INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS ESTADO DE MÉXICO

PROGRAMA DE GRADUADOS EN INGENIERÍA Y CIENCIAS

MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

TESIS

"Estudio para la Implantación de una Autoridad Certificadora y su entorno."

Aspirante: SERGIO ARTURO PEREA PÁEZ

Asesor: Dr. LUIS ÁNGEL TREJO RODRÍGUEZ

Comité de Tesis: Dr. ROBERTO GÓMEZ C.

Dr. JESÚS VÁZQUEZ

Noviembre de 1999

Resumen

Este trabajo de tesis tiene como finalidad servir de guía para la implantación de una infraestructura de certificación para las organizaciones mexicanas, o en su caso poder montar una Autoridad Certificadora independiente.

En este trabajo se establecen los elementos necesarios para poder montar, administrar y operar una Autoridad Certificadora. Así mismo se especifican los Procesos de Certificación que debe seguir una Autoridad Certificadora para poder funcionar de manera adecuada.

Primeramente se hace la presentación de la teoría de Certificados Digitales. Esta teoría consiste en los fundamentos criptográficos de los Certificados Digitales, los cuales están dados en la criptografía de llave pública. Posteriormente se hace un estudio de los Certificados Digitales, desde el punto de vista criptográfico.

Como una de las partes más importantes de este trabajo, se plantea el cómo montar, administrar y operar una Autoridad Certificadora y se establecen sus Procesos de Certificación. Una vez expuesta la teoría acerca de la Autoridad Certificadora, ésta se adecua a la operación cotidiana de una organización y se utiliza una herramienta comercial (Servidor de Certificados de Netscape) como una opción de software práctica para implementar una infraestructura de Certificación.

Con la finalidad de resolver el problema de certificación del ITESM-CEM y con el objeto de servir como una aplicación práctica de este trabajo de tesis, se presenta el "Caso de estudio del ITESM-CEM", en el cual se busca implementar una infraestructura de Certificación a gran escala.

También se hace una breve presentación del protocolo SSL por su estrecha relación con el uso de Certificados Digitales. Y por último se presenta la reseña del trabajo práctico que sustenta gran parte de este trabajo de tesis, el cual fue realizado en el Departamento de Ciencias Computacionales del ITESM-CEM.

ÍNDICE

5. El Servidor de Certificados Netscape

ÍNDICE DE TABLAS Y FIGURAS

1. TABLAS

2. FIGURAS

INTRODUCCIÓN

La tecnología de Certificados Digitales no es muy popular en México, esto es debido a la dificultad que implica su implantación, operación y administración. Además de que requiere de conocimientos especializados base para poderse implantar, operar y administrar. Es objetivo de esta tesis acercar esta tecnología a las personas y organizaciones, para que puedan implantar una Infraestructura de Certificación (Autoridad Certificadora y manejo de Certificados Digitales).

Este trabajo está organizado en siete capítulos y un anexo, los cuales se distribuyen de la siguiente manera: En el capítulo uno, se plantea la problemática dominio de los Certificados Digitales, es el entorno y panorama general de la problemática que se puede resolver mediante el uso de Certificados Digitales.

En el capítulo dos, se presenta la teoría base que se requiere para poder comprender cómo se forma y funciona un Certificado Digital. Básicamente en el segundo

capítulo se presentan los criptosistemas de llave pública y los conceptos de autenticación y firma digital.

Para el tercer capítulo, se estudian los Certificados desde el punto de vista de un sistema criptográfico de llave pública, y se introduce el concepto de Autoridad Certificadora. También se estudian las características de un Certificado Digital, como su formato, tipos de Certificados Digitales, periodo de vida, utilización y su interacción con protocolos como SSL y S/MIME.

El capítulo cuatro es una de las mayores aportaciones de este trabajo de tesis, en él se expresa cómo instalar, administrar y operar una Autoridad Certificadora, que es el alma de la tecnología de Certificados Digitales. Además se plantean los Procesos de Certificación que debe guardar una Autoridad Certificadora. En este capítulo se plantea el Proceso de Certificación en su totalidad (ver "Una visión global de una Autoridad Certificadora, capítulo 4). También se estudia la adopción de la Infraestructura de Certificación dentro de una organización.

El quinto capítulo nos presenta una herramienta de software como opción para montar sobre ella una Infraestructura de Certificación. Esta herramienta es el Servidor de Certificados de Netscape, el cual es explicado a detalle debido a la dificultad que representa para su instalación, administración y operación.

Como otra destacada aportación de este trabajo de tesis, se presenta en el capítulo seis la recomendación para la Certificación de la comunidad del ITESM-CEM. Aquí se presentan los Procesos de Certificación que debe seguir la Autoridad Certificadora del ITESM-CEM para la administración y expedición de Certificados Digitales, así como el manejo de Certificados a gran escala.

En el capítulo siete, se presenta la descripción del trabajo práctico realizado para obtener gran parte de lo expresado en esta tesis. Por último se presentan las aportaciones de este trabajo de tesis en el apartado de "Resultados Obtenidos". En el anexo A, se hace una breve presentación del protocolo SSL, debido a su relación tan estrecha con los Certificados Digitales.

Capítulo 1

PLANTEAMIENTO DE LA PROBLEMÁTICA

1. Panorama General

En la actualidad las instituciones tanto públicas como privadas de México han comenzado a abrir sus redes locales para hacerlas formar parte de redes más amplias. En México existen grandes redes de extensión amplia (MAN) las cuales pueden conectar desde un campus de una universidad hasta localidades situadas en puntos lejanos dentro de la geografía nacional, como ejemplos tenemos a las redes de PEMEX, ITESM, SRE, etc.

La finalidad[1] de la apertura a redes de mayor extensión como Internet, por un lado es la de aprovechar la gran vitrina que significa la web para dar a conocer productos, promociones, proyectos, información de la empresa, servicios y hasta entretenimiento. Por otro lado se tiene la gran ventaja de que la institución se encuentra comunicada con

[1] Las ventajas de las redes de computadoras no son la meta de este trabajo, sólo se mencionan algunas en este documento como parte del contexto y con la finalidad de dar un panorama más amplio.

el resto del mundo a través de Internet y por lo tanto se puede hacer uso de servicios como correo electrónico, páginas de web, transferencia de archivos remota, utilización de computadoras y sus recursos remotamente, entre otros. Además las instituciones pueden aprovechar la infraestructura de Internet para montar una Intranet para manejo exclusivo de la organización, sin estar a la vista del resto del mundo.

Pero no necesariamente se tiene que estar conectado a Internet para trabajar con una red de extensión amplia, también se pueden tener redes privadas con infraestructura propia o rentada. Las cuales presentan ventajas para la parte operativa de la organización y muy probablemente se encuentren aisladas del resto del mundo porque es necesario que la información que por ésta fluye permanezca oculta para el resto del mundo. Aunque el tener una red con estas características no asegura que la información vaya a permanecer confidencial.

Pero más aún, no es necesario estar conectado a una gran red o a Internet para poder llevar a cabo trabajo en red. También se puede hacer dentro de una extensión reducida como lo puede ser la oficina misma, mediante una red local, que de la misma manera se puede aprovechar para llevar a cabo trabajo en equipo, intercambio de mensajes, transferencia de información, etc.

Es muy importante que la red sea una herramienta que ayude a la organización con su trabajo, le traiga beneficios tangibles y le facilite tareas, en pocas palabras que la red sea funcional. Pero un aspecto fundamental que va acompañado íntimamente con la funcionalidad de la red, es la seguridad de la misma. Ya que sin la seguridad, la red pierde parte de su funcionalidad al dejar de cumplir con algunos de sus objetivos, para muchos de los casos, que la red sea segura es fundamental para la organización por lo que si dicha red sufre de inseguridad ésta pierde totalmente su funcionalidad.

El concepto de seguridad en redes de computadoras es muy amplio, pero fundamentalmente se enfoca a la protección de los Activos Virtuales[1], que es toda la información generada en la organización la cual con el tiempo se torna más valiosa,

pasando de ser necesaria hasta indispensable, las bases de datos de nuestros clientes, facturación, estados de cuenta, etc. Información sin la cual simplemente no sabríamos que hacer. Otro activo virtual son las aplicaciones y programas para interpretar nuestra información. Muchas de las redes poseen debilidades que permiten que intrusos se puedan meter a nuestros sistemas. Si alguien se llegara a apoderar de nuestra información o a tomar control sobre nuestras aplicaciones, estaríamos en grandes problemas como organización y es aquí donde entran en función las medidas de seguridad computacional, preferentemente para prevenir porque ya una vez efectuado un ataque hay poco que hacer al respecto.

Como se ha podido plantear, la necesidad de proteger nuestros sistemas de red es inminente, pero estas necesidades difieren de acuerdo al contexto en que las organizaciones se encuentren. Además el campo de estudio de la Seguridad computacional es tan amplio que se tiene que seccionar para poder atacar adecuadamente los problemas que se presentan de una manera efectiva.

Este trabajo de tesis está enfocado al tratamiento de la seguridad computacional en el área de las comunicaciones seguras, específicamente en el tratamiento de Certificados Digitales y Autoridades Certificadoras como una solución en seguridad para las organizaciones mexicanas.

Por lo general las empresas mexicanas tienen que recurrir a contratar los servicios de consultores externos a la organización para resolver sus problemas de seguridad computacional. El documento que el trabajo de tesis arroje, servirá para que las empresas mexicanas puedan consultarlo y obtener de él, las soluciones que el manejo de certificados digitales y una Autoridad Certificadora les provee.

La importancia de éste trabajo de tesis es que las organizaciones de México contarán ahora con una guía en este ramo de la seguridad computacional que les va a permitir establecer un aparato complejo de implantación, manejo y operación de certificados

digitales con Autoridad Certificadora par su organización. Este complejo aparato, es lo que en este trabajo de tesis denominamos como *Infraestructura de Certificación.*

Además presentaremos un caso de estudio sobre una *Infraestructura de Certificación* a gran escala sobre el ITESM-CEM. Este caso de estudio arrojará aportaciones muy importantes para la implantación, operación y administración de una *Infraestructura de Certificación.*

También como parte del trabajo de esta tesis se presenta una herramienta de software como opción para montar sobre ella una *Infraestructura de Certificación.*

Al contar con este documento, las organizaciones que deseen adoptarlo, ahorrarán mucho dinero en costosas consultorías en la materia.

2. Problemática General de Inseguridad Computacional

Un aspecto fundamental en el área de seguridad computacional, es el saber perfectamente que clase de daño nos pueden hacer las personas que ilícitamente realizan actividades con nuestros sistemas. Estando conscientes del problema y sus consecuencias, las instituciones mexicanas pueden delimitar mejor cuáles son sus requerimientos en seguridad computacional, así como darle la real importancia al aspecto de la seguridad en su red, además de poder darles el panorama para tomar en cuenta algunos aspectos posiblemente olvidados.

Es indudable que así como las redes de computadoras son una herramienta muy útil para las organizaciones, también se pueden constituir en un instrumento u objeto en la comisión de actos ilícitos. Este tipo de actitudes del hombre, tiene sus orígenes desde el mismo surgimiento de la tecnología informática, ya que de no existir las computadoras, estas acciones no existirían. Por otra parte, la facilitación de tareas que trae consigo la utilización de redes de computadoras propician que, en un momento dado, el usuario se encuentre ante una situación de ocio, la cual trata de canalizar a través de las

computadoras cometiendo, a veces sin darse cuenta, una serie de ilícitos. En algunos casos el usuario establece una especie de duelo contra la computadora, lo cual también lo lleva a entrometerse en sistemas ajenos y muchas veces sin querer, a cometer ilícitos.

Por desgracia en nuestro país el hablar de delitos informáticos resulta un tanto sin sentido, ya que éstos no se encuentran contemplados en los textos jurídico-penales.

Los ataques informáticos se caracterizan por ser conductas de las llamadas de cuello blanco [2], ya que solo determinado número de personas con cierto nivel de conocimientos puede llegar a cometerlas. Además son acciones oportunistas, ya que se aprovechan de la infraestructura tecnológica de las organizaciones, que suele ser endeble. Por otra parte provocan serias pérdidas económicas, ya que por lo general producen grandes ganancias a quienes las realizan y ofrecen facilidades de tiempo y espacio, ya que en pocos segundos y sin una necesaria presencia física pueden llegar a consumarse.

Por desgracia son muchos los casos y pocas las denuncias debido a la falta de regulación por parte del derecho. Los ataques informáticos resultan ser muy sofisticados y presentan grandes dificultades para su comprobación. Estos actos pueden llegar a ser imprudenciales.

Los ataques informáticos ofrecen facilidades para poder ser cometidos por menores de edad y cabe mencionar que tienden a prolifera cada vez más y siguen siendo impunes ante la ley[1].

Los ataques informáticos producen un provecho para el autor y provocan un daño contra las computadoras conectadas a la red, a un individuo o grupo en su integridad física, honor o patrimonio. Es en estos últimos puntos donde los Certificados Digitales y las Autoridades Certificadoras ofrecen una importante solución.

Algunas de las acciones que se valen de las redes de computadoras como medio en la comisión de un ataque son: Falsificación de documentos (tarjetas de crédito, cheques, etc.), variación de los activos y pasivos en la situación contable de las empresas, planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc.), robo de tiempo de computadora, lectura, sustracción o copiado de información confidencial, modificación de datos tanto de entrada como de salida, aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (Caballo de Troya), variación del destino de pequeñas cantidades de dinero hacia una cuenta inexistente (Técnica de salami), uso no autorizado de programas de cómputo, introducción de instrucciones que provocan interrupciones o caída de un sistema, introducción de virus informáticos, acceso a áreas informatizadas en forma no autorizada, intervención en las líneas de comunicación de datos, destrucción de programas y daño a la memoria.

En nuestro país este tipo de ilícitos no están contemplados en nuestros códigos penales. Si bien es cierto que el nivel de informatización nacional no es tan pronunciado como en otros países, al menos es el suficiente como para un adecuado análisis y tratamiento por la vía del derecho. Habrá que revisar nuestro actual código penal que data de 1931 y que no contempla este tipo de manifestaciones tecnológicas ya que, por ejemplo, el introducirse por la red a un sistema y robarle tiempo de computadora no puede ser catalogado de la misma manera que un robo convencional.

3. Certificados Digitales

Servicios como el firmarse a un servidor, privacia de los mensajes, control de acceso, entre otros, son necesarios para salvaguardar la propiedad intelectual y asegurar comunicaciones confidenciales. Una buena opción para proveer éstos y otros servicios de seguridad son los Certificados Digitales.

Por mucho tiempo la autenticación de los usuarios y el control de acceso a diversos servicios de la red han estado basados en nombres de usuarios ligados con sus

respectivas contraseñas. Sin embargo este método tiene ciertas desventajas ya que las contraseñas son difíciles de administrar debido a que se tiene que mantener una base de datos con nombre del usuario/contraseña en cada servidor individual. Las contraseñas son difíciles de recordar[2]. Además suelen ser inseguras, ya que los métodos basados en contraseñas requieren de mandarla en texto claro por la red. En cuanto a la autenticación, las contraseñas suelen ser débiles ya que si alguien descubre el nombre de un usuario y su contraseña, es relativamente fácil acceder a datos como esa persona.

Un Certificado Digital es una especie de identificación digital para un usuario, servidor, equipo de cómputo o sistema. El Certificado no solo es utilizado para fines de autenticación sino también para aplicaciones de seguridad como integridad y privacidad de los mensajes, firmas digitales y encripción.

Los Certificados Digitales tienen muchas ventajas con respecto a las contraseñas: Los certificados son más robustos para la autenticación ya que requieren que el usuario tenga tanto el certificado como la llave privada, además de que debe conocer la contraseña de dicha llave. Los Certificados son información pública, así que los usuarios deben autenticarse sin la necesidad de mandar información sensible, como la contraseña, por la red. Aunque el certificado de un usuario fuera capturado en su camino por la red, quien lo robó no podría actuar como dicho usuario ya que no tiene acceso a su llave privada.

Para los administradores el manejo de certificados puede resultar más fácil, ya que en lugar de darle mantenimiento a una gran lista de usuarios/contraseña en cada servidor, los administradores pueden simplemente configurar un servidor para darle acceso solamente a los usuarios que presenten un certificado firmado y aprobado por una Autoridad Certificadora. Además los Certificados le permiten a los usuarios el recordar una sola contraseña para acceder a varios servicios.

Los Certificados están cubiertos bajo el estándar X.509 [3] y éstos pueden ser utilizados para proveer una autenticación robusta, así como firmas digitales y encripción. Los

[2] Los usuarios por lo general tienen que recordar más de diez contraseñas.

estándares abiertos permiten a las organizaciones proveer seguridad que incorpore a todas las aplicaciones cliente-servidor a lo largo de toda la organización. Los certificados X.509 permiten a la organización tener comunicación autenticada y privada con gente fuera de la misma institución.

Los Certificados Digitales tienen un gran número de aplicaciones, algunas de ellas son: Los usuarios de Internet, Intranets o Servidores, usan certificados cuando se comunican usando el protocolo SSL [4] (Ver **anexo A**). Los Certificados pueden efectivamente remplazar múltiples contraseñas ya que el usuario solo tiene que recordar la contraseña para tener acceso a la llave privada. Los certificados pueden ser utilizados también en protocolos de correo electrónico seguro, como S/MIME [5] (Secure Multiporpuse Internet Mail Extensions).

Los certificados deben tener una fuente la cual es la Autoridad Certificadora. Una Autoridad Certificadora debe mantener su responsabilidad con las partes que han confiado en ella, esta responsabilidad está acotada por las políticas individuales que cada autoridad establezca, las cuales son materia de estudio de este trabajo de tesis.

4. Problemáticas Dominio de los Certificados Digitales

4.1 Problemática del correo electrónico

El coreo electrónico es una de las herramientas más innovadoras de la actualidad, esté se ha convertido en un medio de comunicación muy popular alrededor del mundo. Tener acceso a una cuenta de correo electrónico es muy sencillo, uno puede tener cuenta de correo electrónico provista por su empresa, escuela o por medio de un proveedor de servicios de Internet. Si no se cuentan con correo electrónico por alguno de estos medios uno puede tramitar una cuenta de manera gratuita en diversos sitios web.

El crecimiento en el uso del correo electrónico ha sido tal, que ahora es normal que una persona tenga una cuenta de correo electrónico y la use de importante manera para mandar y recibir mensajes.

Originalmente el correo electrónico se usaba como medio para intercambiar mensajes, era como mandar una carta por el correo convencional, con la ventaja de que es más rápido y uno puede estar comunicado con todo el mundo a través del correo electrónico de Internet. Pero con el paso del tiempo el correo electrónico se ha vuelto una herramienta para intercambiar información y es posible enviar, anexados al mensaje, archivos generados por nuestras aplicaciones de uso diario, pudiendo contener información importante o confidencial.

Es muy probable que el medio oficial de comunicación dentro de una organización se vuelva el correo electrónico dentro de muy poco tiempo, de hecho ya hay organizaciones que así lo hacen. Pero así como su uso ha proliferado, los usuarios también han aprendido a hacer mal uso de este recurso, es por ello que se deben tomar medidas para proveer seguridad en el manejo del correo electrónico.

Por lo general el correo electrónico se maneja utilizando el software incluido en el navegador de Internet (Aunque existen otras maneras para acceder al correo electrónico, ésta es la forma más sencilla y popular). Para que uno pueda hacer uso del correo electrónico por este medio, sólo hace falta configurarlo con nuestra información de la manera correcta, proceso que es en extremo sencillo.

En la sencillez del proceso de configuración del correo reside la peligrosidad ya que alguien, de manera maliciosa, puede configurar un navegador a nombre de otra persona y usurpar su personalidad para mandar correo electrónico (Ver figura 1). La única información que requiere el infractor para cometer tal ilícito es conocer la dirección de correo electrónico de la otra persona, cuestión que no es difícil de llevar a cabo ya que por lo general se conoce a la persona que será víctima del ataque, además las direcciones de correo electrónico son fáciles de deducir.

