modelo así como los productos que emitirá.

Cuando se ha fortalecido una PKI una comunidad puede requerir de un proyecto donde colaboren organizaciones similares que permitan un mayor desarrollo y presencia a nivel internacional. Cuando se plantea la posibilidad de utilizar una PKI externa se debe primero analizar la compatibilidad entre modelos para definir

la posibilidad de interrelacionarse, tener en cuenta los mismo pasos que la metodología desarrollada para probar la compatibilidad de las PKI que se quieren relacionar. Revisar cuidadosamente la declaración de las políticas y prácticas de certificación de esa CA externa.

Los procesos que cada PKI tiene pueden ser muy semejantes sin embargo se tendría que integrar la administración de los certificados y claves para dar un buen soporte de servicios a los usuarios. Se tendría que analizar el impacto que cada PKI tendría sobre la otra, pues las aplicaciones aumentarían la carga procesos en la infraestructura.

Si se quiere establecer relaciones de confianza con otras PKI deberá pensar en la satisfacción de los estándares de seguridad que tiene la organización propia y con la que se va a relacionar. Este tema a más de ser técnico es legal ya que podría estar conectándose con una entidad vulnerable a un fraude, robo y ataques de intrusos que destruirían la Infraestructura de Clave Pública. Cuando los aspectos legales estén confirmados se podrá tener en cuenta los siguientes métodos técnicos para establecer esa relación de confianza:

- Dos conjuntos de certificados, en donde el usuario tendrá un certificado de la propia CA y otro de la nueva CA. Esto conlleva costos altos de operación y posiblemente las organizaciones encuentren inconvenientes para verificar sus identidades y satisfacer los requerimientos de la CPS. Si las CA son grandes estas operaciones pueden ser no realistas.

- Establecer un modelo de confianza jerárquico, donde las dos CA establecen un nivel más alto de confianza, una CA raíz que firmaría su propia clave pública y sería un ancla de confianza para establecer un grupo y tener una PKI común.

- Varias raíces de confianza en cada aplicación, esto es que cada cliente tendría que modificar e incluir certificados raíz de confianza. Esto significa

que cada usuario tendría un certificado adicional de confianza, pero esto puede ser molestoso en los usuarios.

- Establecer un modelo de certificación cruzada, donde la CA raíz de una organización firme la clave pública de la otra y/o viceversa, es decir la certificación puede ser en una o dos direcciones. De este modelo resulta dos niveles de firmantes una CA raíz y dos subordinadas que firmarán los certificados del usuario.

- El diseñador estará en la capacidad de definir las relaciones con otras PKI y determinar si el elemento humano, tecnológico, material y legal está en capacidad de soportar e integrar una Infraestructura de Clave Pública en el futuro.

4.3.1.7.- Consideraciones sobre la inversión en PKI

Las consideraciones que se deben tomar en cuenta principalmente son el tiempo y el dinero que se invertirá en una tecnología como esta. Los productos y tecnologías que constituyen una PKI pueden ser no cuantificables puesto que los costos dependen del número de usuarios y de cómo ellos se desarrollarán en un tiempo determinado. Se debería incluir también costos de licencias, mantenimiento, actualización y soporte tanto del usuario como del proveedor de los servicios.

Se concebirá también el costo de las instalaciones para el funcionamiento de la PKI, además el costo por recuperación en caso de producirse algún desastre en las instalaciones. En organizaciones muy grandes existe la posibilidad de que la recuperación sea fuera de ese sitio, es decir una instalación adicional, que también tendrá que incluirse si fuese el caso. En cuanto al personal se incluirá el costo los servicios profesionales que se necesitarán para la planeación, organización, diseño, desarrollo, instalación, entrenamiento, administración y soporte de la Infraestructura de Clave Pública.

El costo para poner en funcionamiento una PKI implica muchos pasos que incluyen la preparación, planeación, diseño, desarrollo, instalación, entrenamiento, administración y soporte, pero tampoco se puede conocer su valor real, solo que una buena planeación en cada servicio o proceso que tanga la PKI será un punto a favor para el éxito de la Infraestructura de Clave Pública.

Estas son consideraciones que varían para cada organización pero pueden servir como guía de referencia para determinar el impacto en cuanto a costos que tendrá la PKI. El siguiente es un cuadro que permitirá conocer los aspectos involucrados en el valor que incluirá la tecnología PKI:

PRODUCTOS		INSTALACIONES	PERSONAL	PROCESOS
Clientes	Servidores	Instalaciones seguras	Equipo básico como: gerentes, administradores, etc.	Planeación
Software PKI	Software PKI	Instalaciones de recuperación	Equipo extendido como: desarrolladores, Especialistas, etc.	Diseño
Hardware PKI	Certificados PKI			Desarrollo
Mantenimiento	Hardware PKI			Distribución
	Mantenimiento			Administración

Tabla 4.2

1. Análisis de los Requerimientos Básicos	a. Los motivos para el diseño. Requisitos para el diseño de la PKI. b. Requisitos del usuario. c. Requisitos de seguridad de la PKI
2. Descripción de los servicios	a. Servicio de Administración del Ciclo de Vida de las Claves. b. Servicio de Administración de Certificados. c. Servicio de Listas de Revocación de Certificados (CRL).
3. Descripción de las herramientas y funciones para el desarrollo de los servicios de PKI	a. Manejo de Claves. b. Actualización de Claves. c. Modelos de Confianza de Autoridades de Certificación (CA). d. Manejo de Certificados. e. Protección de la PKI y almacenamiento de claves y certificados.
4. Protocolos de Comunicación	a. Definir los protocolos que se utilizarán para la comunicación y transportación de información valiosa para la PKI.
5. Descripción de Entidades	a. Explicar las obligaciones de la CA, de la RA y de los Propietarios de los certificados. b. Definir las responsabilidades de cada una de las entidades mencionadas para garantizar el cumplimiento de las obligaciones expuestas.
6. Interrelación con otras Infraestructuras de claves públicas externas	Establecer relaciones de confianza con otras PKI de acuerdo a estándares de seguridad de la organización propia con la que se relacionará. Tener en cuenta lo siguiente: • Dos conjuntos de certificados. • Establecer un modelo de confianza jerárquico. • Varias raíces de confianza en cada aplicación. • Establecer un modelo de certificación cruzada. • El diseñador estará en la capacidad de definir las relaciones con otras PKI
7. Consideraciones sobre la inversión en PKI	a. Productos. b. Instalaciones. c. Personal. d. Procesos.
ETAPAS DE LA METODOLOGÍA	