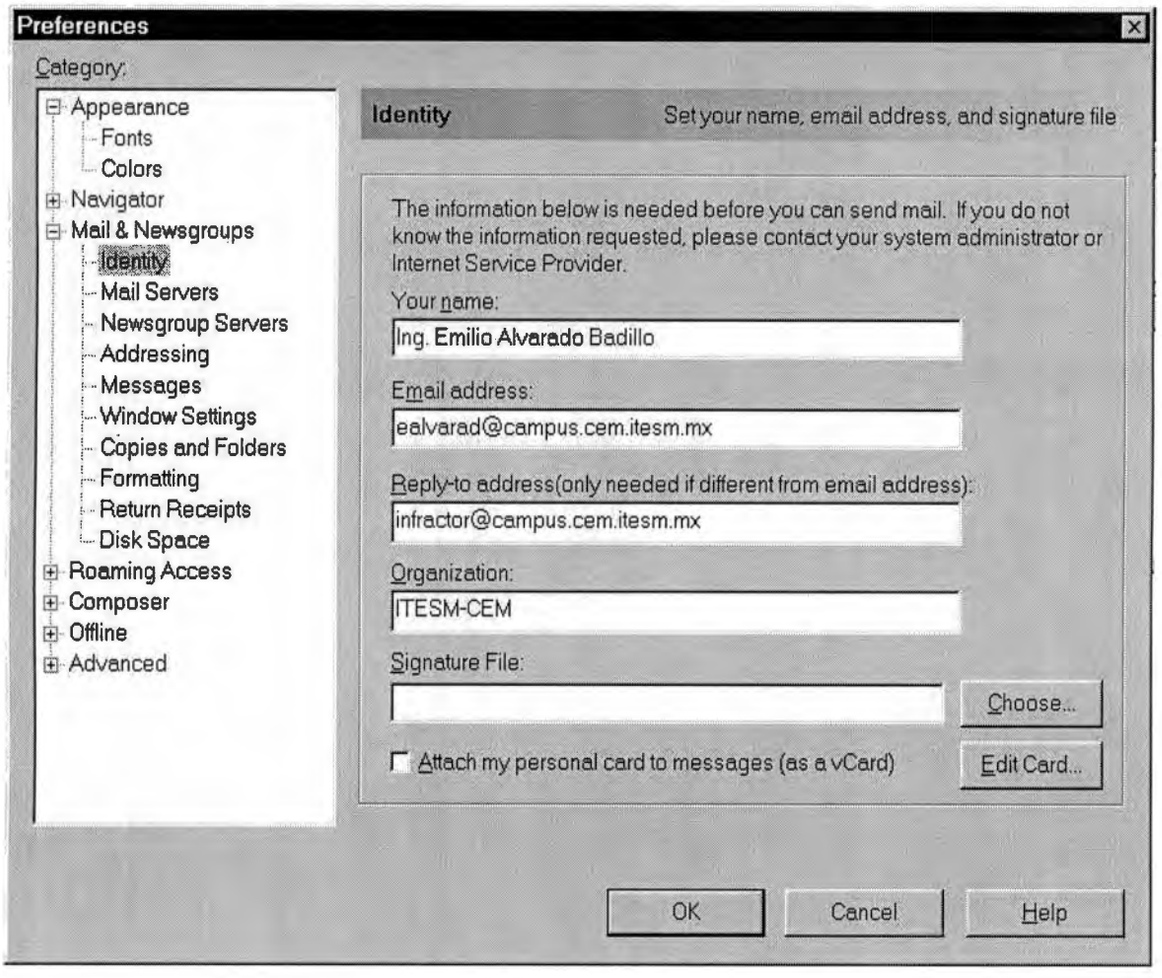

Figura 1: Ejemplo de configuración de un software de correo electrónico a nombre de otro usuario (En este ejemplo se presenta la configuración del correo electrónico a nombre del Director General del ITESM-CEM únicamente con fines de ejemplificación.)

El último paso para consumar el ilícito es escribir un mensaje a nombre de la otra persona para jugarle una broma o causarle serios problemas con los receptores del mensaje. Si el correo electrónico es un medio de comunicación importante u oficial dentro de la organización, a través de él se mandará información confidencial o relevante para el funcionamiento de la institución (estados de cuenta, cartera de clientes, estados contables, etc.). Si alguien manda información falsa a nombre del responsable de la información, puede causar serios problemas dentro de la organización.

Una pequeña ramificación de este problema es la proliferación de correos anónimos, los cuales pueden ser ofensivos, traer amenazas o simplemente ser inofensivos. Al respecto hay poco que hacer ya que hay demasiadas formas de mandar un correo anónimo y la solución de la problemática aquí recae en la importancia que uno le quiera dar a los correos anónimos.

Y no solamente existen las problemáticas planteadas, también existen personas que cuentan con dispositivos para leer el tráfico que pasa por la red, ellos pueden capturar la información y tienen la posibilidad de enterarse de información confidencial, alterarla y reenviarla o darle un mal uso en general.

El uso de Certificados Digitales para resolver estas problemáticas es especialmente útil ya que quien posee un Certificado puede utilizarlo para firmar un mensaje, de la misma manera en que firmaría una carta escrita, solo que en este caso de manera digital. El certificado probará que quien aparece como remitente del mensaje es quien dice ser y que no es un mensaje proveniente de un usurpador. Esto es especialmente útil ya que si bien no podemos evitar que se manden correos anónimos o a nombre de otra persona, si podemos filtrar los correos y solo darles la seriedad debida a los que vengan firmados, además si un correo firmado proviene de un alto directivo podemos asumir que lo que ahí viene es oficial y tendremos la certeza de que se le debe dar la atención adecuada. Con el uso de correos firmados podemos tener la confianza de que su contenido está respaldado por el remitente del correo electrónico.

Además es posible encriptar un mensaje, con la finalidad de que solamente el destinatario del mensaje pueda tener acceso a él. De esta manera si el mensaje llegara a ser visto por intrusos en la red, éste resultaría ininteligible debido a la encripción. Aparte de las bondades mencionadas de los certificados, éstos nos pueden ayudar a saber que el mensaje no fue alterado, es decir, que su integridad no se violó durante su trayecto por la red y eso nos asegura que la información ahí contenida es la que originalmente se envió.

El contar con el correo electrónico como un medio seguro para transferir información por red, especialmente por Internet, nos presenta una alternativa muy interesante para transferencia de información si uno desconfía o tiene la certeza de la inseguridad que ofrecen los sistemas que habitualmente usa, de esta manera se podría basar la comunicación en el correo electrónico de manera importante.

El contar con herramientas que resuelvan estas problemáticas resulta de gran importancia para las organizaciones que en la actualidad utilizan el correo electrónico como herramienta auxiliar en la comunicación, solución que es presentada en este trabajo de tesis.

Aunque la comunicación de red vía correo electrónico es la más transparente para los usuarios, no es la única que se lleva a cabo. También existen comunicaciones entre aplicaciones, servidores, proceso o entidades generales en la red. Dichas entidades también pueden poseer su Certificado Digital y utilizarlo para autenticarse, encriptar, desencriptar, etc.

4.2 Problemática de Sitios de Web Fraudulentos

Actualmente existen muchos sitios de web que venden productos por Internet, estas ventas están basadas en el manejo de tarjetas de crédito principalmente. Para que uno pueda realizar una compra por Internet uno tiene que enviar su numero de tarjeta de crédito para que se realice el cargo de la compra del producto o servicio.

Uno esperaría recibir a vuelta de correo el producto comprado o empezar a hacer uso del servicio adquirido, pero puede suceder que el sitio haya cometido fraude con nosotros y en el mejor de los casos que nunca recibamos lo comprado, ya que los que poseen nuestro número de tarjeta de crédito pueden hacer mal uso de él o también hacer mal uso de nuestros datos personales provistos, trayendo consecuencias muy graves.

De hecho, como es un sitio virtual, que no tiene residencia física ni se nos entrega un comprobante válido y añadamos que, como ya vimos, este tipo de ilícitos no están contemplados por la ley, resulta casi imposible hacer justicia sobre el fraude.

Si el sitio de web contara con un certificado digital, al momento de presentarlo uno podría tener la certeza de que existe alguna Autoridad Certificadora que lo reconoce y prueba su identidad. De esta manera podemos tener más confianza de realizar transacciones por Internet con un sitio que posee un certificado digital.

A este respecto hay que tener mucho cuidado, porque se tiene que verificar el Certificado Digital para constatar que la Autoridad Certificadora que lo expidió es confiable y lo más importante, que sea una Autoridad Certificadora en la cual confiemos. De ser así, podemos realizar la transacción sin temor de ser víctimas de un fraude.

4.3 Problemática de sitios web maliciosos

Como ya se planteó en la problemática general, existen personas que por ocio, por reto o por razones inexplicables del comportamiento humano quieren causar un daño a los recursos computacionales de terceros. Estas personas son consideradas como bándalos (crackers) dentro del mundo de la computación.

Estos delincuentes informáticos son expertos en computación y pueden encaminar sus ataques hacia personas o instituciones en específico o pueden querer causar daño sin importar a quien. Algunos de los ataques que estas personas perpetran pueden ser prevenidos mediante el uso de Certificados Digitales y su respectiva Autoridad Certificadora.

Es el caso de los desarrolladores de software, los cuales pueden poner a disposición de quien lo desee sus programas y productos mediante Internet, nada nos asegura que el sitio no fue montado por los citados delincuentes informáticos y que el software provisto

contiene código malicioso mediante el cual el infractor puede tener control de nuestro sistema o causarle daño a nuestros archivos o aplicaciones. En este caso resultan aplicables los certificados digitales ya que un sitio de distribución de software por la red podría poseer un certificado que al presentarlo se asegure que existe una Autoridad Certificadora que lo respalda.

En el aspecto de los desarrolladores de software es muy importante poner atención en que estén certificados de ser un sitio confiable ya que existen muchas herramientas y lenguajes de programación que pueden ser útiles para que un delincuente informático explote debilidades conocidas de los sistemas con mala intención.

También es muy probable que nuestros sistemas se infecten de virus por medio de la red. Estos virus pueden ser introducidos de manera accidental o premeditada, si se hace de manera premeditada se busca que tengamos fácil acceso a cierto programa y que lo corramos en nuestro sistema, trayendo como consecuencia la infección de nuestros archivos.

Entonces podemos incluir en la política de seguridad de la organización que por razones de protección no se puede bajar software de la red, a menos que el sitio que lo provee presente un certificado expedido por una Autoridad Certificadora confiable que lo avale.

De la misma manera que en el caso de los sitios web fraudulentos, como en este mismo, es necesario que nuestra Autoridad Certificadora tenga relaciones con otras Autoridades Certificadoras a través de Internet para tener un panorama más amplio para certificar sitios en Internet. Este tipo de relaciones entre Autoridades Certificadoras son también tema de estudio de esta tesis y se presenta también como una alternativa de Seguridad Computacional.

Capítulo 2

TEORÍA DE CERTIFICADOS DIGITALES

Los certificados digitales son una importante herramienta de seguridad computacional especialmente del dominio de la seguridad en redes de computadoras. Su aplicación principal se da en redes computacionales grandes que cuentan con gran número de estaciones y servicios, pero lo más importante, un gran número de usuarios. Una red de este tipo puede ser Internet.

Para poder entender cómo trabajan los certificados digitales, es necesario comprender una serie de conceptos que son integrados para poder conformar un Certificado Digital. Estos conceptos están envueltos en lo que en este trabajo se denomina *Teoría de Certificados*, objeto de estudio de este capitulo.

La *Teoría de Certificados* envuelve una serie de conceptos, herramientas, algoritmos, etc. que juegan un papel importante alrededor de los Certificados Digitales, en este capítulo se hará una presentación de estos elementos por separado, y se irán integrando para formar el concepto de Certificado Digital.

1. Criptosistemas

La Criptografía es el conjunto de técnicas o procedimientos que alteran los símbolos de información sin alterar su contenido, convirtiendo la información modificada en un conjunto de símbolos sin sentido para las partes que no disponen de dichas técnicas. La ciencia que se encarga del estudio de los aspectos de esta información en condiciones secretas es la Criptología.

Un Criptosistema, es el conjunto de procedimientos que se llevan a cabo con el fin de brindar seguridad a la información, mediante la utilización de técnicas criptográficas.

Para llevar a cabo el proceso de encripción, las técnicas generalmente usadas son algoritmos con bases matemáticas que transforman la información en un formato llamado *texto cifrado*. Por otra parte, el proceso de desencripción consiste en la utilización de otro algoritmo que transforma la información encriptada en un formato legible llamado *texto plano*, que es la información original.

La finalidad principal de un Criptoanálisis es romper un criptosistema, es decir, descubrir los elementos que componen un criptosistema, lo cual básicamente significa el descubrir la parte medular de un criptosistema, que es la *llave*.

Básicamente, la llave es una entrada al *algoritmo de encripción*[2] que le va a indicar el patrón de tratamiento que se le dará a la información para generar el *texto cifrado*. El tratamiento que se le da a la información puede consistir en permutaciones, rotaciones, sustituciones, funciones matemáticas o muchas otras técnicas.

Debido a que la llave del criptosistema marcó el patrón de tratamiento que se le dio a la información en *texto claro*, se requiere de la misma llave para poder desencriptar la

[2] Está fuera del alcance de este trabajo, el estudiar cada uno de los algoritmos criptográficos aquí mencionados, para su estudio se proveen referencias al lector.

información. A este tipo de sistemas criptográficos se les conoce como Criptosistemas Simétricos, y generalmente sus algoritmos están basados en rotaciones, permutaciones y substituciones de la información en *texto claro*.

Para compartir información entre dos entidades, es recomendable encriptar la información antes de enviarla. Para que el receptor de dicha información tenga acceso a ella, debe poseer la llave del criptosistema usada para el proceso de encripción. La llave puede ser compartida mediante el uso de las siguientes técnicas:

- El emisor escoge la llave, y físicamente la entrega al receptor
- Un tercero puede escoger la llave y físicamente entregarla a las dos entidades comunicantes.
- Si las entidades comunicantes ya han mantenido comunicación previa, una de ellas puede hacer llegar la nueva llave, encriptada con la anterior.
- Si las entidades tienen una comunicación segura con una tercera, esta tercera entidad puede hacerles llegar las llaves.

Este tipo de técnicas son las que generalmente se aplican en los Criptosistemas Simétricos.

2. Criptosistemas de Llave pública

En Internet, y en la mayoría de las redes de computadoras que actualmente son utilizadas por millones de personas diariamente alrededor del mundo, la información que se envía hacia una computadora destino en la red, pasa por numerosas computadoras y dispositivos antes de alcanzar su destino. Por lo general los usuarios y administradores de esos equipos intermediarios no están monitoreando el tráfico en la red.

Por desgracia, existen personas determinadas a monitorear el trafico que pasa por la red, y pueden interceptar o espiar las comunicaciones privadas. Además, estas personas

roban la información original, la alteran y la ponen de nuevo en la red, para que ésta llegue alterada a su destino.

Muchas de estas acciones son perpetradas aprovechando las debilidades de las arquitecturas y protocolos de red. Redes tan grandes e importantes como Internet son propicias para la comisión de estas acciones. Debido a la arquitectura de Internet, y por supuesto de las Intranets, siempre habrá una forma de interceptar información, espiar comunicaciones privadas, alterar información en tránsito, etc. En general, hacer mal uso de la información que pasa por la red.

Es por ello que han tenido que aplicarse medidas de seguridad. Para proveer de seguridad a la información en tránsito por la red, se han explotado muchos de los avances que en materia de criptología existen.

Especialmente en el área de seguridad en redes computacionales, la criptografía de llave pública ha jugado un papel muy importante, ya que su teoría es aplicable a muchos conceptos de seguridad, que serán expuestos a continuación en este capítulo.

Los sistemas criptográficos de llave pública difieren substancialmente de los sistemas simétricos, tratados en la sección anterior, ya que los algoritmos de llave pública están basados en complejas funciones matemáticas, a diferencia de las substituciones y permutaciones utilizadas generalmente por los algoritmos en los criptosistemas simétricos.

Pero la diferencia principal entre estos dos criptosistemas es justamente la propiedad de asimetría, lo cual envuelve el uso de dos llaves, a diferencia de la encripción convencional que solo requiere de una llave. Es por ello que también son conocidos como sistemas asimétricos. El uso de dos llaves ha traído consigo profundas consecuencias en las áreas de confidencialidad, distribución de llaves y autenticación. Áreas que juegan un papel importante en la construcción de un Certificado Digital.

En un sistema convencional de encripción, el mismo algoritmo con la misma llave es usado para encriptar y desencriptar. Por su parte, un sistema de llave pública utiliza el mismo algoritmo para encriptar y desencriptar utilizando un par de llaves, una para el proceso de encriptado y la otra para desencriptar el *texto cifrado* encriptado con la primera llave. Más aún, en el sistema convencional ambas partes deben conocer el algoritmo y la llave. En el sistema asimétrico cada una de las partes deben poseer una de las dos llaves. En el sistema simétrico la llave debe permanecer secreta, mientras que en el asimétrico sólo una de las llaves debe permanecer en secreto.

Por su naturaleza, los sistemas simétricos resultan útiles tanto para cuestiones locales como de red. Por su parte, los sistemas de llave pública son más aplicables para cuestiones de trabajo en red y no resultan tan prácticos para cuestiones locales. Es por ello que son tan populares en el área de seguridad en redes computacionales.

Como pudimos ver, en un sistema asimétrico sólo una de las llaves permanece en secreto y se le conoce como la *llave secreta* y a la otra llave se le conoce como la *llave pública.* Un mensaje encriptado por alguna de estas dos llaves, sólo puede ser desencriptado usando la otra llave del par de llaves. Por ejemplo, un mensaje enviado por la red que fue encriptado con la llave privada, solo puede ser desencriptado usando la llave pública. Por otra parte, si un mensaje fue encriptado usando la llave pública, sólo podrá ser desencriptado con la llave privada.

La llave privada debe permanecer en secreto y en poder únicamente de su dueño, por su parte, la llave pública puede ser distribuida entre las personas con las que se tiene comunicación y/o ponerla en un lugar público para que pueda ser accedida cuando ésta se requiera. A estos lugares se les llama llaveros públicos y son servidores a los cuales un individuo puede mandar su llave pública para que ésta quede accesible a todo el mundo. Los interesados en intercambiar información bajo este esquema con el individuo accederán a este llavero para obtener su llave pública.

El funcionamiento de los sistemas asimétricos es como sigue: Cada individuo posee su par de llaves (pública y privada). La llave pública es accesible a todo el mundo, mientras que la llave privada permanece accesible únicamente a su dueño. Un individuo que posee su par de llaves, puede mandar un mensaje encriptado a otras personas, que usaran su llave pública (disponible a todo el mundo) para desencriptarlo. De la misma manera la gente puede enviarle mensajes encriptados usando su llave pública ya que con su correspondiente llave privada desencriptará el mensaje.

Debido a que un mensaje encriptado por una de las llaves sólo puede ser desencriptado usando la otra llave, tenemos la seguridad de que nadie más que el receptor podrá leer el mensaje enviado, ya que sólo él posee la otra llave del sistema, en este caso la llave privada.

La seguridad del sistema recae en que a un individuo se le puede enviar información encriptada con su llave pública y a pesar de que alguien logre interceptar la información en su trayecto por la red, no lo podrá ver, ya que no posee la llave privada, que es la única que puede desencriptarlo.

Se dice que si la información encriptada que viaja por la red es interceptada por algún individuo, éste no podrá verla ya que lo único que podrá observar es una serie de símbolos ilegibles y sin sentido. Lo que estaría observando en este caso es el *texto cifrado*, que mantiene a la información en condiciones secretas. Para que alguien pueda ver esa información tal cual es, es decir en *texto claro*, se requiere desencriptarla proceso para el cual es necesaria la otra llave del criptosistema y que sólo la posee el verdadero receptor de la información.

La seguridad en el sentido opuesto es frágil, ya que si bien es cierto que un individuo puede enviar información encriptada con su llave privada a alguien que posee su llave pública, podría suponerse que solo el receptor puede tener acceso a dicha información.

El problema que se presenta aquí, es que la llave pública es accesible a todo el mundo y si alguien llega a interceptar la información encriptada con la llave privada, lo único que tiene que hacer es conseguir la llave pública y descubrir la información que viajaba encriptada. Más bien la seguridad en este sentido de la aplicación de las llaves está enfocada, como veremos a continuación, a la autenticación.

El algoritmo de criptografía de llave pública más utilizado alrededor del mundo es el llamado RSA [6] que fue desarrollado por los laboratorios del mismo nombre (RSA Laboratories). Este algoritmo provee métodos para encriptar información, mediante el uso de llaves públicas y privadas. La encripción RSA está definida en PKCS-1 (Public Key Criptographic Standards), que es parte de un conjunto de estándares para sistemas criptográficos de llave pública.

Como ya lo pudimos ver, los sistemas criptográficos de llave pública son sistemas de gran fuerza y nos proveen de una seguridad robusta. Pero no son irrompibles, es decir, alguien con muchos conocimientos, habilidad y las herramientas adecuadas, puede en determinado momento adivinar las llaves. Es por ello que es muy recomendable que las llaves sean de un tamaño muy grande. Entre mayor es el tamaño de una llave, mayor es la dificultad de poderla descubrir.

3. Autenticación

Un grave problema en materia de seguridad computacional, es el de la impersonalización, el cual se da cuando un impostor se hace pasar por el emisor o el receptor de un mensaje. Esta práctica es muy común dentro de las organizaciones cuando se tienen rivalidades o enemistades y se quiere causar un problema serio a un tercero al mandar un mensaje usurpando su personalidad para inculparle de la autoría de dicho mensaje.

Más aún, se puede capturar el mensaje original, alterar su contenido y devolverlo a la red para que llegue a su destino original.

Las posibilidades de impersonalización se pueden ver diezmadas si los usuarios son forzados a autenticarse, es decir, a probar su identidad.

Debido a las propiedades de los sistemas criptográficos asimétricos, es posible usarlos para autenticar al emisor de un mensaje. La propiedad que se explota para lograr ese fin es que un mensaje encriptado con una de las dos llaves del criptosistema únicamente puede ser desencriptado usando la otra llave.

Partiendo de este hecho, tenemos que un usuario posee su par de llaves (pública y privada). El usuario mantiene en secreto su llave privada y la otra llave la hace pública. Si el usuario encripta un mensaje utilizando su llave privada, éste podrá ser desencriptado únicamente usando su correspondiente llave pública, por lo que el desencriptar exitosamente un mensaje comprueba que el usuario fue quien encriptó el mensaje.

La aplicación es sencilla, si un usuario quiere enviar un mensaje a sus colegas, el usuario encripta el mensaje usando su llave privada. Cuando sus colegas reciban el mensaje encriptado, usarán la llave pública de esa persona para desencriptar el mensaje.

Si los receptores del mensaje lograron desencriptarlo, el mensaje debió haber sido encriptado con la llave privada del usuario emisor, ya que la llave pública del usuario emisor es la única que puede desencriptar mensajes encriptados con su correspondiente llave privada.

Debido a que ya se comprobó que el mensaje fue encriptado con la llave privada del usuario emisor, y él es el único que tiene acceso a esa llave privada, entonces podemos comprobar también que él encriptó el mensaje y en consecuencia que fue él quien envió el mensaje. Comprobando de esta manera su identidad.

Si por otra parte los receptores no logran desencriptar el mensaje, quiere decir que posiblemente el mensaje no haya sido enviado por el usuario. Si alguien más mandó el mensaje a nombre del usuario y lo encriptó usando su propia llave privada, la llave pública del usuario original no podrá desencriptar el mensaje. Entonces podemos deducir que alguien más envió ese mensaje a nombre del usuario original.

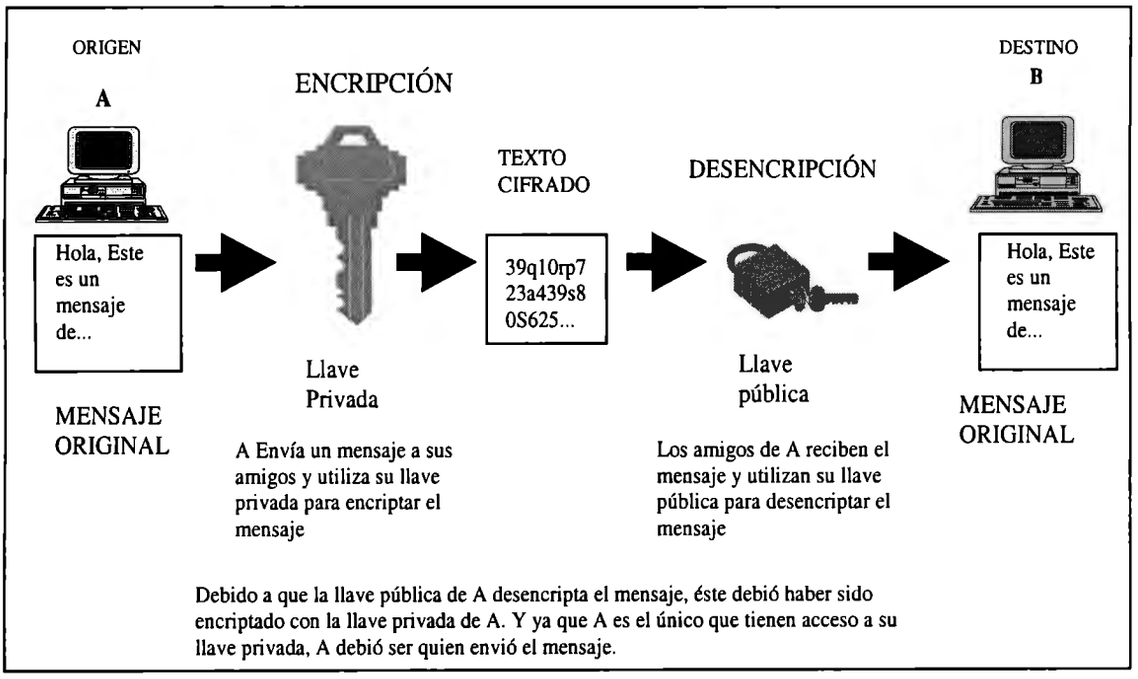

Figura2: Ejemplo del funcionamiento de un sistema critográfico de llave pública y su aplicación en la autenticación.

De esta manera y bajo este esquema nos podemos proteger de la impersonalizacion.

4. Firmas Digitales

En la sección anterior tratamos las técnicas para aplicar las propiedades de la criptografía de llave pública en la autenticación. En realidad el proceso de autenticación es más complejo y estas técnicas son la base para construir un sistema más robusto llamado *Firma Digital.*

Una *firma digital* debe hacer las veces de una firma escrita, en el sentido de que debe verificar al autor del mensaje, además de la hora y fecha de creación del mismo. La firma digital debe ser capaz de autenticar el contenido del mensaje y también debe poder ser verificada por terceros, par resolver disputas.

La seguridad de una firma digital recae en que mediante ella se puede validar que un usuario en específico envío un mensaje, es decir, el usuario emisor no puede negar haber enviado el mensaje. Por otra parte, la firma digital debe verificar que en efecto el mensaje recibido fue el que originalmente se envió, es decir, que el mensaje no fue alterado en su trayecto por la red.

El funcionamiento de las firmas digitales requiere auxiliarse de *funciones hash* y de *algoritmos de huella digital* (message-digest algorithms). Una *función hash*, es una función aritmética que convierte una entrada de longitud variable en una salida de longitud fija (a la cual se le conoce como valor hash).

Para poder generar una firma digital para un mensaje, la función hash es utilizada para generar un valor hash, el cual es una cadena de longitud fija para el mensaje, que es mucho más largo y variable en longitud. En otras palabras, se crea una versión corta del mensaje.

Este valor hash es llamado *huella digital,* y ya que estas *funciones hash* producen una *huella digital* para un mensaje, son conocidas como *algoritmos de huella digital.*

El propósito principal de los *algoritmos de huella digital* es producir una representación del mensaje que sea corta y rápida de encriptar, además de que el receptor del mensaje puede usar la huella digital para verificar que el contenido del mensaje no ha sido alterado.

Los algoritmos de huella digital deben ser funciones de un solo sentido. La función debe obtener de manera sencilla la huella digital del mensaje, pro debe ser muy difícil

obtener el mensaje a partir de la huella digital. Esta propiedad nos asegura que quien tiene acceso a la huella digital no puede remplazar el mensaje por otro que genere la misma huella digital.

Además los algoritmos de huella digital deben producir huellas digitales únicas para cada mensaje, es decir, tiene que ser muy difícil encontrar dos mensajes que produzcan la misma huella digital. Es por ello que también nos podemos asegurar que nadie puede remplazar el mensaje transmitido con un mensaje que tenga la misma huella digital.

Como ejemplos de algoritmos de huella digital tenemos a MD5 [7] que fue desarrollado por los laboratorios RSA. MD5 produce una huella digital de 128 bits y es muy popular en una gran variedad de software.

Otro ejemplo es SHA-1 [8](Short for secure Hash Algorithm), que fue desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) en conjunto con la Agencia Nacional de Seguridad (NSA). SHA-1 produce una huella digital de 160 bits, este algoritmo es más lento que MD5, pero la huella digital es más grande, lo que la hace más resistente a ataques de fuerza bruta que escogen mensajes aleatoriamente para generar la misma huella digital.

El funcionamiento de la firma digital es el siguiente:

- El emisor utiliza un algoritmo de huella digital para generar una versión corta del mensaje original. Esta versión corta del mensaje es conocida como la *huella digital* (message digest).
- Posteriormente el usuario emisor encripta la *huella digital* del mensaje utilizando su llave privada, y envía el mensaje junto con la *huella digital* encriptada hacia su receptor.
- Ya recibido el mensaje, el receptor desencripta la *huella digital* del mensaje.
- El receptor utiliza la *función hash* contenida en el mensaje para generar una *huella digital* del mismo.

- El receptor compara la *huella digital* que él mismo generó, contra la huella digital del mensaje que desencriptó.

Si la comparación da como resultado que las dos huellas digitales son idénticas, quiere decir que en efecto el emisor en realidad es quien dice ser, y además que el mensaje es el que originalmente fue enviado, es decir, que no sufrió alteración alguna durante su trayecto por la red.

Por el contrario, si la comparación da como resultado que las huellas digitales no son las mismas, entonces el receptor puede deducir que el mensaje fue enviado por un impostor tratándose de hacer pasar por el usuario original, o que el mensaje fue modificado o sufrió algún daño durante su transcurso por la red.

En este caso la huella digital del mensaje encriptada, sirve como firma digital del mensaje ya que verifica la identidad del emisor y el contenido del mensaje. En este concepto se ven envueltos muchos aspectos que nos comprueban la seguridad de esta técnica.

Si alguien más envió el mensaje haciéndose pasar por el emisor, este impostor no tiene acceso a la llave privada del emisor original, así que debe usar una llave privada diferente para encriptar la *huella digital* del mensaje.

Ya que el receptor utiliza la llave pública del usuario original para desencriptar *la huella digital* del mensaje, y no la llave pública que corresponde a la llave privada usada por el impostor, la *huella digital* desencriptada no coincidirá con la generada por el receptor.

Si el mensaje fue alterado durante su transcurso por la red, la función hash generará una *huella digital* diferente cuando se aplique al mensaje recibido.

De esta manera atacamos el problema de la repudiación, que se da cuando un emisor niega haber enviado cierto mensaje, si éste cuenta con su huella digital, se podrá comprobar que fue él quien envió el mensaje.

5. Certificados Digitales

Como ya lo hemos estudiado previamente, un sistema de llave pública puede servir para varios propósitos en cuestiones de seguridad computacional. Como lo pudimos constatar, estos sistemas nos puede ayudar con los aspectos de autenticación y firmas digitales, con el fin de comprobar la identidad del emisor de un mensaje.

Pero este esquema fracasa cuando alguien posee una llave pública a nombre de otra persona. Bajo estas condiciones el impostor puede hacer que todo el esquema de los sistemas de llave pública funcione a la perfección. Lo único que tiene que hacer el impostor es generar un par de llaves (pública y privada) a nombre de otra persona. Siendo este el caso, volvemos a sufrir los problemas de usurpación de personalidad y las consecuencias que trae consigo.

Es por ello que se requieren de mecanismos que aseguren que una llave pública realmente pertenece a cierta persona. Los mecanismos aquí referidos son conocidos como Certificados Digitales.

Un Certificado Digital es un documento digital que asienta que una llave pública y su correspondiente llave privada pertenecen a un individuo en particular, certificando de esta manera la identidad de dicho individuo.

Los Certificados Digitales son expedidos por autoridades confiables conocidas como Autoridades Certificadoras. Estas entidades son responsables de verificar la identidad de un individuo y su posesión de una llave pública.

Al poner nuestra confianza en una Autoridad Certificadora, tenemos la tranquilidad de que el portador de un certificado es realmente quien dice ser, y que es realmente el dueño de la llave pública que porta, ya que lo certifica una autoridad en la que nosotros confiamos. Bajo este esquema se le da fuerza a los sistemas de llave pública para proveernos de mayor seguridad.

Capítulo 3

CERTIFICADOS DIGITALES

1. Tecnologías de llave pública y los Certificados Digitales

Las tecnologías de llave pública han sido de gran utilidad para el desarrollo de la seguridad computacional, uno de los más relevantes avances en esta materia son los Certificados Digitales, los cuales explotan al máximo las características de los sistemas criptográficos de llave pública.

Los sistemas de llave pública son my complejos, ya que se forman a base de la integración de diversos elementos, como lo son los algoritmos criptográficos con bases matemáticas, la utilización de dos llaves (en vez de una, como en los sistemas criptográficos tradicionales), aunados a una muy efectiva funcionalidad.

La flexibilidad de los sistemas de llave pública nos permite aplicarlos para cuestiones de autenticación y firmas digitales, así como las tradicionales funciones de encripción y

desencripción. Todos estos elementos son conjugados para formar un Certificado Digital, herramienta de seguridad computacional que nos permite integrar elementos para obtener una comunicación más segura. (Los sistemas de llave pública son estudiados en el capítulo "Teoría de Certificados")

Los sistemas de llave pública nos pueden ayudar en las labores de autenticación, encripción, desencripción y firmas digitales, pero no nos aseguran que quien posee una llave pública es en realidad quien dice ser.

Debido a este tipo de problemas requerimos de mecanismos más sofisticados que nos aseguren que el propietario de una llave pública es en realidad quien dice ser. Es por ello que para solucionar este problema surgen los Certificados Digitales.

2. ¿Qué es un Certificado Digital?

Un Certificado Digital es un documento digital que asienta que una llave pública y su correspondiente llave privada pertenecen a un individuo en particular, certificando de esta manera la identidad de dicho individuo.

Un certificado tiene el propósito de hacer disponible a otras personas una llave pública personal. Las demás personas pueden utilizar esta llave para mandarle mensajes encriptados o comprobar su identidad. Los certificados lo identifican a uno cuando manda mensajes a otras entidades en la red, es decir sirven como prueba de que un individuo es quien dice ser.

3. La Autoridad Certificadora

Los Certificados Digitales son expedidos por autoridades confiables conocidas como Autoridades Certificadoras. Estas entidades son responsables de certificar la identidad de un individuo y su posesión de una llave pública.

Al poner nuestra confianza en una Autoridad Certificadora, tenemos la tranquilidad de que el portador de un certificado es realmente quien dice ser, y que es realmente el dueño de la llave pública que porta, ya que lo certifica una autoridad en la que confiamos.

4. Tipos de Certificados Digitales

Los Certificados Digitales pueden ser expedidos tanto a individuos como a sistemas y a organizaciones. Un certificado puede comprobar la posesión de una llave pública de un individuo, servidor, organización o sistema y ayuda a comprobar sus identidades.

Existen varios tipos de Certificados Digitales, entre los que se encuentran los siguientes:

- *Certificado Personal*: Certifican la identidad y posesión de una llave pública de cierto individuo. En algunos casos, un servidor puede requerir el certificado de un cliente para poder establecer una conexión segura. El cliente muy probablemente tendrá que enviar su certificado personal para autenticarse ante el servidor.

- *Certificado de Servidor*: Éstos certifican la identidad y la posesión de una llave pública de un servidor en particular. El servidor puede presentar su certificado para probar su identidad y para poder establecer una comunicación segura con otras entidades en la red.

- *Certificado de Correo Seguro*: Certifican la identidad y la posesión de una llave pública de un usuario de correo electrónico. Este tipo de certificado es utilizado para verificar la identidad del usuario, encriptar, desencriptar y firmar mensajes de correo electrónico.

- *Certificado de Autoridad Certificadora*: Así como un individuo es certificado por alguna Autoridad Certificadora, otras Autoridades Certificadoras se pueden certificar entre sí al expedirse un documento digital que certifique su identidad y la posesión de la llave que utiliza para firmar los certificados que expiden.

Pueden existir certificados que combinen una o varias de las funciones antes mencionadas, esto depende directamente de la implementación que utilice la aplicación utilizada.

5. Formato de un Certificado Digital (X.509)

El formato para un Certificado Digital esta definido por la ITU-T en la recomendación X.509 [3] y de acuerdo a esta recomendación un certificado debe contener información tanto de la entidad que lo solicitó como de la Autoridad Certificadora que lo expidió. Un certificado consta básicamente de dos partes: La información del certificado y la firma de la Autoridad Certificadora que lo expidió.

Algunos de los datos contenidos en un Certificado Digital son:

- Número de versión (con respecto a la versión del X.509)
- Número de Serie del Certificado (Cada Certificado expedido por una Autoridad Certificadora debe tener un número de serie único)
- El algoritmo para firmar, utilizado por la Autoridad Certificadora (Ejemplo PKCS #1 MD5 con RSA)
- El Nombre Distinguido de la Autoridad Certificadora que expide el certificado. (los nombres distinguidos son expuestos más adelante en este capítulo)
- El periodo de validez del certificado.
- El nombre distinguido de la entidad o sujeto a quien se le expide el certificado.
- Información acerca de la llave pública que esta siendo certificada. Incluye el algoritmo de llave pública y una representación en cadena de bits de la llave pública.

- Opcionalmente puede contener extensiones especiales con información adicional (las extensiones son permitidas a partir de la versión 3 de X.509)

La segunda parte del certificado incluye tanto la firma de la Autoridad Certificadora que expidió el certificado, como el algoritmo de firma utilizado por la Autoridad Certificadora para generar su firma digital. Cualquiera que reciba el certificado puede utilizar ese algoritmo para verificar que el certificado fue firmado utilizando la llave privada de la Autoridad Certificadora.

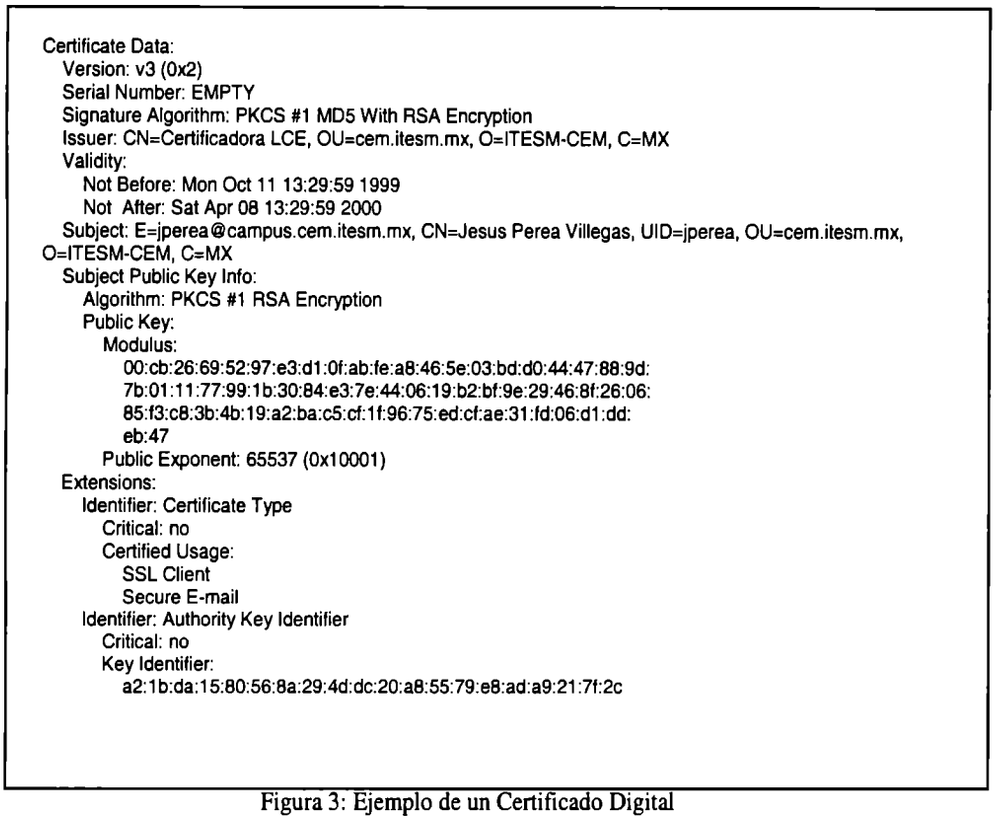

Figura 3: Ejemplo de un Certificado Digital

6. Periodo de Vida de Un Certificado Digital

Todos los Certificados tienen un periodo de vida, el cual esta dado principalmente por la fecha de expiración. La fecha de expiración de un certificado se publica en el mismo y se puede consultar para verificar si un certificado aún es válido. Si la llave pública de alguien se ha comprometido, esta llave no debe ser usada mas y el certificado debe ser revocado. También puede terminar el periodo de vida de un certificado cuando su

dueño ya no esta autorizado para utilizar su llave (por ejemplo, cuando un empleado ya no pertenece a una organización y se le tiene que revocar su certificado).

Las Autoridades Certificadoras tienen la obligación de publicar una lista de certificados revocados, para que los certificados que aparezcan en ella ya no sean aceptados. Este mecanismo funciona de manera muy similar al boletín de tarjetas de crédito, en el cual se publican los números de las tarjetas que no deben ser aceptadas por los establecimientos comerciales.

7. Extensiones de Certificados Digitales

A partir de la versión 3 del estándar X.509, se permite incluir campos adicionales a los certificados. Estos campos adicionales son conocidos como extensiones y pueden contener información adicional que se requiere esté en el certificado, para ajustarse a los requerimientos de alguna organización en particular.

Una extensión de certificado consiste de tres partes:

- El identificador para la extensión, el cual determina el tipo de dato ASN.1 [9] del campo *valor* y cómo se debe interpretar ese valor.
- Una bandera llamada *critica,* la cual especifica si la extensión es crítica o no al certificado. Si la extensión no es crítica y el certificado es enviado a una aplicación que no puede entender la extensión, basándose en el identificador de la extensión, la aplicación puede ignorar la extensión y aceptar el certificado. Por su parte, si una extensión es crítica y una aplicación no puede entenderla, ésta debe rechazar el certificado.
- Una cadena de octetos que contienen la codificación DER [10] del valor de la extensión. Típicamente, la aplicación que recibe el certificado checa el identificador de la extensión para determinar si puede reconocer el identificador. En caso afirmativo, la aplicación utiliza el identificador de la extensión para determinar el tipo del valor usado.

En base a lo anterior nos podemos dar cuenta que no todas las aplicaciones tienen la capacidad de soportar extensiones en los certificados, por lo que no podrán interpretar los certificados que las posean.