V. APLICABILIDAD DE LA METODOLOGÍA PARA EL DISEÑO DE UNA PKI EN LA ESPE-L

5.1.- ESTUDIO DE LA INFRAESTRUCTURA TECNOLÓGICA NECESARIA PARA APLICAR LA METODOLOGÍA DE DISEÑO DE PKI

5.1.1.- ANÁLISIS DEL ESTADO ACTUAL

El mundo en el que nos desenvolvemos dominado por Internet, el comercio electrónico con nuevas maneras de comercializar productos y servicios hace que la ESPE-L tenga que mantenerse a la vanguardia de estas nuevas tecnologías, este es el caso de la infraestructura de Clave Pública. Con la metodología propuesta es tiempo de analizar la situación de la ESPE-L para aplicar dicha metodología.

La ESPE-L es una organización dedicada a la educación superior, compuesta por alumnos, profesores y personal administrativo y de servicio que cuenta con una instalación tecnológica necesaria para la formación académica pero una Infraestructura de Clave Pública requiere elementos hardware y de comunicaciones adicionales que permitan generar y almacenar claves, así como la administración de los certificados. Además se requiere personal dentro del marco técnico y legal para proporcionar los servicios de la PKI.

Por lo tanto la ESPE-L para aplicar la metodología diseñada necesitaría de todos los recursos mencionados para captar usuarios no solo de la politécnica sino fuera de ella. Se deberá invertir en tecnología que permita soportar los servicios de seguridad que suministra una Infraestructura de Clave Pública

5.1.2.- INFRAESTRUCTURA TECNOLÓGICA NECESARIA PARA APLICAR LA METODOLOGÍA

Definitivamente una Infraestructura de Clave Pública agrupa elementos de hardware, software, comunicaciones, procedimientos y políticas que gestionan principalmente los certificados digitales y claves. Entonces para garantizar las funciones de la PKI en cuanto a hardware y comunicaciones se requerirá una conexión a Internet los 365 días al año, un equipo con capacidad de procesamiento y memoria altos, equipos de comunicación para redes, elementos para backups, UPS y equipos que mantengan el funcionamiento de la PKI.

En lo que se refiere a software se utilizará protocolos de comunicación seguros que cifrarán la información que maneja la PKI. En capítulos anteriores ya se han estudiado estos protocolos de los que se escogerán los más óptimos para acreditar los servicios de la PKI. Para establecer buenos niveles de seguridad a la PKI se tendrá que instalar un Firewall para la filtración de paquetes tanto de Internet como de la intranet, asimismo en la seguridad física se restringirá el acceso al personal. Con lo sugerido se establecerá una infraestructura de comunicaciones para el funcionamiento de la PKI y principalmente de la Autoridad de Certificación (CA).

Tomando en cuenta el número de usuarios de la comunidad politécnica se sugiere como punto importante dentro de la PKI utilizar sistemas y dispositivos de seguridad para almacenamiento de claves esencialmente privadas y de los certificados digitales. Contribuyendo así para el acceso rápido a los servicios que ofertar la Infraestructura de Clave Pública.

5.2.- ESTUDIO DE LOS REQUISITOS NECESARIOS PARA APLICAR LA METODOLOGÍA EN LA UNIVERSIDAD

Una Infraestructura de Clave Pública puede ser ajustable a la politécnica, aunque no tiene comercio electrónico tiene aplicaciones e información que

requieren los servicios de seguridad básicos: autenticación, integridad, confidencialidad y no repudio. Ésta infraestructura basada en criptografía asimétrica la que generará dos claves y que la pública junto con información adicional formará un certificado que identificará digitalmente a una persona.

Los beneficios que ofrece una PKI a nivel de usuarios geográficamente distantes pueden ser aplicado a la ESPE-L que aunque no va a ser lucrativa proveerá los servicios básicos de seguridad para aplicaciones propias de la comunidad politécnica, puesto que ellos se encuentran conectados a Internet mediante laboratorios y computadoras a las que tienen acceso personal docente y administrativo.

La ESPE-L cuenta principalmente con el apoyo legal, pues con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se puede dar inicio a la estructuración y creación de una Autoridad de Certificación (CA) que es el elemento principal en la PKI y la que proveerá los servicios y funciones definidos en la metodología. Con esto y la tecnología tanto en hardware como en software se puede iniciar el aplicativo que se quiere dar a la metodología.

La Escuela Politécnica del Ejercito sede Latacunga deberá contar mas que todo con los equipos para proveer los servicios de certificación y claves a la comunidad politécnica dentro de un marco legal y tecnológico para la Autoridad de Certificación (CA) raíz que para este caso será la misma universidad, por tanto será la promotora y creadora de las normas para las prácticas de certificación.

5.3.- DESARROLLO DE UNA PKI INICIAL PARA LA ESPE-L

Con la metodología desarrollada se inicia su aplicación, se definieron varios pasos los que permitirán guiarse para que la PKI en la ESPE-L tenga resultados reflejados en la seguridad de las aplicaciones que posee.

5.3.1.- ANÁLISIS DE LOS REQUERIMIENTOS BÁSICOS

5.3.1.1.- Motivos para el diseño

La ESPE-L cuenta con aplicaciones dirigidas a estudiantes y profesores que incluye servicios de consultas de notas, correo electrónico, ftp, web, biblioteca virtual y si se quisiera añadir otros como comercio electrónico el diseño de la PKI podría ser de más utilidad y se sacaría beneficio a sus funciones. Con esto se logrará los servicios de seguridad para los procesos de la politécnica y brindar mayor soporte de información al usuario.