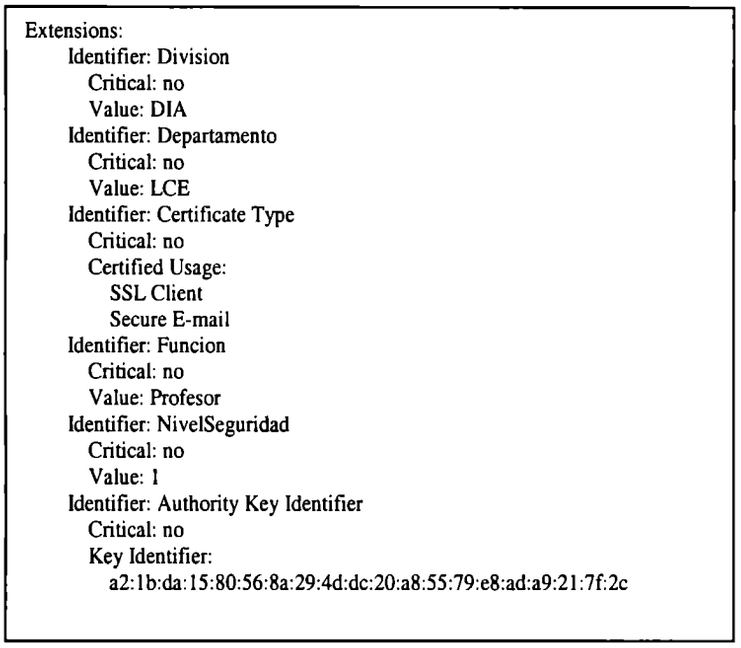

Figura 4: Ejemplo de Extensiones de Certificado. (Se han añadido más Campos al Certificado Digital en forma de extensiones como: Nivel de Seguridad, Departamento, tipo de Certificado, identificador de la llave de la Autoridad Certificadora, entre otros.)

8. Utilización de los Certificados Digitales

Los Certificados digitales ayudan a verificar la identidad de un individuo. Si usted manda su certificado y firma un mensaje con su llave privada, el receptor puede usar la llave pública que se encuentra en el certificado para verificar su identidad. Su certificado y su llave privada sirven como pruebas de que usted es quien dice ser.

Aunque debemos decir que las aplicaciones de los Certificados Digitales son tan amplias como la imaginación de quien lo posee. Muchas aplicaciones serán tratadas a lo largo de este trabajo.

9. SSL y Certificados Digitales

Protocolos seguros como SSL (Secure Sockets Layer) recaen en el uso de certificados digitales como medio para autenticar a las dos partes que participan en una comunicación. Cuando un cliente inicia una sesión SSL con un servidor, el servidor envía su certificado al cliente para identificarse. Si el servidor requiere autenticación del cliente mediante certificados, el cliente enviará su certificado al servidor para identificarse.

Al momento de verificar los certificados, tanto el cliente, como el servidor verificarán que los certificados presentados hayan sido expedidos por una Autoridad Certificadora confiable, de ser así el certificado es aceptado.

Los Certificados Digitales y SSL tienen una relación muy estrecha, ya que SSL es un protocolo seguro que explota en gran medida la tecnología de Certificados Digitales para establecer comunicaciones seguras entre dos entidades a través de la red.

En algunas de sus fases, una conexión SSL requiere del uso de Certificados Digitales. SSL es un protocolo muy popular en Internet y es ampliamente utilizado para realizar transacciones seguras. Debido a su estrecha relación con los Certificados Digitales, se presenta el protocolo SSL en ***anexo A***.

10. S/MIME y Certificados Digitales

Cuando usted envía un correo electrónico a otra persona, el mensaje puede ser ruteado a través de diversos sitios antes de llegar a su destino. En estos puntos intermedios, es posible que alguien pueda ver o alterar el mensaje de correo electrónico. Además de ello

no hay prueba de que el mensaje en realidad vino de la persona quien firma como remitente.

Es por ello que han surgido herramientas para tener un correo electrónico más seguro, para autenticar al emisor y para proteger la privacidad e integridad del mensaje. S/MIME [5] (Secure Multipurpose Internet Mail Extensions) es una de esas herramientas y es un sistema basado en el formato dictado por X.509. S/MIME nos permite encriptar un mensaje de correo electrónico (lo que significa que el mensaje no podrá ser leído en su transcurso por la red), firmar mensajes e incluir nuestro certificado en los mensajes de correo electrónico (lo que significa que el mensaje no puede ser alterado y que el receptor puede comprobar nuestra identidad) .

Bajo S/MIME, un mensaje puede ser firmado par verificar que un mensaje fue enviado por una persona en particular y que éste no fue cambiado desde su envío hasta su recepción (integridad del mensaje). El mensaje puede incluir el certificado de quien lo envía y el receptor lo utiliza para verificar la firma digital. Además bajo S/MIME los mensajes pueden ser encriptados para asegurar una comunicación privada. El mensaje es encriptado usando la llave pública del receptor, contenida en el certificado. Cuando el mensaje es recibido, éste es desencriptado usando la llave privada del receptor, que solamente él conoce. Se puede hacer una correspondencia entre certificados y una lista de control de acceso para que documentos confidenciales puedan ser protegidos de acceso no autorizado. Los certificados pueden ser usados para verificar la validez de otros certificados. Al verificar que la llave usada para firmar el certificado del servidor sea la apropiada respecto a la autoridad certificadora que lo expidió.

11. Cómo funcionan los certificados digitales

Muchas de las características de los criptosistemas de llave pública son integradas para formar la tecnología de Certificados Digitales. Esta tecnología, debido a la gran variedad de elementos que la integran resulta difícil de entender y manejar, especialmente por personas que no tienen formación informática.

Muchas veces el comprender el funcionamiento y utilidad a fondo de la tecnología de Certificados Digitales no es necesario, especialmente para personas que sólo desean explotar esta tecnología. Para ellos sólo basta el saber que los Certificados Digitales sirven básicamente para autenticar y la manera básica de operación.

Para otro tipo de personas que seguramente se ocupan de los aspectos técnicos, los computólogos o simplemente alguien interesado en explorar más acerca del funcionamiento de los Certificados Digitales se requiere de un conocimiento más profundo.

Un Certificado Digital esta construido sobre la tecnología de llave pública. Los certificados son expedidos por autoridades confiables conocidas como Autoridades Certificadoras. Un usuario que desea obtener un Certificado Digital, tiene que contactar a una Autoridad Certificadora en la que confíe y solicitarle un Certificado. Una vez hecha la solicitud, la autoridad certificadora resolverá si otorga o no el certificado acorde a sus criterios y políticas de expedición de certificados.

Al momento de la solicitud, la Autoridad Certificadora que expedirá el certificado debe brindar al usuario las herramientas para generar un par de llaves, una pública y una privada (Ejemplo: Bajo el algoritmo RSA). Debe pedir los datos del usuario, que acorde a las políticas de esa Autoridad Certificadora se consideren necesarios, estos datos incluyen: Nombre, dirección de correo electrónico, teléfono, nombre de la organización, etc.

Hay que tomar en cuenta que durante el proceso de recopilación de datos y de generación de llaves se debe mantener una comunicación segura con la Autoridad Certificadora. Los medios para establecer una comunicación segura los debe proveer la Autoridad Certificadora.

La Autoridad Certificadora tiene la obligación de comprobar la identidad del solicitante, es decir, debe comprobar que quien solicita el certificado es en realidad quien dice ser, de esta manera podrá expedir un Certificado ya que previamente comprobó que los datos que envió son verídicos. De esta manera, la Autoridad Certificadora puede certificar la identidad de quien presenta el Certificado, y que la llave pública contenida en él le pertenece.

Posterior a su expedición, la Autoridad Certificadora debe hacer llegar su certificado al solicitante, quien desde ese memento podrá comenzar a hacer uso de él.

Cuando un individuo usa su certificado para enviar mensajes por la red, los receptores del mensaje pueden utilizar su llave pública, que se encuentra en el certificado, para encriptar información y establecer comunicaciones seguras por la red. La seguridad radica en que todo lo que se encripta con la llave pública sólo puede ser desencriptado utilizando la llave privada, a la cual sólo tiene acceso el emisor del mensaje.

Un usuario puede enviar su certificado en un mensaje y utilizarlo como firma digital. Internamente se utiliza un algoritmo de huella digital (message digest algorithm) para crear una versión reducida del mensaje, llamada huella digital (message digest). Se utiliza la llave privada del usuario para encriptar la huella digital del mensaje y el emisor envía el mensaje, la huella digital encriptada y su certificado.

El receptor utiliza el algoritmo de huella digital, incluido en el mensaje, para generar la huella digital del mensaje que recibió. Además el receptor desencripta la huella digital que recibió con ayuda de la llave pública que se incluye en el certificado, y la compara con la huella que recientemente generó. Si las dos huellas digitales son exactamente iguales, quiere decir que el mensaje fue realmente enviado por la persona que firma como remitente y además se comprueba que el mensaje no fue alterado durante su camino por la red, de otra manera las huellas digitales diferirían. Además el receptor puede comprobar la identidad del remitente y la propiedad de su llave pública, ya que lo

certifica una Autoridad Certificadora en la que confía y quien previamente comprobó la identidad del remitente.

La Autoridad Certificadora no debe retener las llaves privadas de los usuarios, esto la convertiría en un blanco de ataques par obtener las llaves de otras personas. Las llaves privadas permanecen con su dueño y es su responsabilidad el mantenerla en secreto y darle un buen uso.

Al enviar un certificado junto con un mensaje, es posible comenzar a mantener comunicación segura con otras entidades en la red, debido a que en el Certificado se incluye la llave pública y ésta estará disponible para encriptar información de regreso al emisor.

Capítulo 4

AUTORIDAD CERTIFICADORA

1. ¿Qué es una Autoridad Certificadora?

Una Autoridad Certificadora es la entidad responsable de expedir certificados digitales, dicha entidad debe ser confiable ya que la certificación nos debe asegurar que la comunicación se está dando entre las entidades deseadas, además de que sirve como mecanismo para detectar una trampa.

El propósito principal de una Autoridad Certificadora es el de ligar una llave pública al nombre de una entidad contenido en el Certificado y de esta manera garantizar a terceras partes que se han tomado medidas de seguridad para poder asegurar que esta relación (nombre y llave pública) es válida para ambas partes.

2. Funciones de una Autoridad Certificadora

Los Certificados digitales están descritos en la recomendación ITU-T X.509 [3] la cual describe dos niveles de autenticación: Autenticación Simple, la cual se basa en el tradicional esquema del uso de una contraseña como verificación de la identidad provista; y Autenticación Robusta, la cual tiene que ver con el uso de credenciales conformadas mediante técnicas criptográficas complejas. Es este segundo esquema de autenticación el que nos ocupa dentro de una Autoridad Certificadora.

Las funciones generales de una Autoridad Certificadora son las de controlar los servicios de autenticación, además del manejo de los Certificados Digitales. Las Autoridades Certificadoras están gobernadas por sus *Procesos de Certificación*, los cuales deben ser los adecuados para proveer la confiabilidad requerida.

Los Procesos de Certificación o CPS (Certification Practice Statements) son la parte más importante de una Autoridad Certificadora, desafortunadamente estos procesos están fuera del alcance de X.509 y es responsabilidad de la Autoridad Certificadora definir los suyos propios.

Debido a que no existen Procesos de Certificación estándares, ni se han estipulado cuales deben ser estos procesos, en este trabajo de tesis se definen los *Procesos de Certificación* de una Autoridad Certificadora para que puedan ser tomados como guía para las organizaciones mexicanas que desean contar con estos esquemas de seguridad.

El complejo compuesto por funciones, políticas, tareas específicas, procedimientos, etc., que en su conjunto y funcionando como un sistema forman lo que llamamos los *Procesos de Certificación*, que es el alma de una Autoridad Certificadora.

En este capítulo serán descritos paso a paso y de manera detallada las funciones y procedimientos que conforman el Proceso de Certificación de una Autoridad Certificadora, de tal manera que el lector sea capaz de montar una Autoridad

Certificadora. Entonces, cada punto de este capítulo forma parte de los *Procesos de Certificación* y todo el capítulo en su conjunto es la descripción de éstos.

El trabajo de este capítulo está orientado a responder la pregunta, ¿Cómo montar una Autoridad Certificadora?. Los procesos aquí presentados son aplicables tanto a Autoridades Certificadoras para una organización, como a Autoridades Certificadoras independientes que residirán fuera de alguna organización, cuyo giro es exclusivamente la seguridad computacional mediante el uso de Certificados Digitales.

3. Generalidades operacionales de una Autoridad Certificadora

Una Autoridad Certificadora se compone no solamente del software diseñado específicamente para la expedición y manejo de Certificados Digitales. Lejos de eso, una Autoridad Certificadora es un sistema complejo constituido por sistemas computacionales para realizar tareas criptográficas, sistemas de manejo de Certificados, recursos humanos y los fundamentales Procesos de Certificación.

Una Autoridad Certificadora tiene la obligación de ser una Autoridad en todo el sentido de la palabra ya que tiene la responsabilidad de asegurar que quien porta un certificado expedido por ella, es en realidad quien dice ser, detrás de ésto hay una compleja labor que forma parte del Proceso de Certificación.

Los Procesos de Certificación deben ser claros para todos los usuarios y deben estar disponibles a todo mundo, ya que gran parte de la confiabilidad de una Autoridad Certificadora depende de ellos.

Se debe contar con una interfaz de fácil acceso para poder tramitar un Certificado Digital con esa Autoridad Certificadora y debe publicarse la parte de los Procesos de Certificación que tienen que ver con los tiempos de respuesta en el trámite de un Certificado Digital y las condiciones de aceptación o rechazo de la solicitud de Certificado, así como los motivos de revocación de un Certificado.

Es imprescindible que se sigan al pié de la letra los Procesos de Certificación, éstos serán descritos más adelante en este capítulo.

Se debe también infundir una cultura de seguridad y hacer explícitas a los usuarios las ventajas del uso de Certificados Digitales. Además se debe brindar asesoría y soporte técnico en la materia a los usuarios que así lo requieran, ya que se trata de un esquema demasiado complicado para muchos y se requiere mucha ayuda.

4. La Oficina de Certificación

Para el caso en que se desee montar una Autoridad Certificadora dentro de una organización, ésta deberá contar con su propia Oficina de Certificación o Departamento de Certificación. Esto es debido a la complejidad y número de funciones que cumple una Autoridad Certificadora.

Si bien es cierto que el trabajo de montar, administrar y operar una Autoridad Certificadora es muy difícil, no se requiere de un staff de trabajo muy numeroso en la Oficina de Certificación, simplemente se requiere de personas muy capaces en el área de la informática. Claro está que el número de personas requeridas para la oficina de Certificación depende del tamaño de la organización, ya que de eso depende el número de Certificados Digitales a manejar. Se estima que una Oficina de Certificación conformada por un grupo de trabajo de 5 personas puede funcionar para la mayoría de los casos.

El describir el perfil de las personas para la Oficina de Certificación corresponde a los expertos en el manejo de los recursos humanos, lo único que se puede sugerir es que sean personas del área de sistemas con conocimientos de criptografía, especialistas en seguridad computacional, conocedores de redes de computadoras y con actitud de servicio.

5. Organización Jerárquica de una Autoridad Certificadora

La organización jerárquica de una Autoridad Certificadora se compone del Administrador de la Autoridad Certificadora y de su grupo de operadores.

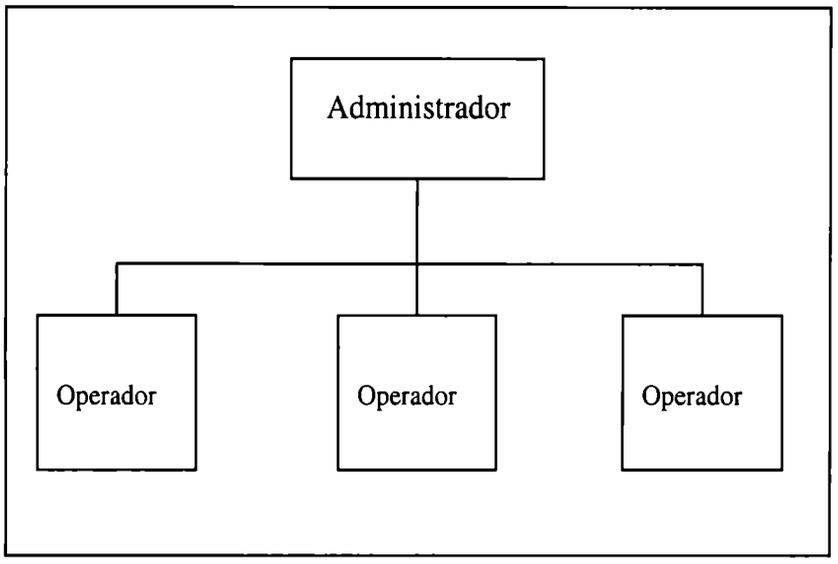

Figura 5: Organización Jerárquica de una Autoridad Certificadora

El responsable en jefe de una Autoridad Certificadora es el Administrador. El papel de Administrador es el más importante dentro de una Autoridad Certificadora ya que además de ser quien dirija la Autoridad Certificadora, será el personaje con mayor responsabilidad dentro de la oficina de Certificación. Las funciones del Administrador de la Autoridad Certificadora son las siguientes:

- Montar la Autoridad Certificadora.
- Conformar su equipo de trabajo.
- Dirigir la Autoridad Certificadora.
- Implantar los Procesos de Certificación.
- Planear el ciclo de vida de la Autoridad Certificadora

Dentro de las tareas del Administrador, la más importante es la referente a los Procesos de Certificación. Esta labor es demasiado compleja ya que se compone de muchas tareas individuales, todas ellas descritas más adelante en este capítulo.

Como ya se mencionó, los Procesos de Certificación (CPS) están fuera del alcance del estándar X.509, por lo que realmente no se sabe cuáles son éstos. La definición de los procesos de certificación es responsabilidad de cada Autoridad Certificadora. A pesar de que en este trabajo presentaremos los Procesos de Certificación que una autoridad Certificadora necesita implantar, también es responsabilidad del Administrador el definir tareas dentro de esos Procesos que sean particulares a su organización ya que es muy probable que se requieran políticas, reglas o procedimientos que se adecuen a una organización en específico.

El papel de un operador de una Autoridad Certificadora es básicamente el de apoyar en los Procesos de Certificación al Administrador realizando tareas como:

- Tramitación de Certificados
- Revocación de Certificados
- Mantenimiento a la lista de certificados expedidos
- Mantenimiento a la lista de certificados revocados

Por separación de funciones, lo ideal es que cada operador se haga cargo de un grupo de tareas en específico, pero esto depende de los recursos humanos con los que cuente la oficina de Certificación.

En realidad un operador de una Autoridades Certificadoras puede llevar a cabo tantas tareas como el Administrador considere pertinentes, tiene que dominar la mayoría de ellas, o por lo menos las tareas críticas ya que uno de los operadores será el candidato a ascender a Administrador o debe poder responder en caso de que falte el Administrador.

6. Expedición de Certificados

El proceso de expedición de certificados es la tarea medular de una Autoridad Certificadoras. Este proceso es muy importante, debido a que detrás de él se encuentra el proceso de comprobación de la identidad de un usuario, lo cual habla del trabajo y las medidas de seguridad que fueron tomadas dentro de la Autoridad Certificadora para poder expedir un documento (Certificado Digital) donde se asegure que quien lo presenta es realmente quien dice ser y que la llave pública que presenta en realidad le pertenece.

6.1 Solicitud de Un Certificado Digital

La expedición de un Certificado Digital es un proceso que se compone de diferentes tareas, la primera de ellas es la Solicitud de un Certificado Digital. Una Autoridad Certificadora es responsable de proveer un medio accesible para la solicitud de Certificados Digitales. El trámite de un Certificado Digital puede hacerse directamente en la Oficina de Certificación, donde un Operador de la Autoridad Certificadora sea el encargado de entregar las solicitudes de Certificados Digitales a los interesados.

Es muy importante que la Solicitud de Certificado Digital contenga información muy completa sobre el solicitante, de tal manera que nos ayude en la tarea de comprobar su identidad.

También la Autoridad Certificadora puede proveer de un sistema computacional de fácil acceso a los usuarios, mediante el cual puedan hacer llegar sus Solicitudes de Certificados Digitales. Este sistema debe proveer de una interfaz para ingresar los datos y enviar una Solicitud de Certificado Digital directamente al sistema de expedición de Certificados de la Autoridad Certificadora.

A continuación se presentan los datos a proveer por parte del solicitante:

DATOS PERSONALES

- **Titulo**
- **Nombre Completo**
- **Fecha de Nacimiento**
- **Dirección**
  - **Calle**
  - **Número**
  - **Número Interior**
  - **Colonia**
  - **Delegación/Municipio**
  - **Estado**
  - **Código Postal**
  - **País**
- **Teléfono particular**
- **Dirección de correo electrónico**
- **Radio Localizador**
- **Teléfono Oficina**
- **URL**
- **Teléfono Celular**
- **Referencias personales**

INFORMACIÓN LABORAL

- **Número de nomina**
- **Compañía**
- **Departamento**
- **URL**
- **Dirección**
  - **Calle**
  - **Número**
  - **Número Interior**
  - **Colonia**
  - **Delegación/Municipio**
  - **Estado**
  - **Código Postal**
  - **País**
- **Teléfono Oficina**
  - **Extensión**
- **Dirección de correo electrónico**
- **Nombre del jefe inmediato**
- **Radio Localizador**
- **URL**
- **Teléfono Celular**
- **Referencias personales**

Figura 6: Datos del Solicitante

No necesariamente los datos que aparecen en la solicitud serán los que aparezcan en el certificado, los datos que se deben incluir en un Certificado Digital se expondrán más adelante en este capítulo.

Las ventajas de contar con un sistema computacional como interfaz para la solicitud de un Certificado Digital, son que se tienen capturados de manera automática los datos de los solicitantes en la base de datos. Además de que no es necesario que el solicitante se desplace hasta la Oficina de Certificación para hacer el trámite. Esto último lleva consigo la desventaja de que es impersonal y no sabemos en realidad quién envió la solicitud, lo que puede retardar el proceso de certificación.

Por su parte, el llevar a cabo el trámite del Certificado Digital directamente en la oficina de Certificación tiene la ventaja de que podemos acelerar el proceso de certificación ya que se cuenta con la persona en ese mismo lugar. El tener que solicitar un Certificado Digital en persona es un proceso robusto y hablaría muy bien de la confiabilidad de la Autoridad Certificadora, pero el desplazar a todos los solicitantes a la sede de la Oficina de Certificación puede no resultar práctico si se trata de una Autoridad Certificadora que está fuera de la organización. Si se trata de una Autoridad Certificadora interna a la organización, esta práctica no tiene mayor complicación.

Una vez que el solicitante haya entregado su solicitud de Certificado Digital ante la Oficina de Certificación, ésta deberá iniciar el trámite interno para poder aceptar o rechazar la solicitud de Certificado Digital. Este trámite deberá llevarse a cabo en un plazo no mayor a 5 días hábiles, plazo que debe ser publicado para información de todos los solicitantes y respetado por la Oficina de Certificación.

6.2 Comprobación de la Identidad de un Solicitante

La importancia del proceso de certificación de un usuario causa un impacto directo en la confiabilidad de la Autoridad Certificadora, ya que entre más robusto sea el proceso de

comprobación de la identidad de un usuario, mayor será la confianza que se transmite a los usuarios.

El proceso de comprobar la identidad de un solicitante debe ser conocido por todo mundo, de tal manera que queden claros y explícitos los procedimientos que lleva a cabo la Autoridad Certificadora para la comprobación de identidades. Este proceso debe estar sujeto a cambios de mejora continua para aumentar la robustez del proceso y de esta manera elevar la confianza por parte de nuestros usuarios.

Si el proceso de Comprobación de la Identidad de un solicitante falla, es decir, que alguien haya solicitado un Certificado Digital haciéndose pasar por otra persona y éste haya sido expedido, todo el sistema de seguridad fallará en cascada. Esto es debido a que todas las llaves coincidirán, las comprobaciones de identidad y firmas digitales serán las correctas, ya que la Autoridad Certificadora emitió un certificado que en realidad no es válido. Pero como el impostor logró burlar las medidas de Comprobación de la Identidad, ahora podrá hacer uso de todos los privilegios del certificado del usuario por quien se hizo pasar. Es por ello que el proceso de Comprobación de la Identidad es crítico.

Un operador de la Oficina de Certificación deberá requerir al solicitante presente dos identificaciones oficiales con fotografía en original y copia, éstas pueden ser: Cédula Profesional, Pasaporte, Credencial de elector, Licencia de conductor, entre otras. La finalidad de presentar el original de la identificación, es la de practicarle una inspección para verificar su autenticidad y comprobar que la fotocopia sea efectivamente de la identificación exhibida. En la mayoría de los casos, las credenciales expedidas por dependencias oficiales mexicanas cuentan con señas especiales para poder determinar su autenticidad, la Oficina de Certificación deberá documentarse en la materia para poder realizar una inspección confiable del documento presentado.

El operador de la Oficina de Certificación deberá corroborar que la fotografía coincida con el portador de la identificación, además de verificar que los datos de la persona

coincidan tanto en las identificaciones como en la solicitud de Certificado Digital. La finalidad de presentar dos identificaciones radica en la dificultad de falsificar más de un documento y que ambos puedan pasar exitosamente a una minuciosa inspección. Es indispensable que por lo menos los datos de una identificación coincidan con los provistos en la solicitud de Certificado Digital.

Si la Autoridad Certificadora es interna a la organización, el solicitante deberá presentar su credencial de empleado junto con su número de nómina y el Operador de la Oficina de Certificación deberá corroborar la información contra la base de datos del Departamento de Recursos Humanos.

Si el solicitante no cubre con esta parte del proceso de comprobación de la identidad, su solicitud de Certificado Digital será rechazada. Se tendrá que anotar en la solicitud la razón por la que fue rechazada y se integrará el expediente de la persona con la solicitud y las copias de los documentos presentados.

Con la finalidad de corroborar la dirección del solicitante, el operador deberá requerirle dos comprobantes de domicilio en original y copia. Estos documentos pueden ser Credencial de elector, Recibo Predial, Recibo Telefónico, Estados de cuenta bancarios, entre otros. Por lo menos el solicitante deberá presentar su Credencial de elector con su domicilio tal y como se encuentra en la solicitud.

Si se trata de una Autoridad Certificadora interna a la organización, se deberá consultar la base de datos del departamento de Recursos humanos y verificar la dirección del solicitante.

Los documentos originales exhibidos, serán devueltos al solicitante inmediatamente después de que se les haya practicado su inspección, las fotocopias serán retenidas por la Oficina de Certificación como prueba de la comprobación de identidad y conformarán el expediente del solicitante junto con su solicitud de Certificado Digital.

La finalidad de comprobar el domicilio del solicitante es la de corroborar que está presentando información verídica acerca de su persona, si el sujeto no puede comprobar su domicilio se puede considerar al sujeto sospechoso de querer usurpar una personalidad y es suficiente razón para negarle la expedición de un Certificado Digital.

A pesar de que se trate de una Autoridad Certificadora fuera de la organización o de haber enviado la solicitud electrónicamente, el solicitante deberá presentarse a las Oficinas de Certificación a cubrir los trámites anteriormente citados. La finalidad de llevar a cabo algunas tareas en presencia del solicitante habla de la robustez del proceso de Certificación, lo cual reditúa en mayor confianza hacia nuestra Autoridad Certificadora.

Una vez concluidos los trámites en presencia del solicitante el operador deberá entregar al solicitante (en caso de haber pasado con éxito las pruebas anteriores) el identificador de su solicitud para futuras referencias. Además el solicitante deberá firmar (firma manuscrita) su Solicitud y el Operador deberá verificar la firma contra las presentes en las identificaciones presentadas. Si el solicitante no es capaz de firmar de manera idéntica, será razón suficiente para rechazar la solicitud.

El Operador deberá enviar un correo electrónico a la cuenta provista por el solicitante informando que una solicitud de Certificado Digital ha sido tramitada en la Oficina de Certificación de esa Autoridad Certificadora, además de solicitarle el identificador de su solicitud a vuelta de correo electrónico. De recibir el identificador adecuado, se pueden proceder a las demás pruebas. En caso de recibir una respuesta que niegue que dicha persona (la verdadera dueña de la cuenta de correo) haya solicitado un Certificado Digital, la solicitud será rechazada de inmediato.

Posteriormente un Operador de la Autoridad Certificadora deberá llamar al domicilio del solicitante para corroborar sus datos con la persona que tome la llamada. Los datos a corroborar serán tres, escogidos al azar de entre la siguiente lista:

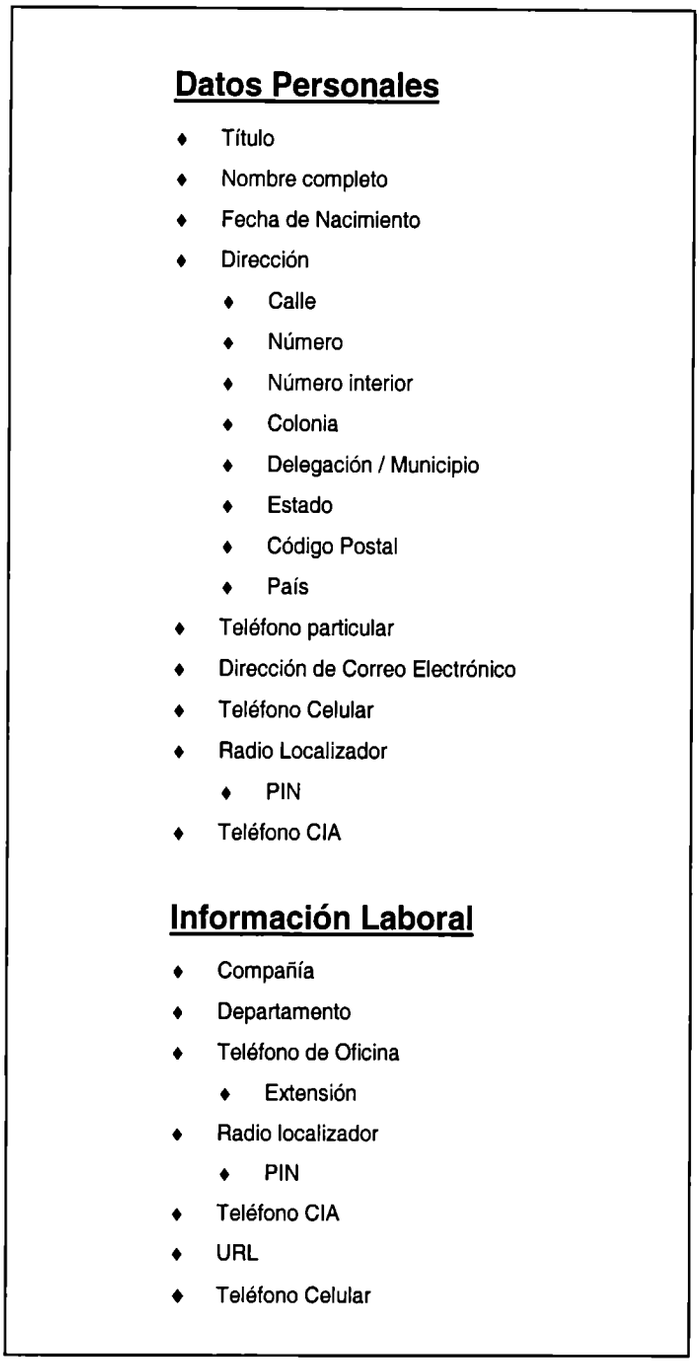

Figura 7: Datos del Solicitante a Comprobar

Se debe registrar el nombre de la persona que atendió la llamada y el número de preguntas que respondió de manera correcta. El propósito de llamar a casa del solicitante es el de verificar que haya provisto de datos verdaderos a la Oficina de Certificación, por lo que se espera que la persona que tome la llamada conteste correctamente al menos una pregunta de manera correcta.

Cabe la posibilidad de que la persona que atienda la llamada no desee proveernos de la información, en este caso se deberá anotar en la solicitud el hecho y proseguir con las pruebas de identidad. Este echo no significa que la solicitud haya sido rechazada.

En caso dado que el teléfono particular provisto no llegara a ser contestado después de varios intentos en diversos días y horarios, se puede considerar como un dato falso y la solicitud quedará rechazada, lo cual deberá ser documentado en la solicitud.

Si fuese el mismo solicitante quien tomase la llamada, obviamente pasará exitosamente la comprobación del teléfono particular lo cual también se registrará en la solicitud. Si la persona que contesta coincide con el nombre provisto, pero niega haber solicitado un Certificado Digital, de inmediato se rechaza la solicitud de Certificado. Y se registra como intento de usurpación.

Como lo hemos podido constatar, ésta no es una prueba muy importante pero nos provee de elementos que nos permitirían en determinado caso, rechazar una solicitud de Certificado Digital.

De manera similar deberá realizarse la comprobación de los datos laborales del solicitante, esta fase se llevará a cabo llamando al jefe inmediato del solicitante para solicitarle la corroboración de los datos. Además se debe contactar al solicitante y pedirle nos diga el identificador de su solicitud que le fue asignado. Si esta prueba no es aprobada, la solicitud de Certificado Digital deberá ser rechazada, debido a que existe sospecha de usurpación de personalidad. Este hecho también se debe registrar.

Por último y de manera muy similar a como se hace en una investigación bancaria, la Oficina de Certificación deberá contactar a las referencias personales provistas por el solicitante para precisamente pedir referencias del sujeto que solicita el Certificado Digital. En dado caso que las referencias fueran negativas la solicitud deberá ser rechazada, de otro modo la solicitud será aceptada y la oficina de Certificación procederá a expedir el Certificado Digital.

Podemos resumir el trabajo de pruebas de la Comprobación de la Identidad en los siguientes pasos:

1. *Identificación del Solicitante*
2. *Comprobación del Domicilio del Solicitante*
3. *Firma de la Solicitud por parte del Solicitante*
4. *Verificación de la posesión de la cuenta de correo electrónico*
5. *Comprobación del Teléfono particular del Solicitante*
6. *Comprobación de los Datos Laborales del Solicitante*
7. *Contacto con las Referencias Personales del Solicitante*

No todos los pasos tienen que ser aprobados estrictamente al 100% por el solicitante. Los pasos que se deben cubrir forzosamente son los enumerados: 1,2,3,4 y 6. Para el caso en que la Autoridad Certificadora resida dentro de la organización, se pueden llevar a cabo únicamente los pasos 1, 4 y 5, apoyados de la Oficina de Recursos humanos para corroborar todos los datos provistos por el solicitante.

Como primer paso a la comprobación de la identidad de un usuario el Operador debe buscar su expediente ya que bajo ninguna circunstancia debe expedirse un Certificado Digital a una persona cuya solicitud haya sido previamente rechazada. Esto es debido a que el sujeto sería sospechoso de haber falsificado documentos o una vez conocidas las pruebas, manipular las circunstancias con la finalidad de aprobarlas.

Debido a que el conocer a detalle las pruebas que se realizan para comprobar la identidad de un usuario se puede prestar a que alguien pueda manipular las circunstancias con la finalidad de pasar las pruebas, es conveniente que se haga del conocimiento de todo mundo el proceso pero sin divulgar sus detalles, es decir se puede publicar el qué mas no el cómo.

7. ¿A quién se le debe expedir un Certificado Digital?

Una Autoridad Certificadora de una organización debe expedir certificados digitales únicamente a los miembros de la misma organización, sin importar su rango, jerarquía o posición dentro de la organización. También puede expedir Certificados Digitales a sus colaboradores más cercanos como lo pueden ser clientes y proveedores para poder establecer un sistema de comunicación segura con ellos.

No se deben expedir Certificados a personas ajenas a la Organización ya que la responsabilidad sobre el mal uso del certificado recaería en la Autoridad Certificadora que lo expidió, y por lo tanto de la organización.

Una Autoridad Certificadora que se dedica a expedir Certificados Digitales a todo mundo prácticamente no tiene restricciones a este respecto, únicamente debe cuidar bien el aspecto de la certificación de un usuario.

8. Notificación de Rechazo de una Solicitud de Certificado Digital

La Oficina de Certificación tiene la obligación de notificar a una persona que su solicitud de Certificado Digital fue rechazada. Además de ello, la Oficina de Certificación debe darle las razones por las cuales su Solicitud no procedió. Esta notificación puede llevarse a cabo, ya sea citando al Solicitante en la Oficina de Certificación para ahí informarle del rechazo de su solicitud, mediante una llamada telefónica o vía correo electrónico.

9. Emisión de un Certificado Digital

Dentro del proceso de Expedición de un Certificado Digital, hemos definido un subproceso que llamaremos "Emisión de Certificado Digital", el cual se encargará de la parte técnica para poder expedir un Certificado Digital acorde al estándar X.509 y a los estatutos aquí presentados.

Básicamente las especificaciones técnicas de un Certificado Digital se encuentran descritas en el capítulo "Certificados Digitales", las cuales se encuentran soportadas en el capítulo "Teoría de Certificados Digitales". Basándose en los lineamientos dictados en los capítulos previos, es como se debe llevar a cabo el proceso técnico de la Emisión de un Certificado Digital. En esta sección, únicamente ahondaremos en los aspectos que así lo requieran.

Para la Emisión de un Certificado Digital se deben tener en mente los siguientes aspectos:

- Un Certificado Digital tiene un número de serie único.
- Los algoritmos criptográficos utilizados en los capítulos "Teoría de Certificados" y "Certificados Digitales", como RSA, MD5, SHA, etc. Podrán ser utilizados en cualquiera de sus variantes acorde al criterio del Administrador, por supuesto, siempre teniendo en mente el brindar la mayor seguridad.
- Hacer uso de la convención de Nombres Distinguidos (presentada más adelante en este capítulo).
- Todo Certificado debe tener un periodo de validez.
- El proceso de emitir un Certificado Digital incluye el generar las llaves tanto pública como privada para su respectivo Certificado utilizando los algoritmos criptográficos como se indica en los capítulos "Teoría de Certificados" y "Certificados Digitales".

9.1 Campos de un Certificado Digital

Para poder emitir un Certificado, primero debemos definir cuáles son los campos que debe contener. X.509 establece que un Certificado debe contener información tanto del solicitante, como de la Autoridad Certificadora que lo expidió. Por lo tanto podemos dividir un Certificado en dos partes, la información contenida en el Certificado y la firma de la Autoridad Certificadora que lo expidió.

La parte de la firma digital esta cubierta con el uso de los algoritmos criptográficos de los capítulos "Teoría de Certificados" y "Certificados Digitales", los cuales recordemos

que se pueden utilizar en cualquiera de sus variantes acorde al criterio del Administrador. La parte de la información del Certificado contiene campos como los son: Número de versión del X.509, número de serie del certificado, información acerca de los algoritmos criptográficos, el periodo de validez del Certificado, los nombres distinguidos de la Autoridad Certificadora y del dueño del Certificado, etc.

Pero toda esa información realmente puede no hablar mucho acerca del dueño del Certificado, o dicha información puede resultar insuficiente desde el punto de vista de la organización. Si se requiere aumentar la información se tiene que hacer uso de las extensiones para los Certificados Digitales y agregar los campos que se consideren necesarios. Algunos datos que se podrían incluir son: Nombre, Compañía, Departamento o área y Teléfono. Estos datos proveerán de mayor información y servirán para realizar pruebas de autenticidad en caso de sospecha de usurpación de personalidad.

10. Entrega de un Certificado Digital

Si el proceso de comprobación de la identidad de un solicitante, fue aprobado exitosamente, entonces la Autoridad Certificadora tendrá todos los elementos para poder emitir un Certificado Digital a esa persona.

Una vez emitido el Certificado Digital, la Autoridad Certificadora deberá hacer llegar éste a su dueño. Hay que recordar que para que todo el Sistema de Seguridad basado en Certificados Digitales funcione, se debe hacer entrega también de las llaves pública y privada.

El hacer entrega del certificado y la llave pública no representa mayor dificultad, ya que ambos van integrados en el Certificado y son información pública y en dado caso que fuese interceptada por terceros, no sería de utilidad al infractor debido a que como ya lo sabemos, se requiere de la llave privada para que todo el criptosistema funcione. Entonces esta entrega se puede llevar a cabo vía correo electrónico.

10.1 Entrega de la llave privada

El problema comienza cuando se trata de hacer entrega de la llave privada, ya que ésta es información demasiado delicada y estrictamente confidencial, sólo su dueño debe tener acceso a ella. Eso significa que ni siquiera la Autoridad Certificadora debe conservar copia de las llaves que genera, eso la convertiría en blanco de ataques y se podría responsabilizar a la Autoridad Certificadora si se llegase a dar un mal uso de las mismas.

Debido a la naturaleza delicada de la llave privada, ésta se puede entregar de manera personal en la Oficina de Certificación junto con el Certificado y su llave pública. El operador debe solicitar el identificador de la Solicitud par poder hacer la entrega de las llaves.

Una alternativa es que desde el momento mismo de la solicitud de Certificado sean generadas las llaves (ya sea en persona o vía un sistema computacional) y se quede en posesión del solicitante la llave privada. En caso de que la solicitud fuera rechazada no importa que el usuario tuviera la llave privada ya que necesita el resto de los elementos del rompecabezas para que el criptosistema pueda funcionar.

11. El Expediente de Usuario

Por cada usuario es indispensable llevar su expediente, este documento cumplirá funciones administrativas para la Oficina de Certificación. El expediente estará conformado por la siguiente documentación: Solicitud de Certificado, Dos fotocopias

de identificaciones del usuario, Dos fotocopias de comprobantes de domicilio del usuario, Observaciones.

La Solicitud se compone de la siguiente información:

- Datos Personales
- Información laboral
- Referencias personales
- Solicitud Aceptada Si o No
- Motivo del Rechazo de la Solicitud
- Observaciones

En la parte de observaciones del Expediente, se registra información relevante acerca del uso del Certificado, por ejemplo, si presentó mal uso del Certificado, si alguna vez perdió o expuso la llave privada, etc.

12. El Buen Uso de las Laves

Es muy importante que los usuarios hagan buen uso y tengan cuidado de sus llaves y de su certificado digital. La llave privada es la que requiere de mayores cuidados ya que el resto de las piezas son información pública. Debido a que la llave privada es un elemento de uso continuo, ésta debe residir en el disco duro local del usuario. Para protegerla se deben tomar las siguientes medidas:

- Debe residir en una carpeta no accesible por red.
- Debe almacenarse encriptada.
- Debe permanecer protegida con una contraseña.

Es muy importante no hacer respaldo de la llave privada ya que se podría dejar expuesta u olvidada. En caso de desear hacer respaldo de la llave privada éste debe residir en un medio de almacenamiento magnético encriptada y protegida con contraseña.

Además de estas medidas de seguridad se debe tener en cuenta que este tipo de sistemas funcionan de manera personal, por lo que no se deben prestar las cuentas de correo, ni los certificados, ni las llaves.

La mayoría de los sistemas como el correo electrónico seguro, manejan de manera transparente la encripción de la llave privada.