Básicamente estas serían las razones para que la politécnica requiera de una PKI y para lo cual se generará una clave pública y otra privada y que cada poseedor tendrá que cuidar y administrar para evitar fallos en la infraestructura.

5.3.1.2.- Requisitos para el diseño de la PKI

El diseño de la PKI deberá ser muy amplia para permitir agregar nuevas aplicaciones que requieran de los servicios de seguridad. La arquitectura de la PKI y su funcionamiento será como se describe:

El servidor PKI que lo constituirá un servidor que contendrá los certificados válidos y firmados por la ESPE-L contendrá además un repositorio de los certificados emitidos renovados y revocados, las Autoridades de Registro que serán las secretarías de cada facultad que recogerán las solicitudes de certificación y verificarán físicamente a los usuarios de la comunidad politécnica.

Los clientes PKI serán las aplicaciones de que la ESPEL ponga a disposición a través de un browser. Los estudiantes tendrán sus claves de autenticación mediante el algoritmo de clave asimétrica El Gamal. Para los certificados se empleará el estándar X.509 y para su correcto funcionamiento existirá personal encargado de la administración del mismo.

La infraestructura de hardware para las comunicaciones de la Autoridad de Certificación (CA), la ESPEL, es semejante a un ISP debido a la información que almacena y por las posibles penetraciones que intrusos a través de Internet pretendan realizar. Actualmente la ESPE-L cuenta con dos subredes una Académica y una Administrativa que provee los servicios de Internet y aplicaciones de acuerdo a los departamentos. Básicamente la CA es un servidor que se encontrará ubicado en el departamento de Organización y Sistemas y a través del cual se generaran las claves y certificados a los usuarios de la comunidad politécnica.

Las redes a las cuales provee un servicio de Internet se encuentra protegida por un firewall además de otros elementos de comunicaciones que aunque no se observa en el gráfico son importantes para mantener un nivel de seguridad aceptable en la Infraestructura.

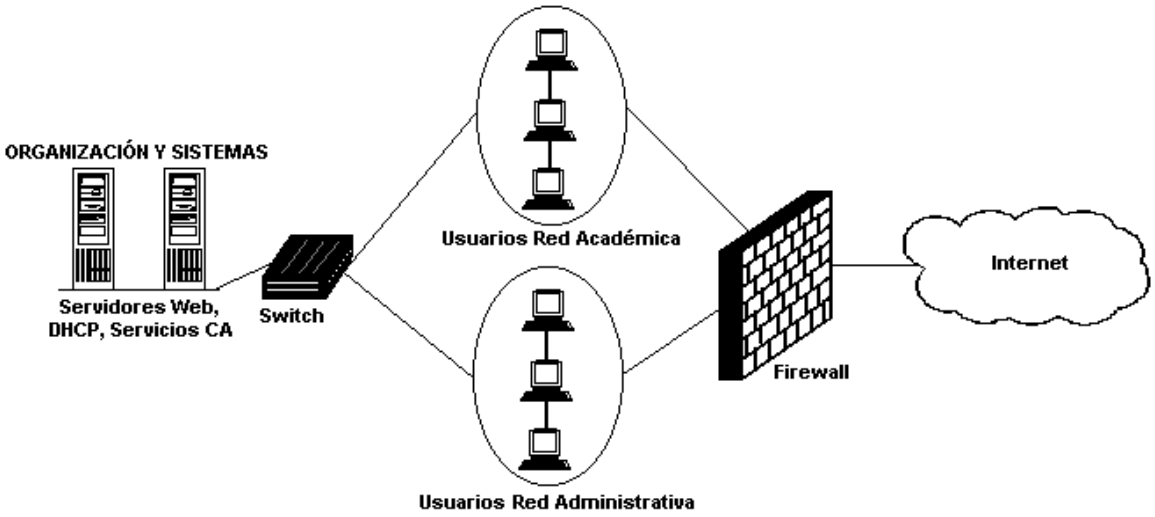

Figura 5.28

5.3.1.3.- Requisitos del usuario

Satisfacer al usuario que en este caso serán personas, es el principal objetivo de la PKI, por esto se los clasificará de acuerdo al nivel de acceso permitido a los recursos. La preparación al usuario debe ser previa e intensa para que el impacto de la tecnología no sea un obstáculo para la ESPE-L, en este caso los usuarios

serán los alumnos y docentes que geográficamente están cercanos a los servicios de la PKI, por lo tanto la identificación de estos será fácil. El número de posibles usuarios está directamente relacionado con el número de alumnos matriculados en cada período académico y de los docentes por el número de profesores a tiempo completo que se desempeñan en cada facultad de la ESPE-L.

La Infraestructura de Clave Pública cumplirá con las necesidades de seguridad que requiere la politécnica y permitirá que sus usuarios manejen los módulos implementados de acuerdo a los requerimientos de cada uno.

5.3.1.4.- Requisitos de seguridad de la PKI

Con la aplicación del algoritmo asimétrico El Gamal para la generación de claves y los certificados se ofertará confiabilidad al usuario, con la firma de documentos se establecerá autenticidad e integridad. En lo que se refiere a seguridad en las áreas aplicables a la PKI se observará mejor control de acceso a la información y desde luego autenticación para los niveles permitidos a cada usuario.

Plan de recuperación en caso de ataques o robos

El plan constituye varios recursos ideados para la ESPE-L con el objeto de mantener la “continuidad del negocio“, es decir en la medida de lo posible seguir brindando los servicios de la PKI. Es responsabilidad de la CA y sus entidades proteger los recursos e información de la PKI, para lo cual se tendrán medidas de prevención y de seguridad.

Medidas de Prevención:

- Mantener backups de los datos de la PKI para garantizar respuestas inmediatas a fallas técnicas.

- En lo posible mantener estos backups en un lugar de fuera del normal funcionamiento de la PKI, lo que funcionará después como Centro Alternativo de Proceso de Datos.
- Mantener una buena distribución física de los equipos computaciones y de comunicación, además de una correcta ventilación.