13. Intercambio de Llaves

Como ya lo estudiamos, para que este tipo de sistemas puedan funcionar, requerimos compartir nuestra llave pública con las personas con las que deseamos mantener comunicación. Cada vez que enviamos un mensaje con nuestro Certificado, junto con él viaja nuestra llave pública, quedando disponible al receptor del mensaje. De esta manera un usuario puede enviar mensajes firmados con su Certificado Digital a las personas con las que desea mantener comunicación con la finalidad de hacerles disponible su llave pública.

Otra manera de hacer disponible una llave pública es inscribirla en un llavero público, el cual es de acceso universal, de esta manera quien esté interesado en mantener comunicación segura con otro usuario buscará su llave pública y la obtendrá vía el llavero digital. Para el caso de los Certificados Digitales los llaveros públicos se denominan Directorios, donde se pueden obtener los Certificados Digitales de las personas.

Comparando ambos sistemas de intercambio de llaves podemos decir que en el primero el dueño del Certificado tiene el control de las personas que tienen acceso a su Certificado Digital, ya que él mismo se los hizo disponible. Por otro lado en el sistema de Directorio el usuario no tiene control sobre las personas que tienen acceso a su Certificado Digital. Al final de cuentas ambos sistemas cumplen la misma finalidad y es

decisión del Administrador de la Autoridad Certificadora el instalar un servicio de Directorio o llevar el intercambio de llaves persona a persona.

14. Revocación de un Certificado

De la misma manera que una Autoridad Certificadora puede expedir un Certificado Digital a una persona, o negárselo acorde a los Procesos de Certificación que la gobiernan, una Autoridad Certificadora puede dar de baja un Certificado Digital de un usuario apegada también a los Procesos de Certificación establecidos.

Un Certificado Digital puede ser dado de baja por las siguientes razones:

Baja solicitada por el usuario: Si un usuario voluntariamente pide que su certificado sea dado de baja éste tendrá que ser dado de baja por parte del personal de la Oficina de Certificación. Este caso se puede dar si es que la persona que solicita la baja de su certificado ya no trabajará más en la organización (Autoridad Certificadora interna a la Organización) o el usuario ya no desea contar con un Certificado Digital.

A este respecto nos tenemos que detener para hacer algunas observaciones. Si en una organización el uso del Certificado Digital es oficial y su utilización es de carácter obligatorio, entonces la Autoridad Certificadora deberá advertir al usuario del riesgo que corre al solicitar la baja de su Certificado, pero bajo ningún motivo puede negar la baja de su Certificado ya que éste es personal.

Baja por exposición de llaves: Si las llaves del usuario fueron expuestas y se sospecha que alguien más puede tenerlas en su poder y hacer mal uso de ellas, el usuario cuyas llaves se hayan en peligro, debe notificarlo a la Oficina de Certificación para que su certificado sea dado de baja. De igual forma, si el sistema del usuario ha sufrido de un ataque informático y se sospecha que la llave privada pudo haber caído en manos ajenas, el Certificado debe darse de baja.

Baja por finalización del periodo de vida del Certificado: Este tipo de baja es transparente y sucede cuando el periodo de vida de un Certificado expira. Después de su fecha de expedición el Certificado ya no es válido, por lo tanto se encuentra dado de baja.

Baja por abandono de la organización: Si la persona poseedora del Certificado Digital, por alguna razón dejará la organización, su certificado deberá ser dado de baja. Esto último aplica solamente en el caso de que la Autoridad Certificadora sea interna a la organización, ya que como lo vimos anteriormente únicamente podrán tener Certificado Digital los miembros de la organización y los colaboradores más cercanos.

Baja por orden superior (mal uso del Certificado): El Administrador de la Autoridad Certificadora o sus superiores pueden dar de baja el Certificado a un usuario, si consideran que hace mal uso de él o desean que ya no posea más un Certificado Digital.

El dar de baja un Certificado Digital no implica que el usuario deba devolverlo, ya que en este tipo de cuestiones digitales, una persona puede duplicar la información con mucha facilidad, así que el exigir la devolución del Certificado no tendría mucho sentido. Además recordemos que la Autoridad Certificadora no guarda las llaves que genera.

Entonces la pregunta es, ¿Aún si un Certificado es dado de baja, sigue funcionando? La respuesta es si, ya que técnicamente no existe imposibilidad alguna para que el usuario no pueda utilizarlo. El certificado ya ha sido expedido y entregado junto con su juego de llaves, por lo que el dejarlo de usar por baja depende únicamente del usuario, quien puede decidir seguir usándolo.

Al proceso de dar de baja un Certificado Digital también se le puede llamar, proceso de revocación de un Certificado.

15. Notificación de Revocación de un Certificado

Es responsabilidad de la Autoridad Certificadora el notificar a una persona que su Certificado Digital ha sido dado de baja, este proceso debe ser sencillo ya que se puede hacer enviando un correo electrónico al usuario, notificándole de la baja de su Certificado y exponiendo las razones de la misma.

16. La Lista de Certificados Expedidos

La Autoridad Certificadora tiene la obligación de publicar una lista, que contenga todos los Certificados que ha expedido. Esta lista tiene la finalidad principal de servir de consulta para poder corroborar que efectivamente un Certificado fue expedido por la Autoridad Certificadora que lo firma. Aquí añadimos un punto más de seguridad, ya que cabe la posibilidad de que surja otra Autoridad Certificadora que se haga pasar por la original. Esta lista debe ser de acceso universal. Es derecho y obligación de los usuarios de la Autoridad Certificadora el consultar esta lista.

17. La Lista de Certificados Revocados

La Autoridad Certificadora tiene la obligación de publicar una lista, que incluya todos los Certificados que ha revocado. Esta lista tiene como función principal, la de servir de consulta en dado caso que se desee saber si un Certificado aún es válido. La autoridad Certificadora debe ser demasiado cautelosa en el mantenimiento de esta lista ya que el periodo de actualización puede aprovecharse para la comisión de ilícitos.

Esta técnica de mantener una lista con todos los Certificados revocados nos ayuda a detectar quiénes están utilizando Certificados que ya no son válidos. Es derecho y obligación de los usuarios el consultar esta lista.

18. El uso de Certificados Revocados y Duda en la Procedencia de un Certificado.

Como ya lo estudiamos previamente, técnicamente una persona puede seguir utilizando su Certificado a pesar de que se le haya prohibido el uso del mismo, para evitar estos problemas contamos con la lista de Certificados Revocados. El gran problema es que todos los usuarios deberían consultarla con frecuencia y realmente nunca se sabe cuando ha ocurrido un cambio en dicha lista.

Es obligación de los usuarios el consultar la lista de Certificados Revocados, pero por otro lado, el Administrador de la Autoridad Certificadora debe comunicar vía correo electrónico a todos los usuarios, que el Certificado perteneciente a cierta persona, ha sido dado de baja. De la misma manera el Administrador puede enviar la notificación de que un nuevo Certificado ha sido expedido, para que éste sea buscado en la lista de Certificados Expedidos de la Autoridad Certificadora. Si se tiene duda de la procedencia de un Certificado, el usuario mismo puede consultar la lista de Certificados Expedidos para despejar su duda.

19. Trámite por Segunda vez de un Certificado Digital

Un Certificado Digital puede ser dado de baja o puede expirar. El usuario que lo poseía puede querer tramitar otro Certificado Digital. En este caso el proceso es mucho más sencillo ya que el Solicitante ya ha probado su identidad, lo que significa que el Proceso de Comprobación de la Identidad será considerado como aprobado. Esto no necesariamente significa que la aprobación del segundo Certificado sea automática.

El proceso para solicitar un Certificado Digital por segunda vez comienza de la misma manera que el proceso seguido para solicitarlo por primera vez. El Solicitante debe entregar su solicitud de Certificado Digital al operador de la Oficina de Certificación, exponiendo en la misma solicitud que se trata de una petición por segunda vez. El

Operador debe consultar el expediente del Solicitante para consultar el motivo de la baja, únicamente se podrán expedir Certificados Digitales por segunda vez si el Certificado expiró y además no se hizo mal uso del mismo, debido a que las llaves fueron comprometidas o si la baja fue solicitada por el mismo usuario.

Si el Solicitante cubre con dichas especificaciones, el Operador de la Oficina de Certificación procederá a autorizar la Solicitud.

El usuario debe tener especial cuidado en guardar su anterior Certificado Digital y conservar sus llaves. Esto es con la finalidad de que pueda recuperar mensajes encriptados con el Certificado y llaves anteriores. Si el usuario necesita tramitar otro Certificado por pérdida del anterior, la Autoridad Certificadora no se puede responsabilizar de la recuperación de mensajes que funcionaban bajo el Certificado y llaves anteriores.

Si las herramientas de software utilizadas para expedir Certificados Digitales lo permiten, y el Certificado de un usuario expiró, es recomendable expedir el mismo Certificado Digital modificando la fecha de expiración. De esta manera no tendremos problemas por cambio el cambio de llaves.

20. Nombres Distinguidos

Los Nombres Distinguidos son representaciones en formato de cadena de caracteres, que identifican de una manera única a usuarios, sistemas y organizaciones.

Un Nombre Distinguido, por lo general comienza con el nombre propio de la entidad a describir y es precedido por los demás datos de la entidad hasta llegar a la especificación del país. Típicamente un Nombre Distinguido contiene la información presentada en la Tabla 1.

TABLA 1: Componentes de un Nombre Distinguido

Componente	Nombre	Descripción
CN	Nombre Común Common name	Identificador de la persona u objeto (entidad). Ejemplos: CN= Sergio Perea CN=campus.cem.itesm.mx
E	E-mail	Identifica la dirección de correo electrónico de la entidad Ejemplo: E=sperea@campus.cem.itesm.mx
OU	Unidad Organizacional Organization Unit	Identifica la Unidad (departamento) dentro de la Organización Ejemplos: OU=Cómputo Especializado
O	Organización	Identifica la organización en la que la entidad reside Ejemplos: O=ITESM-CEM
L	Localidad	Identifica la localidad en la que reside la entidad Ejemplo: L=Atizapan de Zaragoza
ST	Estado State/Province Name	Identifica el Estado en el que reside la entidad. Ejemplo: ST=Estado de Méxio
C	País Country	Identifica el país en el que reside la entidad. Ejemplo: C=Méxio

En los Certificados Digitales los Nombres Distinguidos son utilizados para identificar lo siguiente:

- Al individuo que posee el par de llaves de un Certificado
  CN=Sergio Perea, OU=Cómputo Especializado, O=ITESM-CEM, C=MX

- Al Servidor que posee el par de llaves de un Certificado
  CN=campus.cem.itesm.mx , OU=DI, O=ITESM-CEM, C=MX

- A la Autoridad Certificadora que firmó el Certificado
  OU=Certificadora LCE, O=ITESM-CEM, C=MX

Los Nombres Distinguidos están definidos en el estándar X.520 [11] y deben ser usados para representar a la entidad dueña del Certificado Digital.

21. Políticas de Certificados

Acorde a X.509, una Política de Certificado es una serie de reglas que indican la aplicabilidad de un Certificado a una entidad o aplicación en particular con requerimientos de seguridad. Esto quiere decir que un certificado puede aplicar para ciertas funciones y negar algunas otras.

Supongamos que la Asociación mundial de aerolíneas planea definir algunas políticas de Certificado para su implantación en la industria aeronáutica. Bajo la infraestructura de llave pública de la Asociación mundial de aerolíneas y la infraestructura de llave pública de cada aerolínea individual, se tienen que definir dos políticas de Certificado: La política de propósito general y La política de propósito comercial.

La política de propósito general esta definida para el uso del personal para proteger información de rutina, como correo electrónico casual, autenticación en la web, etc. Para estos propósitos, las llaves pueden ser generadas, almacenadas y manejadas usando sistemas de bajo costo. Esta política aplica a todos los empleados de todas las lineas aéreas.

Para el caso de la política de propósito comercial, ésta es usada para la protección de transacciones financieras o para llevar a cabo operaciones estratégicas entre las diferentes líneas aéreas. Esta política aplica únicamente a los altos directivos autorizados de las líneas aéreas.

Las políticas pueden ser implantadas en las extensiones de Certificados definidas en *X.509, éstas pueden* ser definidas de dos formas: Críticas o No Críticas. Si la política es

no crítica, entonces quiere decir que la política indicada es aplicable al usuario o entidad que presenta el Certificado, pero el Certificado no está restringido para dicho uso. Ya de manera previa la aplicación debió haber sido configurada para requerir un Certificado que incluya la política de propósito general. En el ejemplo anterior, a un empleado común se le expedirá un Certificado que incluya la política de Propósito general.

En el caso de una Política Crítica, ésta funciona de manera diferente, ya que el certificado está restringido al uso que le impone la política. Utilizando también el ejemplo de las líneas aéreas, a un directivo de alto rango de alguna línea aérea, se le expedirá un Certificado que incluya la Política de propósito comercial, que es crítica, por lo que sólo estará autorizado para las tareas que la política restringe. Esto es debido a la importancia de las tareas definidas en las políticas críticas (transacciones financieras, operaciones estratégicas entre organizaciones, etc.) Se restringe a una sola función a los certificados, para evitar el abuso del poder del que gozan. Por ejemplo, un Certificado que faculta a una persona a únicamente realizar transferencias de fondos, le impedirá llevar a cabo un retiro de fondos.

La definición de políticas de Certificado es tan amplia como las necesidades de una organización, aunque estas son difíciles de implementar ya que se debe añadir un campo más al Certificado Digital con el nombre de la política. El manejo e implantación de extensiones X.509 está cubierto en el capítulo "Caso de estudio ITESM-CEM".

Los Certificados Digitales en sí, cumplen la función de certificar que una persona o entidad es realmente quien dice ser. Por eso las restricciones no deben ser a nivel de certificado, sino directamente en las aplicaciones. Si una persona o entidad ha comprobado mediante su Certificado Digital su identidad, las restricciones se deben poner en los sistemas, de esta manera evitamos definir políticas de Certificado.

No se le debe dar un uso inadecuado a los Certificados Digitales, la autenticación es sobre las personas o entidades de la red, una vez superada esa primera barrera los sistemas mismos deben ser los que se encarguen de los demás aspectos de la seguridad.

22. Tipos de Autoridades Certificadoras

Las Autoridades Certificadoras pueden ser internas a una organización o externas a la misma empresa. En el primer caso, la propia organización es quien lleva la responsabilidad de operar la Autoridad Certificadora y generalmente los certificados que son expedidos por esta autoridad son para los miembros de la organización y en algunos casos para colaboradores cercanos como clientes y proveedores.

En el caso de una Autoridad Certificadora externa a la organización, el proceso de certificación es delegado a una Autoridad Certificadora.

Una Autoridad Certificadora debe, primero que nada, establecerse como una autoridad ya que tendrá potestad para emitir o denegar la expedición de certificados digitales a los solicitantes. Además sobre ella recaerá la responsabilidad de los certificados que expidió, lo cual implica un gran compromiso en materia de seguridad computacional, para con la organización que solicitó sus servicios de certificación.

Acorde a sus Procesos de Certificación, la Autoridad Certificadora deberá establecer a quién se le otorgará un certificado y a quién se le negará uno.

Existen tres tipos de Autoridades Certificadoras:

- Autoridades Certificadoras Públicas
- Autoridades Certificadoras Comerciales
- Autoridades Certificadoras Privadas

El primer caso se trata de instituciones que ofrecen un servicio público para cuyo acceso se requiere de un Certificado Digital. Éste es el caso de un banco que expide Certificados digitales a sus clientes para poder acceder a sus servicios en línea.

En el caso de las Autoridades Certificadoras Comerciales, se trata de organizaciones que se dedican a vender Certificados Digitales a las personas e instituciones en general. Y por último, tenemos a las Autoridades Certificadoras Privadas, las cuales son internas a una organización.

Los tópicos estudiados en este capítulo sirven para poder montar una Autoridad Certificadora en general, sin importar el tipo que ésta sea.

22.1 ¿Qué tipo de Autoridad Certificadora Requiere la Organización?

La respuesta a esta pregunta, depende de varios aspectos referentes a la misma organización. Si otra organización ha requerido el trámite de un Certificado Digital para un servicio ofrecido o para la comunicación entre organizaciones, es recomendable hacer uso de los Certificados que provee una Autoridad Certificadora Pública. Por ejemplo, podemos tramitar un Certificado con un banco para poder realizar operaciones bancarias con las cuentas de la empresa por Internet. Este es buen momento para reflexionar en contar con una Infraestructura de Certificación propia.

Si la Organización es muy pequeña y/o no se cuenta con la infraestructura computacional necesaria para montar una Certificadora propia, se puede hacer uso de los servicios de una Autoridad Certificadora Comercial. Aunque hay que tener las reservas necesarias al confiar en terceras partes para efectos de Certificación.

En principio, el resto de las organizaciones manejan información importante, la mayoría de éstas cuenta con sistemas computacionales para administrar su información y la mayoría utilizan Internet en su operación diaria. Esas Organizaciones deben proteger su operación informática diaria mediante una infraestructura de Certificación propia.

22.2 ¿Cómo elegir una Autoridad Certificadora confiable?

El tratar de responder esta pregunta trae consigo otra serie de preguntas más:

- ¿Confiable en relación con quién?
- ¿Confiable para qué?
- ¿Confiable para quién?
- ¿Confiable por cuánto tiempo?

Realmente la confianza es un tema que se sale de las cuestiones técnicas de la infraestructura de llave pública, pero debemos tratarlo ya que se debe confiar en una Autoridad Certificadora. Ésta se va a encargar de uno de los aspectos de seguridad más importantes de la Organización.

Entonces debemos contestarnos las cuatro preguntas citadas anteriormente. Realmente son muy difíciles de responder ya que cada Autoridad Certificadora se va a declarar a sí misma confiable.

Realmente esto viene a reforzar un poco más la razón del porqué se debe contar con una propia Autoridad Certificadora. Realmente no sabemos si podemos confiar en terceras partes.

Únicamente está en nosotros el confiar o no en determinada Autoridad Certificadora, no existe una fórmula para poder saber si una Autoridad Certificadora es confiable o no.

Lo único que se puede hacer es dejar en claro que se debe tener mucho cuidado con respecto a las Certificadoras Comerciales, ya que sus Procesos de Certificación muy probablemente resulten débiles, aún para las organizaciones con mínimos requerimientos de seguridad. Además, en el supuesto caso de que se llevase a cabo una

exhaustiva tarea de comprobación de la identidad de un solicitante, es mucho más probable que ésta tarea pueda ser burlada en una Autoridad Certificadora Comercial que dentro de una misma Organización, ya que se tiene al sujeto trabajando ahí mismo y ha pasado un proceso de identificación previo desde la oficina de recursos humanos.

Para muchas de las Certificadoras comerciales, es suficiente realizar el pago de un Certificado para que éste sea expedido, lo cual nos habla de la nula confiabilidad que se les puede tener.

Es por ello que los Procesos de Certificación de una Autoridad Certificadora se deben hacer públicos, si éstos satisfacen al usuario, se puede adoptar esa Autoridad Certificadora si no, se buscará otra. Así queda asentado que lo mejor es contar con una Infraestructura de Certificación propia.

23. Responsabilidad de una Autoridad Certificadora

Definir la Responsabilidad de una Autoridad Certificadora para con sus usuarios (sujetos o entidades que poseen un Certificado Digital expedido por ella) es en realidad un tópico difícil, ya que dichas responsabilidades son aquellas que la misma Autoridad Certificadora quiera tomar.

Una Autoridad Certificadora, por ejemplo, puede tomar toda la responsabilidad de un fraude cometido por el uso de un Certificado que se expidió erróneamente a un individuo haciéndose pasar por otro. Por otro lado, la Autoridad Certificadora puede decidir dejar establecido que no se hace responsable por cualquier uso que se le dé a los Certificados que expidió.

En realidad solamente depende de la Autoridad Certificadora el decidir que garantías y responsabilidades guarda para con sus usuarios, lo que hay que tomar muy en cuenta es que éste es un aspecto muy importante que habla de la seriedad y confiabilidad de una Autoridad Certificadora.

De hecho el usuario y la Autoridad Certificadora deben celebrar un contrato, en el cual se especifiquen las garantías y responsabilidades que tiene la Autoridad Certificadora para con él, y las obligaciones que tiene que guardar el usuario. Si se trata de una Autoridad Certificadora que se dedica a vender Certificados Digitales a las personas en general, de estos factores puede depender el precio del Certificado Digital.

Se deben establecer claramente los siguientes puntos en la relación entre la Autoridad Certificadora y el usuario:

Obligaciones, Autoridad Certificadora

- Notificación de aceptación de Solicitud y expedición de Certificado
- Notificación de expedición de Certificado a los demás usuarios
- Notificación de revocación de Certificado
- Notificación de revocación de Certificado a los demás usuarios

Obligaciones, Usuario

- Protección de la llave privada
- Buen uso de las llaves y el Certificado Digital

- Notificación a la Autoridad Certificadora en caso de pérdida o exposición de la llave privada
- Notificación a la Autoridad Certificadora en caso de detectar un mal uso de Certificado Digital.

Términos de operación:

- Garantías y limitaciones sobre las garantías
- Daños Cubiertos (negligencia, fraude, otros, etc.)
- Acciones en Caso de pérdida o exposición de la llave
- Indemnizaciones

Estos son algunos de los puntos que se pueden incluir en el contrato entre la Autoridad Certificadora y el usuario. La definición de estos términos es total responsabilidad de la Autoridad Certificadora y varía enormemente entre organizaciones, ya que dependen directamente de los estatutos de la institución.