Medidas de Seguridad

Seguridad física en lo que es control de accesos y elementos de emergencia.

- Mantener la integridad del personal de comunidad politécnica a través de elementos como extintores y medicamentos de emergencia.
- Permitir el acceso al personal permitido en cada área.

Seguridad de datos

- A través de los servicios que ofrece la PKI.
- Clasificar la información de acuerdo al grado de sensibilidad y determinar su grado de protección.
- Mantener una bitácora del acceso de usuarios a los archivos.
- Es recomendable implementar la segregación de funciones.

Recuperación en caso de ataques o fallas

Evento	Solución
Perder la clave pública.	Dar aviso a la CA para dar de baja la clave y el certificado respectivo.
Se han comprometido las claves por un ataque de criptoanálisis.	La CA revocará los certificados y deberá generar nuevamente las claves.
La CA revoca los certificados	Publicar inmediatamente la lista de revocación de certificados y dar a conocer los usuarios.

Fallas en el del adaptador de red o placa base del servidor de CA.	Verificar rápidamente y de ser necesario reemplazar los elementos dañados y reiniciar el equipo para restaurar los servicios de la PKI.
Fallas en el disco duro del servidor de la CA.	Reemplazar y restaurar el servidor a partir de una copia de seguridad reciente.
Fallecimiento o incapacidad del titular del certificado.	Revocación inmediata del certificado.
Jerarquía de CA comprometida	Renovar claves y certificados, enviarlos a los usuarios correspondientes para reestablecer la jerarquía de certificación.

Tabla 5.3

5.3.2.- DESCRIPCIÓN DE SERVICIOS

5.3.2.1.- Servicio de Administración del Ciclo de Vida de las Claves

Más que un servicio será una responsabilidad de la PKI ofrecer éste servicio, de acuerdo al soporte de hardware de la politécnica se ha decido por un sistema centralizado en donde las claves se generarán en un punto central a través de los algoritmos mencionados y serán proporcionados a cada uno de los usuarios personalmente debido al entorno en donde se desenvolverá la PKI. Este será la definición de protección que se le darán a las claves durante su transportación al usuario final.

El sistema de recuperación para claves actuales, anteriores o antiguas no será necesario implementarlo y en el caso de que existan claves comprometidas se generará un par nuevo. En cambio es importante mantener un archivo log para posibles auditorias o para determinar accesos no autorizados.

5.3.2.2.- Servicio de Administración de Certificados

Este servicio es vital para la PKI incluye el registro para la certificación y se lo hará por medio de una solicitud a la Autoridad de Registro (RA) en este caso las secretarías de cada facultad de la ESPE-L. El usuario que requiere de certificación personal podrá identificarse físicamente ante las secretarías. No será necesario una Proof of Possession (POP) o Prueba de Posesión de la clave privada correspondiente a la pública ya que este será de manejo cuidadoso y riguroso por el personal que genera y distribuye las claves a los usuarios.

Para la renovación del certificado primero tiene que expirar el que ha estado siendo utilizado, se actualizarán los datos de ser necesario y con ello se generarán nuevas claves para el usuario, para evitar que se creen diferentes tipos de certificados que en el caso de la ESPE-L este procedimiento será más efectivo. En cuanto a la Revocación del certificado se lo realizará porque la clave del usuario se encuentra comprometida o por que ha dejado de pertenecer a la ESPE-L, para lo cual será notificado a través de las secretarías de cada facultad.

La publicación de los certificados revocados se darán a conocer a través de Internet, aunque esto no es vital para la politécnica pues no se están realizando transacciones financieras grandes con los certificados emitidos y no repercutirían el funcionamiento de la PKI. Para un proceso de auditoria se requiere de una entidad registradora de eventos que evidencie los procesos de las entidades involucradas, la CA y usuario final.

5.3.2.3.- Servicio de Lista de Revocación de Certificados (CRL)

Este servicio permitirá la notificación de los certificados revocados se utilizará una CRL simple ordenada por fecha para una mejor búsqueda de certificados, este tipo de CRL se ajusta más a la ESPE-L que aunque no es necesario, es un servicio básico e importante dentro de la PKI.

5.3.3.- DESCRIPCIÓN DE LAS HERRAMIENTAS Y FUNCIONES PARA EL DESARROLLO DE LOS SERVICIOS DE PKI

5.3.3.1.- Manejo de claves

Para la generación de claves se ha escogido El Gamal pues soporta claves de cifrado y firma digital. La CA será la encargada de crear el mecanismo para generar las claves y por medio del personal autorizado entregarla a cada usuario de la ESPE-L, esto a través de un contacto físico con el usuario, evitando que personas no autorizadas tengan la clave y perjudiquen el funcionamiento de la PKI.

5.3.3.2.- Actualización de las claves

La actualización de las claves se realizará anualmente para los usuarios que sigan perteneciendo a la politécnica, en el caso de un nuevo periodo académico en donde habrá el ingreso de nuevos alumnos y el retiro o egreso de los mismos, a los primeros se les generará un par nuevo de claves y su tiempo de valides será el mismo. Para los que dejen de pertenecer a la ESPE-L la revocatoria de los certificados y claves será inmediata, al igual que para los docentes.

5.3.3.3.- Modelos de Confianza de Autoridades de Certificación (CA)

La ESPE-L por su estructura organizacional jerárquica requiere de un modelo de confianza Jerárquico Subordinado en donde la CA raíz será misma politécnica y la que firmará los certificados de alumnos y docentes. Subordinadas a la CA raíz estarán cada una de las facultades que son las Autoridades de Registro.

En caso de que la ESPE-L quiera formar parte de otra CA fácilmente podrá incluirse en el modelo como una CA hoja o mediante certificación cruzada formando así un modelo híbrido. La comunicación estará en todos los niveles y se manejará de acuerdo a las políticas de certificación que emita la politécnica.

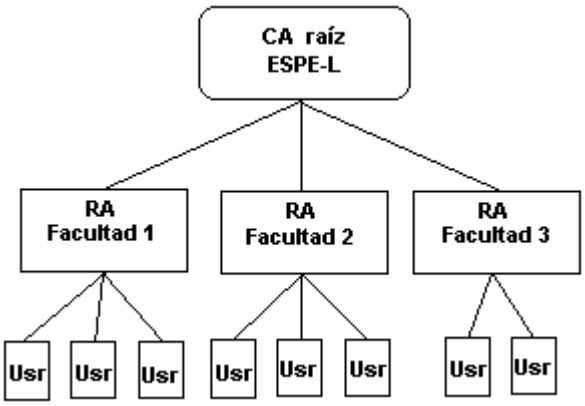

Figura 5.29

5.3.3.4.- Manejo de Certificados

Los certificados que la ESPE-L manejará deben contar con las siguientes etapas para que sean reconocidos y utilizados adecuadamente.

1) El Formato del Certificado, se emitirá certificados para identidad personal y de revocación y suspensión de clave. El formato del certificado para identidad personal y de la solicitud de revocación o suspensión de la clave contendrá los datos que se sugiere en la metodología mostrándose como un documento para ser proporcionado a los usuarios y se encuentra en el Anexo 1 y 2 respectivamente. Para la emisión de los certificados se utilizará el formato del estándar X.509 v3.

2) La Generación del Certificado, como ya se mencionó las secretarías de cada facultad serán las Autoridades de Registro y las que receptarán la solicitud para la certificación de Identidad Personal.

Certificados de Identidad Personal

- El solicitante del certificado se presentará con las siguientes credenciales cédula de identidad y carnet de la ESPE-L ante la RA para verificar su identidad así como la autenticidad y validez de las credenciales.

- La RA comprobará la existencia de una relación académica que vincule al solicitante con la ESPE-L.
- LA CA (servidor) generará un par de claves. La privada será entregada sin que la RA la conozca, mientras que la pública será un certificado digital en poder la Autoridad de Certificación para ser publicada.
- La solicitud (documento) será archivada por la Autoridad de Registro que previamente tendrá que pedir al solicitante ponga su firma manuscrita así se verificará que corresponda con la presentada en la credencial. Luego se procederá con el sellado de la solicitud.
- Con lo que se considera que el solicitante posee el certificado de identidad personal como un miembro de la ESPE-L. En caso de expiración del certificado se notificará vía e-mail al usuario para la actualización de datos y un nuevo proceso de generación del certificado.

3) La Verificación del Certificado, para tomar como válido un certificado y saber que cumple con los requerimientos de seguridad se recurrirá a una última actualización de la Lista de Certificados Revocados. Como no se está realizando transacciones financieras con esto se obtiene un grado de seguridad óptimo permitiendo a los integrantes de la comunidad politécnica involucrarse con la tecnología.

4) La Revocación del Certificado, el mecanismo de revocación del certificado de Identidad Personal a petición del titular se realizará a través de la solicitud con el formato antes especificado, el proceso será el siguiente:

- El titular del certificado junto con las credenciales mencionadas se presentará ante la Autoridad de Registro para verificar la autenticidad e identidad del solicitante.
- Confirmada la identidad del solicitante deberá llenar la solicitud para que sea almacenada.
- La RA comprobará el estado del certificado del solicitante.

- La RA enviará la solicitud revocada a la CA para que sea incluida en la CRL.

5) Las Políticas de Certificación, de acuerdo al ámbito de certificación de la ESPE-L se establecerá las siguientes políticas de certificación.

Políticas de Seguridad

- La ESPE-L como Autoridad de Certificación podrá emitir certificados digitales de identidad personal únicamente para la comunidad politécnica.
- Podrán acceder a la generación de claves y certificados los miembros de la comunidad politécnica que estén legalmente relacionados con las actividades académicas o administrativas.
- La única forma para obtener un certificado será expresamente como se indicó en la generación del certificado.
- Para la revocación de un certificado se procederá de acuerdo a lo establecido en el parte de manejo del certificado.

Período de validez de los certificados

- El período por el cual será válido un certificado de identidad personal en el caso de los alumnos está relacionado con el tiempo que dure el período académico.
- Para el personal docente, administrativo y de servicio el período de validez no sobrepasará un año, en el caso de realizarse contrataciones de personal el período de validez será igual al tiempo que dure el contrato.

Convención de nombres

- La ESPE-L como Autoridad Certificadora establecerá los Distinguished Names (DN) de para emitir los certificados digitales.

- Los certificados emitidos por ESPE-L tendrá como DN a los campos especificados en formato X.509 v3.

Extensiones del estándar X.509

- netscapeRevocationURL, determina la URL donde se encuentra la Lista de Certificados Revocados (CRL) de la ESPE-L.
- netscapeCAPolicyURL, determina la URL donde se encuentra la Declaración de las Prácticas de Certificados (CPS) de la ESPE-L.
- AuthorityKeyIdentifier, identifica la clave pública correspondiente a la privada utilizada para firmar el certificado.

6) La Cadena de Certificado, la ESPE-L es la Autoridad de Certificación raíz donde los niveles de confianza se limitarán a cada una de las facultades de la comunidad politécnica entonces la cadena de certificación se reduce por el número de alumnos y sus facultades. Lo mismo ocurre para el personal docente administrativo y de servicio.

5.3.3.4.- Protección de la PKI y almacenamiento de claves y certificados

El almacenamiento de claves públicas y certificados se mantendrá a través de un servidor que será el mismo que genere las claves. Por lo tanto este es el punto más sensible de la PKI y por ende el que más seguridades físicas y lógicas tendrá. En lo que se refiere a la clave privada se utilizará mecanismos de acuerdo a la capacidad de adquisición de la ESPE-L.

5.3.4.- PROTOCOLOS DE COMUNICACIÓN

Para realizar comunicaciones seguras a través de la web se ha decido por el estándar SSL (Secure Socket Layer) que es soportado por la mayoría de navegadores y servidores web. Para mantener seguridad en correo electrónico se

ha decidido por el S/MIME que cubre los requerimientos de seguridad de la ESPE-L.