Existe un punto en el que hay que ser demasiado cuidadosos, sin bien es cierto que la responsabilidad que toma una Autoridad Certificadora es totalmente decisión propia, de las responsabilidades que tome, se debe vigilar su cumplimiento de manera impecable, ya que si hay in contrato de por medio, se podrían enfrentar responsabilidades legales.

24. Interacción entre Autoridades Certificadoras

24.1 Certificación de una Autoridad Certificadora

Ya conocemos cuales son las funciones, obligaciones y responsabilidades de una Autoridad Certificadora, pero lo que aún no conocemos es a la entidad que facultó a nuestra Autoridad Certificadora a operar como tal. La pregunta es: ¿Quién Certificó a nuestra Autoridad Certificadora?

La Certificación de una Autoridad Certificadora se da a través de otra Autoridad Certificadora, mediante lo que se conoce como Certificado de Autoridad Certificadora. Este Certificado se expide a Autoridades Certificadoras para darles el aval para poder operar.

En el ámbito mexicano, el Banco de México es una Autoridad Certificadora que puede certificar a nivel nacional. En el ámbito internacional existen grandes Autoridades Certificadoras a nivel mundial como lo son RSA, American Express, VerySign, etc.

24.2 Trámite de un Certificado de Autoridad Certificadora

Para llevar a cabo el trámite de un Certificado de Autoridad Certificadora los dos Administradores de las Autoridades Certificadoras deben reunirse. Siempre debe haber una Autoridad Certificadora que solicita el Certificado (Autoridad Certificadora Solicitante) y otra que recibe la solicitud (Autoridad Certificadora Padre).

Ambos administradores deben estudiar los Procesos de Certificación que cada una utiliza y se debe verificar la compatibilidad entre ellos. La Autoridad Certificadora solicitante tendrá que ajustarse a las políticas y procesos de Certificación que la Autoridad Certificadora Padre le imponga. La Autoridad Certificadora Padre puede simplemente aceptar los Procesos de la Autoridad Certificadora solicitante y darle el aval después de haberlos estudiado, sin imponerle alguno.

La Autoridad Certificadora Padre tiene que verificar la confiabilidad, los procesos y sobre todo asegurarse de que la Autoridad Certificadora solicitante sea una entidad digna de confianza y de su certificación. Si el Administrador de la Autoridad Certificadora Padre se encuentra satisfecho con la identidad y procesos de la Autoridad Certificadora solicitante, entonces puede proceder a expedirle su Certificado de Autoridad Certificadora.

La Autoridad Certificadora que recibe el certificado no debe expedir Certificados con un periodo de vida mayor al que le marca su propio Certificado de Autoridad Certificadora. El Administrador debe mantener en mente la fecha de expiración del Certificado para poder renovarlo con anticipación.

Bajo este esquema de cooperación entre Autoridades Certificadoras podemos darnos cuenta de que también es posible que varias Autoridades Certificadoras trabajen conjuntamente. Pueden compartir políticas, algunos procesos, ideas y certificarse entre sí formando con esto Cadenas de Autoridades Certificadoras.

25. Cadenas de Autoridades Certificadoras

Como ya lo vimos, las cadenas de Autoridades Certificadoras se dan cuando Autoridades Certificadoras se certifican entre sí, compartiendo comportamientos en común o simplemente avaladas unas entre otras.

El gran problema de esta práctica es que eventualmente se llegará a una Autoridad Certificadora que se Certifica a sí misma y para los esquemas de confiabilidad, eso no es lo más adecuado.

Si eventualmente tiene que haber Autoridades Certificadoras que se Certifican a sí mismas, entonces queda claro que no es necesario poseer un Certificado de Autoridad Certificadora para poder operar como tal. El Certificado de Autoridad Certificadora es únicamente para agregar confiabilidad a la Autoridad Certificadora. Lo más recomendable es asociarse y que exista la Certificación entre Autoridades Certificadoras, que conformen una elite confiable, que se establezcan como verdaderas autoridades y que tengan la potestad de Certificar.

Es muy difícil el poder establecer una armónica relación entre Autoridades Certificadoras, el gran problema es que cada una puede tener diferentes Procesos de Certificación que aplican para sus intereses pero que pueden resultar inaplicables o

contrarias a las de otras Autoridades Certificadoras provocando la incompatibilidad entre estas. Esto nos lleva a que cada Autoridad Certificadora tenga sus propios clientes y a que no haya compatibilidad entre usuarios en algunos casos.

Es por ello que lo más recomendable para la seguridad de todos es que se llegaran a estandarizar los Procesos de Certificación y que pudiera existir una cooperación transparente entre Autoridades Certificadoras.

25.1 ¿Cómo funcionan las Cadenas de Autoridades Certificadoras (Cadenas de Certificación)?

Como ya lo hemos estudiado, las Autoridades Certificadoras se pueden Certificar unas a otras. La finalidad de la Certificación mutua, es formar Cadenas de Autoridades Certificadoras, y la finalidad de formar una Cadena de Autoridades Certificadoras es la de formar un grupo de Autoridades Certificadoras confiables.

De esta manera se crea un lazo de confianza, ya que la Autoridad Certificadora que Certifica a otra, está de acuerdo en sus Procesos de Certificación. Y no sólo eso, sino que le tiene la suficiente confianza como para certificarla como una Autoridad Certificadora confiable.

El hecho de Certificarse entre Autoridades Certificadoras nos puede ayudar en el aspecto de la confianza, pero en el punto más alto de la cadena, habrá una Autoridad Certificadora que no está Certificada por nadie, o visto de otra manera, está siendo certificada por ella misma. A esta Autoridad Certificadora se le conoce como Autoridad Certificadora Raíz y es la que al final de cuentas Certifica a todas las demás en la cadena de certificación. La Cadena de Autoridades Certificadoras está organizada como una jerarquía en donde todas parten de la Autoridad Certificadora Raíz.

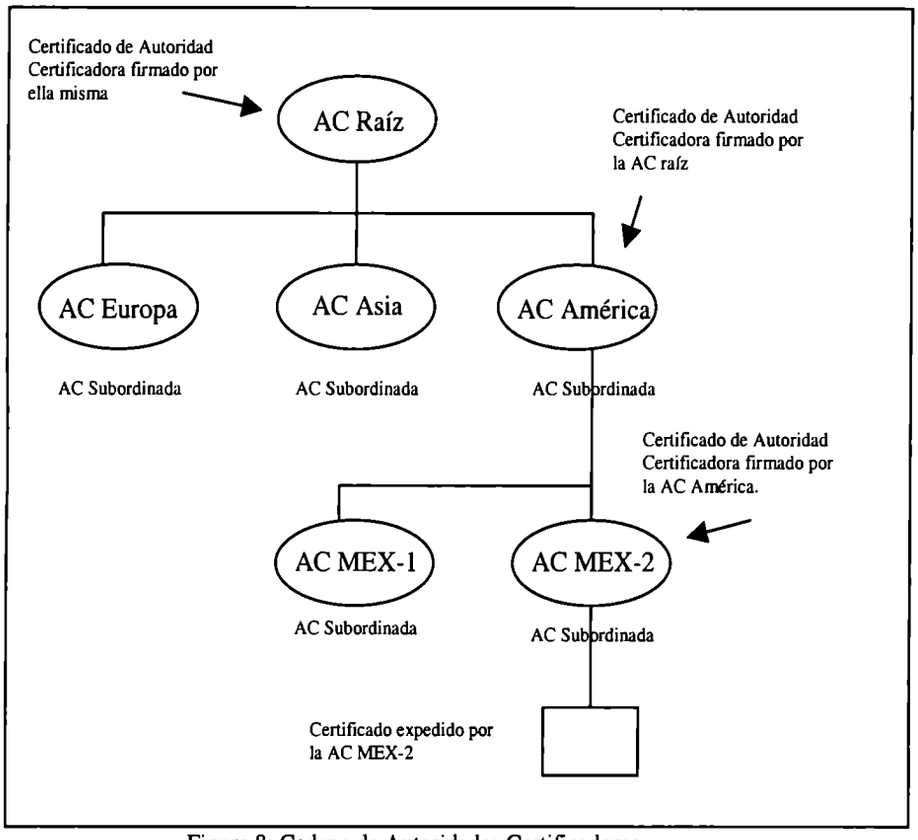

Figura 8: Cadena de Autoridades Certificadoras

Como la Autoridad Certificadora Raíz no ha sido certificada por ninguna otra, ésta debe demostrar por si sola y a través de sus Procesos de Certificación, que es una Autoridad confiable.

Una cadena de certificación consiste de un Certificado, el certificado de una Autoridad Certificadora firmado por el primer Certificado, el Certificado de una Autoridad Certificadora firmado por el Certificado de la Autoridad Certificadora que fue firmado con el primer Certificado, y así sucesivamente.

Básicamente una Cadena de certificación traza el camino desde las hojas hasta la Raíz, dentro de la jerarquía tipo árbol. En una Cadena de certificación ocurre lo siguiente:

- Cada Certificado es seguido por el Certificado de quien lo expidió.
- Cada Certificado contiene el nombre de quien lo expide, quien es sujeto del siguiente Certificado en la cadena (ver figura 7).

- Cada Certificado es firmado con la llave privada de la Autoridad que lo expidió. La firma puede ser verificada con la llave pública incluida en el Certificado de la Autoridad Certificadora que lo expidió. Éste es el siguiente Certificado en la cadena.

El certificado de la Autoridad Certificadora Raíz, se encuentra firmado por ella misma. Esto es, se encuentra firmado usando la llave privada correspondiente a la llave pública de su Certificado. Esta es una Autoridad Certificadora que se certifica a sí misma, por lo que hay que tener cuidado en verificar que este tipo de Autoridades Certificadoras sean realmente dignas de confianza.

De la misma manera, una Autoridad Certificadora que ha trabajado en sus Procesos de Certificación, y que ha construido buena reputación, debe tener especial cuidado en expedir Certificados de Autoridad Certificadora, ya que estas entidades deben ser también de buena reputación. La Autoridad Certificadora que expide un Certificado de Autoridad Certificadora a otra, debe prohibir a esta última que a su vez expida Certificados de Autoridad Certificadora sin su autorización, de lo contrario se perdería el control y se terminaría por Certificar a una Autoridad Certificadora no confiable de manera indirecta.

Dependiendo de los arreglos, estatutos y convenios establecidos, el certificar de manera directa o indirecta a una Autoridad Certificadora no confiable puede traer problemas a la Autoridad Certificadora Padre.

26. Compatibilidad entre Autoridades Certificadoras

Cada Autoridad Certificadora es libre de implementar sus propias políticas y de llevar a cabo sus muy particulares Procesos de Certificación. Es por ello que es muy poco probable que pueda existir compatibilidad entre los Certificados expedidos por

diferentes Autoridades Certificadoras. Es por ello que las autoridades Certificadoras que deseen tener interacción, definan un esquema de compatibilidad.

Esta es una gran desventaja de X509, ya que al dejar completamente abierto el aspecto de los Procesos de Certificación, se crean incompatibilidades resultando en la creación de Islas de Certificación que no son compatibles con nadie. Los sistemas abiertos han representado un gran poso para la compatibilidad de los sistemas modernos, pero este no es el caso para los Certificados Digitales, aun hay mucho camino por recorrer. Se espera que este trabajo sea uno de los pasos que hacen falta por dar.

27. Seguridad física de una Autoridad Certificadora

De la misma manera que se cuida la seguridad computacional, en su parte lógica, también debe existir seguridad física de la Autoridad Certificadora. Los aspectos generales que se deben cuidar son los siguientes:

- Acondicionamiento adecuado del sitio: La Oficina de Certificación debe residir en un espacio cerrado, de acceso restringido, acondicionado con un área de recepción y atención al público y otra área de servidores.

- Acceso Físico: Se debe vigilar la entrada a la oficina de Certificación y se debe autorizar el acceso al área de Servidores, únicamente al personal autorizado.

- Alimentación eléctrica: Se debe vigilar que nunca falle el suministro de energía eléctrica.

- Aire Acondicionado: El área de Servidores debe contar con la ventilación y clima adecuados para los equipos.

- Exposición del Equipo al agua: No se debe exponer el equipo al agua.

- Alimentos: No se podrá consumir alimentos en el área de servidores.

- Medidas de Prevención de incendios: Se deben tener medidas para prevenir incendios.

- Protección de los medios de almacenamiento: Se deben guardar los medios de almacenamiento como, cintas de respaldo, cartuchos, etc. en una caja de protección de documentos contra fuego y sustancias varias.

- Respaldos : Se debe tener un plan para respaldar la información periódicamente.

28. Una visión global de la Autoridad Certificadora

Una vez establecidos los Procesos de Certificación de una Autoridad Certificadora, podemos abstraernos y tener una visión global de la Autoridad Certificadora y su entorno. Para ello nos ayudaremos de dos diagramas, el primero nos presenta el entorno global de una Autoridad Certificadora, y el segundo presenta los procesos más relevantes que leva a cabo una Autoridad Certificadora.

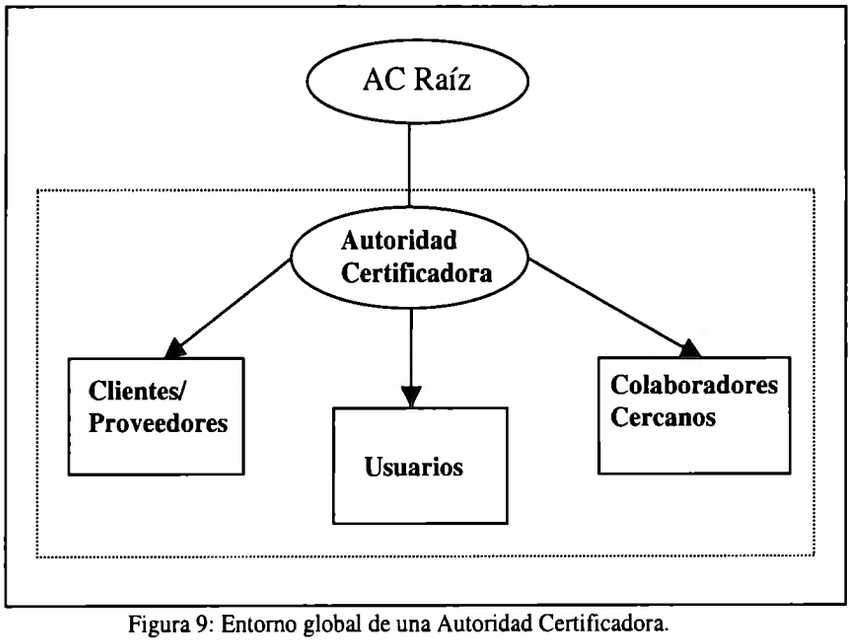

Figura 9: Entorno global de una Autoridad Certificadora.

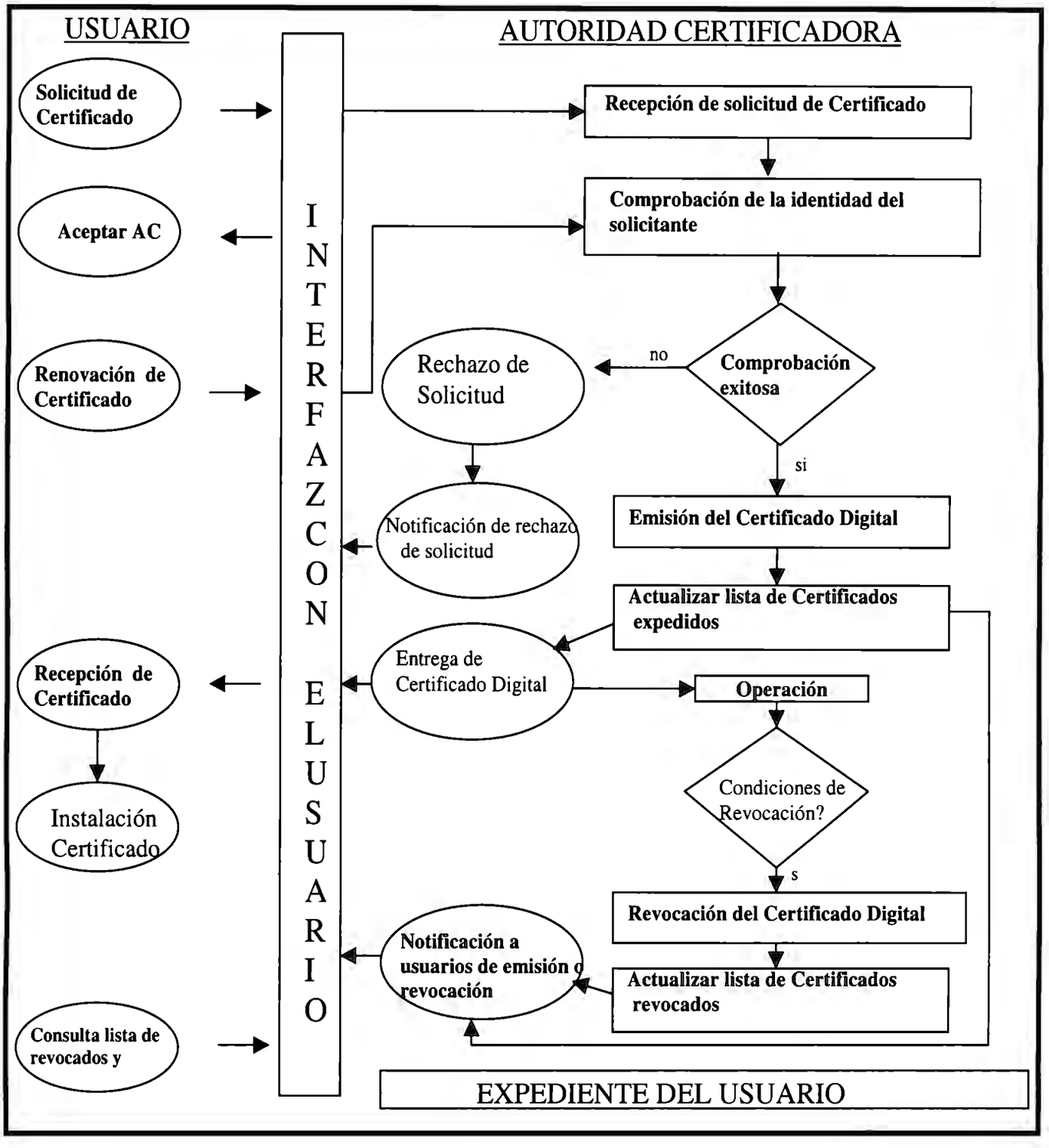

Figura 10: Diagrama general de proceso de una Autoridad Certificadora

29. ¿Porqué tener una Autoridad Certificadora en la Organización? (Problemática que resuelve)

Las organizaciones de hoy en día, dependen cada vez más del Internet para realizar sus tareas. Éstas pueden ser tan cotidianas y simples como el correo electrónico, o tan complejas como una transacción monetaria, compras, ventas o comercio electrónico sobre Internet.

Actualmente muchas organizaciones proveen el servicio de ventas por Internet a sus clientes, ellas mismas realizan compras por Internet o se contactan con sus proveedores y colaboradores cercanos también por Internet. El crecimiento es tal, que las organizaciones están utilizado la infraestructura de Internet para montar sus sistemas privados y en muchos de los casos, tener acceso a ellos desde cualquier parte del mundo, en lo que popularmente se conoce como una Intranet.

Esta dependencia sobre las redes públicas, requiere de una infraestructura de seguridad capaz de proteger nuestra operación informática diaria de las debilidades propias de un sistema de red pública tan grande como lo es Internet. Dentro de la Organización no podemos permanecer sin reaccionar ante los graves problemas de seguridad computacional que existen en todos los sistemas del mundo, ya que si no se toman medidas de protección para nuestros sistemas e información, la organización será un blanco y muy seguramente sufrirá ataques informáticos.

Algunos de los aspectos de la seguridad computacional que requieren de especial cuidado, son la confidencialidad, integridad y privacidad de la información. Además de una autenticación robusta. Estos aspectos pueden ser cuidados utilizando una robusta infraestructura de llave pública en conjunción con los Certificados Digitales y su respectiva Autoridad Certificadora.

Existen empresas que se dedican a proveer el servicio de Certificación, estas son las llamadas Certificadoras Comerciales, y se dedican a vender Certificados Digitales y a certificar entidades en Internet.

En respuesta a la pregunta del ¿porqué tener una Autoridad Certificadora en la Organización?, debemos recordar que una Autoridad Certificadora es un ente confiable, en el cual delegamos la responsabilidad de comprobar la identidad de una entidad en la red, certificarla y asignarle su llave privada. Es aquí donde entramos en la cuestión de la confianza, la Autoridad Certificadora debe ser confiable y la organización debe tenerle mucha confianza, ya que le está delegando algo tan importante para su operación diaria como lo es la seguridad de su información.

Para que una Autoridad Certificadora pueda expedir un Certificado a una entidad en la red, la Certificadora debe estar satisfecha con la identidad del solicitante antes de expedirle un Certificado Digital, pero:

- ¿La Organización esta satisfecha con la identidad de dicha entidad?
- ¿Los procesos que se llevaron a cabo para certificarla son suficientes, acorde a las necesidades de seguridad de la Organización?
- ¿Conocemos los Procesos de Certificación?
- ¿Realmente se llevaron a cabo los procesos de Certificación estipulados por la Autoridad Certificadora?

No hay nada mejor que tener el dominio completo de la seguridad de nuestra propia Organización. Es muy arriesgado delegar al cien por cien responsabilidades a terceras partes y más si se trata de la información de la empresa, que es considerada un activo virtual [1].