5.3.5.- DESCRIPCIÓN DE ENTIDADES

Las entidades que ofertarán los servicios de PKI a la comunidad politécnica y sus obligaciones y responsabilidades se expresan a continuación.

Obligaciones de la Autoridad de Certificación (CA)

- Ofertar y mantener la infraestructura necesaria para la certificación.
- Cumplir con los requerimientos de los servicios básicos de seguridad a la comunidad politécnica.
- Generar los certificados de acuerdo a lo establecido en las Políticas de Seguridad.
- Mantener actualizada las CRL para que el usuario acceda a información rápida y actualizada.
- Revocar los certificados con el procedimiento especificado en el documento de las Políticas de Seguridad.
- Proteger los datos de la comunidad politécnica de acuerdo a las leyes establecidas en el Ecuador.

Obligaciones de la Autoridad de Registro (RA)

- Identificar y autentificar a los usuarios para generación o revocación de un certificado de acuerdo a lo antes establecido.
- Verificará que las solicitudes tanto de generación como de revocación estén con datos reales para generar las claves y certificado.
- Protegerá los datos de los solicitantes y no podrá concederlos a terceros sin autorización, esto de acuerdo a las leyes ecuatorianas.

Responsabilidades de la Autoridad de Certificación (CA)

- La ESPE-L como Autoridad de Certificación garantiza el cumplimiento de las obligaciones expuestas anteriormente.
- La ESPE-L se responsabiliza por cualquier fallo en el procedimiento para la generación, actualización o revocación de los certificados.
- Además es responsable por algún incidente provocado en la generación o renovación de las claves y de su notificación a los usuarios respectivos.
- Es responsabilidad de la CA si la su clave privada ha sido comprometida.

Responsabilidad de la Autoridad de Registro (RA)

- La RA es responsable de la correcta identificación de usuarios de la comunidad politécnica tanto para la generación o renovación de claves y de la generación o revocación de los certificados.

5.3.6.- INTERRELACIÓN CON OTRAS INFRAESTRUCTURAS DE CLAVES PÚBLICAS EXTERNAS

La ESPE-L por el momento no requiere de una interrelación con otras PKI. Pero si fuere el caso se recomendaría que se anexe a una Autoridad de Certificación con un ámbito mayor que le permita certificar su clave y a su vez pueda a través de ésta certificar a la comunidad politécnica. Su estructura no tanto física como lógica podría acoplarse a la nueva PKI.

Los procedimientos básicamente serían los mismos por lo que no existirían cambios drásticos y su impacto sería mínimo, pues al estar involucrados con la tecnología las entidades, servicios, políticas y procedimientos de la PKI en la ESPE-L favorecerían para mejorar los servicios de seguridad en Internet. En caso de que este punto se haga realidad se analizarán los métodos técnicos que recomienda la metodología para que las relaciones de la PKI puedan integrarse y funcionar apropiadamente.

5.3.7.- CONSIDERACIONES SOBRE LA INVERSIÓN EN PKI

Esta tecnología requiere de una inversión y de acuerdo a la metodología se sugiere aspectos en donde el costo de los productos tanto para clientes como servidores puede ser no cuantificable, es necesario considerar lo que se tiene y lo sea necesario adquirir para la Infraestructura de Clave Pública.

El personal requerido para la aplicabilidad de la PKI puede estar especificado en este capítulo, sin embargo se puede mencionar la necesidad de administradores tanto para la generación o renovación de la clave así como para la generación, revocación o suspensión de los certificados. Así como el personal que realice las funciones de Autoridad de Registro. Además de los desarrolladores y especialistas que pongan en funcionamiento el diseño de la PKI. En lo que se refiere a procesos de la PKI su costo puede ser intangible lo que si se puede determinar es su valor en cuanto a seguridad para la comunidad politécnica.

Se puede realizar un análisis estimado sobre la inversión que la ESPEL realizaría en una PKI, de lo que se ha obtenido el siguiente cuadro:

Costo de implementación de una Infraestructura de Clave Pública (PKI) en la ESPE-L

			Costo
Productos	Servidores	Servidor para autenticación, certificado, directorio. Hardware de servidor PKI.	1,500 150
		Subtotal	**$1,650**
Personal	Básico	Jefe de proyecto.	2,000
	Extendido	Especialistas redes. Especialistas seguridades. Especialistas algoritmos.	800 800 800

		Subtotal	**$4,400**
Procesos	Planeación	Dos Analistas	800
	Diseño	Dos Ingenieros	1,000
	Desarrollo	Dos Programadores	1,200
		Subtotal	**$3,000**
		TOTAL	**$9,050**

Tabla 5.4

NOTA: En los procesos de Planeación, Diseño y Desarrollo se define el personal necesario para la implementación de la PKI. En cuanto a la administración de la PKI será responsabilidad del personal del departamento al que fuere asignado manejar sus servicios, herramientas y demás.

En lo que se refiere al tiempo y lo que se incluye en cada proceso de Planeación, Diseño, Desarrollo y Administración se puede explicar en el siguiente cuadro:

			Tiempo Estimado (días)
Planeación	Validación de los requerimientos de la PKI. Estandarización del proyecto. Desarrollo de planes de pruebas, de operación y administración.	Intervienen los dos analistas	10 5 5
	Tiempo parcial		20
Diseño	Diseño de la arquitectura, administración, servicios y operaciones definidas en la metodología.	Intervienen los dos ingenieros	25
	Tiempo parcial		25
Desarrollo	Desarrollo de los componentes de la PKI.	Intervienen los dos programadores	30

	Probar los procesos de administración del usuario final.		10
	Tiempo parcial		40
	Tiempo Total		85

Tabla 5.5

NOTA: El proceso de administración de ejecutará cuando las procesos de desarrollo haya terminado y este en perfecto funcionamiento.

El tiempo estimado para la ejecución de los procesos es de 80 días y están distribuidos de la siguiente forma:

Tiempo(días)	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80
Planeación																
Diseño																
Desarrollo																

Tabla 5.6

5.4.- CARACTERIZACIÓN DE LA SEGURIDAD QUE OFRECE ESTE ESQUEMA A LA UNIVERSIDAD

Muchas organizaciones han visto ventajas reales al incorporar una PKI a su organización y que la ESPE-L pueda beneficiarse de un entorno de red confiable y que sus miembros puedan obtener comunicaciones seguras bajo los servicios básicos de seguridad que mejore sus aplicaciones.

La ESPE-L como centro educativo debe estar permanentemente actualizándose, tecnología como la que se está proponiendo permitirá tomar medidas de seguridad apropiadas para que los recursos como información académica de los alumnos no sea manipulada en beneficio o perjuicio de la comunidad politécnica.

No es fácil precisar cuando ocurrirá un evento que ataque directamente a la información que la politécnica maneja, los elementos que intervienen en una PKI y los servicios que cada uno brinda permitirán crear un modelo de seguridad con la misma confianza del mundo físico al que la mayoría ha estado acostumbrado para realizar transacciones comerciales.

El Internet trajo muchas tecnologías al alcance de todos sólo es necesario que la ESPE-L la convierta en realidad y como se ha probado en otros países cualquier organización que ignore este tema no podrá sobrevivir en mundo del comercio electrónico. El grado de efectividad de los elementos, políticas y servicios de la PKI sólo se podrán medir cuando el diseño de la metodología expuesta se implemente y los resultados sean los esperados.

VI. CONCLUSIONES Y RECOMENDACIONES

6.1.- CONCLUSIONES

- Se ha podido determinar los requisitos en lo que se refiere a hardware, software y comunicaciones necesarios para el diseño de una Infraestructura de Clave Pública. La metodología pone a disposición opciones para el manejo y administración de cada una y para que las organizaciones interesadas en ésta tecnología las analicen y decidan por la que cumplan con los servicios básicos de seguridad.

- Se definieron las funciones y servicios que proporcionan los elementos que intervienen en una PKI. Cada uno complementa los servicios del otro y se relacionan de manera que el nivel se seguridad obtenido con ésta tecnología funcione perfectamente en organizaciones donde el comercio electrónico es su prioridad y por ende que la autenticación e identificación puedan ser tratados como en el mundo cotidiano donde las transacciones son hechas con personas físicamente presentes.

- El uso de una Infraestructura de Clave Pública en una intranet es necesario pues los recursos de la red necesitan de niveles para que se acceda sólo a la información permitida. Pero en el caso de Internet el uso de la PKI es obligatorio ya que es la única forma conocida hasta el momento que brinde el grado de seguridad en los negocios electrónicos y permita que entidades que no se han visto físicamente puedan comprar y/o vender productos o servicios confiando plenamente en que la información no será manipulada maliciosamente.

- El costo de inversión en una tecnología PKI puede ser un obstáculo para muchas organizaciones pero lo que principalmente se busca es disminuir los riesgos y en aspectos que vale la pena protegerlos, es decir información valiosa y que involucre transacciones de alto valor.

- Se reconocieron los fundamentos técnicos sobre los que está basado el diseño de una Infraestructura de Clave Pública y sobre los que se seguirán creando e implementando nuevas tecnologías para que de a poco el paradigma de la seguridad baya encontrando soluciones más sofisticadas creando una sociedad que utilice la PKI y sienta que realmente es útil.

- La aplicabilidad de la metodología para la ESPE-L tiene básicamente los servicios y elementos de la PKI, la forma en que podrían funcionar y ajustarse a las aplicaciones para proporcionar seguridad a los niveles permitidos a los usuarios.

6.2.- RECOMENDACIONES

- Los pasos definidos en la metodología del diseño de una Infraestructura de Clave Pública no son obligados y está abiertos para que otros diseñadores agreguen lo que crean conveniente para sus organizaciones, lo definido es solamente un guía que puede ser objeto de mejoramiento debido a que cada momento aparecen nuevas tecnologías y estándares involucradas con la PKI que hacen que éste esquema sea más fuerte.

- Es importante que la Autoridad de Certificación en este caso la ESPE-L pueda formarse legalmente y una manera de hacerlo sería formado parte de una red de CAs, es decir permitir que las claves sean firmadas por una Autoridad de Certificación reconocida a nivel mundial, para que los servicios puedan ser utilizados en Internet.

- Implementar la PKI es importante para la politécnica pues los beneficios que traería esta tecnología son notables y que tendrán que ser evaluados constantemente y de ser necesario agregar nuevos estándares para su mejor funcionamiento.

REFERENCIAS BIBLIOGRÁFICAS

SIYAN K: Firewalls y la Seguridad en Internet, Prentice Hall Hispanoamericana S.A., México, 1996.

COBB S: Manual de Seguridad para PC y Redes Locales, Mc Graw-Hill/Interamericana de España S.A., Madrid, 1994.

NASH A, DUANE W, JOSEPH C, DEREK B: PKI Infraestructura de Claves Públicas, Mc Graw-Hill, Colombia, 2002.

REFERENCIAS WEB

http://www.nexor.com/public/rfc/index/rfc.html

http://www.microsoft.com/spain/technet/seguridad/pki.asp

http://www.um.es/si/ssl/PKI

http://www.eurologic.es/soluciones/Que-es-PKI.htm

http://www.nsa.gov:8080/

http://www.nist.gov/

http://www.rsa.com/

http://www.verisign.com/

ftp://ftp.upc.es/mirror/cert/info/orange-book/

http://www.iec.csic.es/criptonomicon/

http://www.iti.upv.es/seguridad/

http://www.reduy.com/computacion/ms-com-electronico/technet-1.htm

http://www.htmlweb.net

http://mx.geocities.com/fundamentosdeseguridad/SEMINARIO

www.caibi.org\ibst\index.htm

http://seguridad.diatel.upm.es

http://www.idg.es/iworld/articulo.asp

http://www.spain-lions.net/internet/comercio

http://webs.ono.com/usr016/Agika/3internet/seg_internet.htm

http://www.pki.gva.es

http://www.cetenasa.es/e-business/Talleres/taller1/book1.htm

http://www.microsoft.com/latam/technet/articulos/windows2k/chapt-12/

http://www.kriptopolis.com

GLOSARIO DE TÉRMINOS

Algoritmo de cifrado.- Fórmula o función matemática que se utiliza para cifrar información a través de métodos de factorización.

Autenticación.- Verifica la identidad a través de software o hardware como tarjetas inteligentes, dispositivos biométricos, etc.

Confidencialidad.- Asegura que solo las personas autorizadas tengan acceso a una determinada información.

Crackers.- Persona maliciosa que trata de destruir datos e información por cualquier medio sin consideración de los daños al sistema.

CRL(Certificate Revocation List).- Lista de certificados no válidos emitida por una Autoridad de Certificación.

Criptoanálisis.- Analiza un sistema criptográfico a través de conocimientos matemáticos para evitar o romper dicho sistema.

Criptografía.- Trata sobre la transformación de datos para hacerlos no legibles así como su proceso de restauración o de descifrado.

Criptología.- Ciencia que incluye la criptografía, el criptoanálisis entre otras.

DN (Nombre Distinguido).- En criptografía de Clave Pública cada persona debe tener un nombre único en el directorio. El DN es una cadena única integrada por múltiples atributos que como un todo identifican una entidad (usuario u organización).

E-commerce.- O comercio electrónico es la venta de productos y/o servicios así como los acuerdos económicos con los clientes se los hace a través de Internet.

FIPS(Federal Information Processing Standars).- Estándar Federal para el Procesamiento de Información. Es una norma del gobierno de Estados Unidos con requerimientos de seguridad para módulos criptográficos que se usen para proteger información no clasificada.

Firewall.- Aplica políticas de seguridad para restringir el acceso a datos hacia y desde una red protegiendo sus recursos de ataques de piratas informáticos.

Función hash.- Es una función de un solo sentido, resistente a colisiones que asocia un archivo o documento de longitud arbitraria a una cadena de longitud constante.

Hackers.- Es una persona que accede a los sistemas a través de Internet los explora poniendo a prueba sus conocimientos, su talento y capacidad.

Integridad.- Se refiere a los controles aplicados a los datos para asegurar que el contenido no sea modificado.

Irrenunciabilidad.- Denominada también no repudio, este servicio es aplicado cuando un usuario niega un mensaje transmitido.

Issuing Authorities.- Autoridades de emisión autorizadas por una Autoridad de Certificación raíz que funciona como terceras partes confiables, emitiendo, administrando, suspendiendo o revocando certificados de acuerdo con la práctica pública de dicha CA.

Lammers.- Persona joven con conocimiento básico de redes e informática llamada también falsos hackers.

LRA(Local Registration Authority).- Autoridad de Registro Local que cumple las mismas funciones de una Autoridad de Registro.

MAC(Message Authentication Code).- Código de Autenticación de Mensaje. Es una función que transforma una entrada de longitud variable mediante una clave secreta en un resultado de longitud fija que sirve como una huella digital, un MAC puede ser una Función Hash.

MD5.- Message Digest 5. Función hash desarrollada por RSA.

Phreakers.- Denominación que viene de phone cracker es una persona experta en sistemas telefónicos.

Protocolo (criptográfico).- Es la parte más visible de la aplicación y esta compuesto de esquemas criptográficos conjuntamente con otras operaciones que permiten proporcionar seguridad a una aplicación mas especifica.

PKI(Public Key Infrastructure).- Infraestructura de Clave Pública que utiliza cifrado asimétrico para emitir claves, certificados y firmas digitales entre otros servicios para proveer integridad, confidencialidad, autenticación y no repudio.

VPN(Virtual Private Network).- Red Privada Virtual. Utiliza un túnel cifrado por medio de una red pública para proporcionar privacidad junto con la red privada.

ANEXO 1

ESCUELA POLITÉCNICA DEL EJERCITO – LATACUNGA

SOLICITUD DE CERTIFICADO PARA IDENTIDAD PERSONAL

Fecha: .....
DATOS DEL SOLICITANTE
Apellidos: .....
Nombres: .....
E-mail: .....
Período Académico: .....
Facultad: .....
Nivel: .....
CI: .....
Propósito de la Clave:

- ☐ Autenticación de usuario
- ☐ Firma Digital
- ☐ Cliente HTTP

DATOS DE LA CLAVE PÚBLICA
Algoritmo: El Gamal
Fecha de generación: .....

DATOS DE VALIDEZ
Fecha de inicio: ..... **Hora:** .....
Fecha de caducidad: ..... **Hora:** .....

El solicitante declara que estos datos son verdaderos y se compromete a utilizar la clave pública y privada asociada para fines que se declaran. Además conoce y acepta la política de certificación de la ESPE-L y exonera de toda responsabilidad a ésta de cualquier perjuicio que pudieran causarse con esta clave.

El Agente de Registro El solicitante

ANEXO 2

ESCUELA POLITÉCNICA DEL EJERCITO – LATACUNGA

SOLICITUD DE REVOCACIÓN O SUSPENSIÓN DE CLAVE

Código de Identificación Secreto: .....
CI: .....
Fecha y validez de expendición:.....

En calidad de responsable de la Autoridad de Certificación de la ESPE-L y en representación de .....con domicilio en la ciudad de ..... provincia de .....
Notifica la revocación de la clave con los datos que se incluyen en este documento, y que esta acción tenga el efecto legal para las acciones de las claves, revocada por los siguientes motivos:
.....
.....
.....
.....

DATOS DE LA CLAVE PÚBLICA
Algoritmo: El Gamal
Fecha de generación: .....

DATOS DE VALIDEZ
Fecha de inicio: ..... **Hora:** .....
Fecha de caducidad: ..... **Hora:** .....

El Agente de Registro El solicitante