Es por ello que se recomienda ampliamente el contar con una Autoridad Certificadora dentro de la Organización, para que ésta funcione perfectamente de acuerdo a las

necesidades de seguridad de nuestra empresa y nos provea de la seguridad que provee la tecnología de llave pública en conjunto con los Certificados Digitales.

Todas las Organizaciones manejan información importante, y la mayoría de las Organizaciones cuenta con sistemas computacionales para administrar dicha información. Además, la mayoría de las Organizaciones utilizan Internet en su operación diaria, es por ello que deben tomar medidas en materia de seguridad computacional y contar con una Infraestructura de Certificación propia.

30. Implementar una Autoridad Certificadora en la Organización

Una vez decidido que se montará una Autoridad Certificadora en la organización, ésta se puede implementar basándose en lo estudiado a lo largo de este capítulo. En este capítulo se encuentra descrito todo lo necesario para poder llevar a cabo esa tarea, además se describen los Procesos de Certificación bajo los cuales debe estar gobernada la Autoridad Certificadora. Adicionalmente, en este trabajo de tesis se presenta una herramienta de software para poder montar una infraestructura de Certificación, en el capítulo "El Servidor de Certificados Netscape".

31. Uso de Certificados dentro de la Organización

En esta sección estudiaremos un poco más acerca de la incorporación de los Certificados Digitales en la operación ordinaria de una Organización.

Como ya lo hemos estudiado, los Certificados Digitales son una de las aplicaciones más importantes de las tecnologías de llave pública, es por ello que nos sirven para firmar digitalmente mensajes, encriptar mensajes, desencriptar mensajes, autenticarnos, etc. Dentro de la operación cotidiana de una Organización todas estas operaciones se pueden llevar a cabo basándose en los siguientes lineamientos.

31.1 ¿Qué Documentos deben ir Firmados Digitalmente?

Todo documento (mensaje) que firmamos digitalmente, se puede pensar como un documento al que le hemos estampado nuestra firma manuscrita, por lo tanto, quien firma un mensaje digitalmente, tiene toda la responsabilidad sobre él y debe responder por el contenido de dicho mensaje.

Además el remitente no puede negar haber enviado el mensaje ya que en éste se encuentra estampada su firma digital y para hacerlo necesitó de su llave privada, a la cuál sólo él tiene acceso.

Algunos de los mensajes o documentos digitales que se recomiendan deban ir firmados digitalmente son:

- Ordenes del jefe a sus empleados
- Memorándums
- Comunicados Oficiales
- Avisos de la Dirección
- Avisos Oficiales de Otras áreas
- Mensajes de interacción con nuestros clientes (facturas, cotizaciones, etc.)
- Peticiones de información entre áreas
- Interacción entre áreas ó departamentos
- Información de rutina entre los miembros de la Organización

31.2 ¿Qué documentos deben ir encriptados?

Los documentos o mensajes que se envían por la red, siempre corren el peligro de ser vistos por personas que se dedican a espiar por la red, inclusive dentro de la misma Organización. Es por ello que a nuestra información importante que viaja por la red se le debe dar un trato especial de mayor cuidado, por lo que debe ir encriptada.

Algunas de las comunicaciones que deben encriptarse son las siguientes:

- Comunicación entre Directivos
- Información Confidencial
- Contratos
- Manejo de cifras e información confidencial (sueldos, estados contables, estados de cuenta, etc.)
- Información que no debe caer en manos de la competencia

31.3 ¿Qué documentos pueden no ir firmados ni encriptados?

Algunas comunicaciones de menor importancia, pueden no ir encriptados ni firmados, aunque es muy recomendable que todo mensaje salga por lo menos firmado.

Algunas de las comunicaciones que pueden carecer de firma o encripción pueden ser:

- Comunicación a nivel personal entre los miembros de la organización
- Comunicaciones sin relación con la Organización

31.4 ¿Qué tipos de Acceso a sistemas requieren de Certificado Digital?

En principio todo acceso a los Servicios computacionales de la Organización debería estar restringido a la presentación de un Certificado Digital. Pero debido a que este tipo de tecnología aún no se ha desarrollado del todo, se puede migrar poco a poco del antiguo control de acceso, basado en contraseñas, a uno basado en Certificados Digitales.

Se puede tomar como base la siguiente guía:

- En primera instancia, todo acceso de nivel Administrador debe estar sujeto a la autenticación por medio de Certificados Digitales.

- La Autenticación para el Acceso a los Servidores Críticos de la Organización se debe hacer por medio de Certificados Digitales.
- Todo acceso a los recursos computacionales desde fuera de la Organización se debe hacer presentando un Certificado Digital.
- El Acceso a las aplicaciones críticas de la Organización se debe restringir mediante el uso de Certificados Digitales.

Gradualmente se debe migrar el control de acceso a todos los servicios computacionales al uso de Certificados Digitales, comenzando por los más críticos hasta terminar con los menos críticos.

32. Terminación de una Autoridad Certificadora

El periodo de vida de una autoridad Certificadora es finito. En determinado momento la Autoridad Certificadora debe dejar de existir. Las razones por las que una Autoridad Certificadora deba terminar son muchas. Algunas de las razones pueden ser: La exposición de la llave de la Autoridad Certificadora, fin de la Organización, partida del Administrador de la Autoridad Certificadora o simplemente la decisión de dejar de operar. Para poder dar buen termino a una Autoridad Certificadora, se deben llevar a cabo las siguientes acciones:

1. Dar aviso a todos los usuarios de la Autoridad Certificadora de la terminación de la misma.
2. Dar aviso a todos los colaboradores cercanos (clientes, proveedores, etc.) y a las Autoridades Certificadoras que mantienen interacción con ésta, de su terminación.
3. Debido a que la Autoridad Certificadora ha terminado, los Certificados que ha expedido ya no serán validos por lo que deberán revocarse, al no haber una Autoridad Certificadora que los respalde.
4. Se debe notificar a los que no son usuarios, de la terminación de la Autoridad Certificadora, es decir, se deben colocar todos los Certificados en la lista de Revocados y esta lista debe permanecer accesible a todo el mundo.

En dado caso que la llave da la Autoridad Certificadora se haya perdido o expuesto, irremediablemente se debe terminar la Autoridad Certificadora, ya que de esta manera cualquiera podría falsificar un Certificado con relativa facilidad. Este es el mismo caso si el Administrador de la Autoridad Certificadora deja de laborar en la Oficina de Certificación, a pesar de que se lleve a cabo un cambio de contraseñas y de acceso a la llave privada, cabe la duda de que el anterior administrador haya conservado una copia de las llaves y hacer mal uso de ellas.

Capítulo 5

El Servidor de Certificados Netscape

El Servidor de Certificados de Netscape, no es una Autoridad Certificadora es únicamente una herramienta de software en la cuál se apoyará una Autoridad Certificadora.

Una Autoridad Certificadora es un sistema complejo, constituido por los sistemas computacionales para realizar las tareas criptográficas y el manejo de Certificados. Además se compone por los recursos humanos y los Procesos de Certificación.

De hecho, los Procesos de Certificación son la verdadera identidad de una Autoridad Certificadora y no el software que se utiliza para la implementación de las cuestiones

técnicas. Para la descripción de los Procesos de Certificación se ha dedicado el capítulo "Autoridad Certificadora" en su totalidad.

En esta sección se describirá paso a paso y de manera detallada, la instalación, configuración, operación y administración del Servidor de Certificados de Netscape.

Por lo general, el manejo de Certificados Digitales y el manejo de una Infraestructura de Certificación, son cuestiones que representan gran dificultad. Se debe tener una preparación técnica de alto nivel para poder llevar a cabo estas tareas, ya que traen consigo una gran carga de conceptos de naturaleza compleja.

En esta sección, se tratará de manejar de la manera más sencilla posible los conceptos detrás del Servidor de Certificados de Netscape, para hacer accesible a la mayoría de los Administradores de sistemas su implementación, operación y administración.

1. Instalación del Servidor de Certificados Netscape

1.1 Condiciones Iniciales

El Servidor de Certificados de Netscape, está sujeto a los términos detallados en el acuerdo de licencia. Para poder hacer uso de este producto, éste debe estar perfectamente licenciado.

Esta sección está parcialmente orientada a la plataforma Windows NT, ya que es la plataforma operativa más popular en la actualidad. Pero no hay que perder de vista que el proceso de instalación es básicamente el mismo sobre cualquier plataforma. El resto de los procesos no difieren de plataforma en plataforma.

1.2 Requerimientos Técnicos

- Windows NT 3.5 o superior con Service Pack 4
- 64 MB de memoria RAM
- Red TCP/IP con el protocolo DHCP sin estar habilitado

- Descompresor de Archivos para Windows
- Una partición del tipo NTFS
- Navegador Netscape 3.0 o superior

1.3 Requerimientos de Almacenamiento secundario

- 25 MB para instalar el software del Servidor de Certificados
- 20 MB para instalar el software del Servido de Base de Datos
- 20 MB para la Base de Datos de los Certificados

Es muy probable que se llegue a requerir mayor espacio para almacenar los certificados en la base de datos. La cantidad de 20MB es suficiente para manejar 2000 certificados con sus correspondientes 2000 solicitudes. Se deben añadir 6MB adicionales de espacio por cada 1000 Certificados adicionales.

1.4 El paquete de Instalación

El paquete de instalación consta, entre otros, de los siguientes archivos importantes:

- OWS712NT.ZIP, Paquete de Instalación del Servidor de Base de Datos
- CERTSVC.EXE, Paquete de Instalación para el Servidor de Certificados

Para poder llevar a cabo la instalación es necesario iniciar una sesión en el servidor y cambiarse a un directorio temporal. Desde este directorio se llevará a cabo la instalación y debe ser diferente al directorio destino del software.

1.5 Configuración de Red

En cuanto a las configuraciones de Red, se deben tomar en cuenta los siguientes puntos:

- Hay que asegurarse de que el protocolo DHCP de encuentre desactivado
- El nombre del host TCP/IP, debe ser el Nombre de Dominio Calificado completo dado de alta en el DNS (Ejemplo: nikita.cem.itesm.mx)

- Si el servidor se encuentra en un dominio de firewall interno, se debe usar el dominio interno en lugar del Dominio externo.
- El nombre del host para redes Windows debe ser el nombre no calificado del nombre de Dominio. Es decir, si el nombre completo de Dominio es "nikita.cem.itesm.mx", el nombre de redes Windows deberá ser "nikita".

2. El Servidor de Base de Datos

El Servidor de Certificados de Netscape, cuenta con un Servidor de Base de Datos Informix. Su finalidad principal es la de administrar la Base de Datos de los Certificados Digitales. Además de tan importante función, puede ser un apoyo a otras tareas, almacenando información de operación diaria de la Autoridad Certificadora, configuraciones y control de usuarios.

2.1 Importancia de la Base de Datos

La función que cumple la base de datos dentro de todo el complejo de la Autoridad Certificadora es fundamental, ya que en ella se almacenan y administran materias primas para la Autoridad Certificadora como lo son los Certificados Digitales mismos.

Además de almacenar los Certificados Digitales, sus características y sus parámetros operacionales, la Base de Datos también almacena información de la configuración del Servidor de Certificados y del control de usuarios.

A pesar de su importancia, el manejo de la base de datos es transparente para los administradores del Servidor de Certificados. Por lo general el Administrador, poco interesado en el manejo de Bases de Datos, pocas veces se da cuenta de la interacción que el Servidor de Certificados tiene con ésta, pero sin lugar a dudas no se puede perder de vista que sin el Servidor de Base de Datos el Servidor de Certificados no puede funcionar.

2.2 Cuidado de la Base de Datos

Falsamente se podría pensar que al ser una base de datos que almacena todos los Certificados de la Autoridad Certificadora, podría convertirse en un blanco de ataques por parte de personas interesadas en poseer toda esa información. Lo que hay que tomar en cuenta es que esta información al final de cuentas es pública, y todo mundo puede tener acceso a ella.

De esta manera, el móvil de un ataque no sería el apoderarse de todos los Certificados Digitales, mas bien sería con la finalidad de afectar de manera importante a la Autoridad Certificadora ya que se estaría atacando su centro operacional.

Es por ello que se le deben tener las precauciones debidas a nuestra BD como hacerle respaldos, restringir el acceso, etc. El Servidor de Base de Datos Informix, cuenta con las herramientas necesarias para poder llevar a cabo la administración de la Base de Datos, sin embargo se recomienda fuertemente que quienes vayan a tener a su cargo la Base de Datos de una Autoridad Certificadora, se documenten de forma importante en el área de la administración de Bases de Datos.

2.3 Instalación y Configuración del Servidor de Base de Datos

A continuación son descritos los pasos para llevar a cabo la instalación del Servidor de Base de Datos Informix, para el servidor de Certificados Digitales de Netscape:

1. Para poder instalar el Servidor de Base de Datos, primero es necesario descomprimir el archivo "ows712nt.zip" del paquete de archivos provistos por el proveedor. Los archivos descomprimidos quedan en un subdirectorio llamado owsnt4.0 .

2. Como segundo paso, se debe ejecutar el comando "setup.exe" generado de la descompresión de los archivos del paso anterior.

3. El proceso de instalación se divide en tres partes:

1) Proveer información personal y seleccionar las opciones de instalación.

3) Copiar los archivos.

4) Configurar el Servidor de Base de Datos.

4. Ingresar el número de serie y la llave del producto

5. Ingresar datos personales (nombre, título y compañía, dirección, e-mail, etc.)

6. Después de haber ingresado los datos personales, el instalador pregunta por el software a ser instalado, elegir instalar el Servidor de BD y herramientas de administración, esto es muy conveniente ya que se proveen herramientas que auxilian a las labores de administración de la Base de Datos. Además se debe especificar el directorio en el cual serán instaladas las aplicaciones.

7. El usuario puede elegir entre realizar la instalación típica, mínima u optimizada. Todas varían entre sí en el espacio en disco que ocupan para el almacenamiento de los certificados, los archivos de registro de actividades (logs) y los respaldos. Aproximadamente se requieren 20MB para inicialmente manejar 2000 Certificados con sus respectivas 2000 solicitudes. Se deben añadir 6 MB por cada 1000 certificados adicionales.

8. Después de que el instalador haya copiado los archivos al disco duro, se debe configurar el servidor de Base de Datos. Primeramente se le debe dar un nombre, el nombre predeterminado es "ol_NombreDelaMaquina". Se puede elegir entre dejar este nombre o cambiarlo a gusto del usuario.

9. Posteriormente se debe elegir el nombre de la Base de Datos. Se recomienda que sea el mismo que el servidor de Base de Datos para evitar confusiones.

10. Se debe elegir la partición y un fragmento en Megabytes de la misma partición para que el servidor almacene la información. También se puede elegir una localidad espejo para la información. Es altamente recomendable que la información se encuentre replicada en una localidad espejo localizada en

diferente partición a la original. Las opciones predeterminadas por lo general son buena opción para elegir.

11. Después, se debe seleccionar el dispositivo de respaldo. Éste puede ser un directorio dentro del mismo disco duro.

12. También se debe seleccionar el dispositivo para almacenar los archivos de registro de actividades (logs). Éste puede ser un directorio dentro del mismo disco duro.

13. De manera automática es añadido un usuario al dominio. Éste será el administrador de la Base de Datos. Hay que asignarle una contraseña de administrador. El usuario siempre se llama "informix" y es muy importante que se le cambie la contraseña predeterminada.

14. Se puede elegir una maquina dentro del dominio o fuera de él como SQLHOST compartido. Ésta se convierte en cliente del Servidor de la Base de Datos y puede tener acceso a ella. Por seguridad se recomienda que sea el mismo host local o una maquina dentro del mismo dominio ya que se debe tener el mismo usuario.

15. Posteriormente comienza la fase de Inicialización del Servidor de Base de Datos, este proceso puede tardar unos minutos.

16. Se ha creado el Grupo de Dominio "Admin_Informix" y el usuario global "informix". Se debe añadir usuarios al grupo para administrar la Base de Datos.

17. Se debe re iniciar el sistema para que se efectúen las modificaciones al registro.

18. Es necesario Iniciar el Servidor de Base de Datos, auxiliándose de las herramientas instaladas. Para esta labor se debe utilizar el "Command Center" y poner el servidor en línea y disponible.

19. Por último se debe crear un usuario de Dominio, que el Servidor de Certificados utilizará para conectarse con la Base de Datos, se recomienda el nombre de "cmsdbuser".

3. Instalación del Administrador de Servidores Netscape

Por lo general los servidores Netscape son administrados a través de una herramienta llamada "Administrador de Servidores" (Netscape Administration Server). Se debe contar con esta herramienta antes de que el Servidor de Certificados pueda ser instalado. Es por ello que la instalación del Administrador de Servidores es el primer paso después de ejecutar el comando "certsvc.exe". Dicho comando es el que instalará nuestro Servidor de Certificados, pero antes, se debe instalar y configurar el Administrador de Servidores.

El Administrador de Servidores nos sirve para configurar, administrar, prender o apagar el Servidor de Certificados. A continuación se listan los pasos para instalar y configurar el Administrador de Servidores:

1. Ejecutar el comando "certsvc.exe"; Aparecerá una leyenda indicando que este programa instalará el Servidor de Certificados.

2. Aceptar el acuerdo de licencia de uso del producto y se debe escoger el directorio destino de instalación. Después de ello los archivos de la aplicación se copiarán al disco duro.

3. Configurar el Administrador de Servidores
   a) Dar el nombre del servidor (Ejemplo: campus.cem.itesm.mx)
   b) Dar el nombre del usuario que fungirá como administrador del Administrador de Servidores y establecerle una contraseña.
   c) Asignarle un número de puerto. Éste será el puerto escuchado por el Administrador de Servidores y es diferente e independiente al de otros Servidores. Es recomendable escoger la opción ya presentada de forma predeterminada por el sistema.

d) El Administrador de Servidores corre como un cierto usuario en el sistema. Este usuario debe ser diferente a un usuario bajo el cual corre el servidor de web. Éste será el único usuario que podrá escribir en los archivos de configuración.

4. Después de haber configurado el Administrador de Servidores, el proceso ha terminado. Es necesario correr el Administrador de Servidores para poder instalar un nuevo Servidor de Certificados.

4. Instalación del Servidor de Certificados

Una vez instalado y configurado el Administrador de Servidores, se debe arrancar éste para poder instalar un nuevo Servidor de Certificados. Los pasos para instalar el Servidor de Certificados son los siguientes:

1. Ejecutar el Administrador de Servidores y elegir Instalar un nuevo Servidor de Certificados.
2. Ingresar la información que se solicita
   a) Nombre del Servidor: Dar el nombre de Dominio calificado completo del servidor o el alias dado de alta en el DNS (Ejemplo: nikita.cem.itesm.mx)
   b) Dirección de Enlace: Este campo aplica sólo si el servidor corre en una máquina con múltiples direcciones IP, y si el servidor debe escuchar sólo a una de las dos. Ésta es la dirección que se debe especificar en este campo. El campo debe dejarse en blanco si la máquina sólo tiene una dirección IP.
   c) Puerto: Proveer el número de puerto en el que correrá el servidor, éste puede ser un número entre 1 y 65535. El puerto estándar par el protocolo HTTPS es el 443. Si se usa un puerto diferente se tendrá que especificar el puerto en el URL para tener acceso el Servidor de Certificados, por lo que se recomienda dejar el puerto predeterminado.
   d) Identificador del Servidor: Se le debe dar un nombre al servidor que lo identifique, este nombre será usado en el Administrador de Servidores.
   e) Para este punto, la instalación del Servidor de Certificados debió resultar exitosa y se debe elegir la opción de realizar mayores configuraciones al nuevo servidor.

5. Configuración del Servidor de Certificados Netscape

La Configuración del Servidor de Certificados se encuentra dividida en siete pasos. Cada uno de los pasos contiene sus respectivas instrucciones. El seguir estos pasos sin conocer la Teoría de Certificados Digitales, explicada en el capítulo del mismo nombre, no será posible. Es por ello que se recomienda la lectura previa de ese capítulo. A continuación se explican los siete pasos para poder configurar el Servidor de Certificados:

1. ***Generación de las llaves para la Autoridad Certificadora***: Se deben generar la llave pública y la llave privada de la Autoridad Certificadora, estas llaves son usadas para crear y verificar firmas digitales para los certificados expedidos por la Autoridad Certificadora. La llave privada se almacena encriptada usando una clave especificada por el usuario. Debido a la gran importancia que tiene esta llave, ésta debe estar en un directorio perfectamente seguro.

   Para generar la generación de llaves, el Servidor de Certificados provee el programa "gen-sgn-key". Están disponibles dos tamaños de llaves 512 o 1024 bits. El tamaño recomendado es de 1024 bits. Para dicho tamaño el comando sería el siguiente:

   gen-sgn-key –k 1024

   También se debe especificar la locación donde residirá el archivo con las llaves y el nombre del archivo. Es recomendable utilizar otra localidad diferente a la sugerida, de tal manera que sea una localidad únicamente conocida por el administrador. Por último se debe proveer una contraseña para proteger a la llave privada, ésta contraseña será requerida cada vez que el servidor sea arrancado.

2. ***Generación de las llaves para comunicaciones SSL***: También se debe generar el par de llaves para las comunicaciones SSL. Este par de llaves es utilizado por el servidor para mantener comunicación segura con sus clientes a través de la red.

El proceso de generar las llaves SSL es esencialmente el mismo que se efectuó en el paso anterior, únicamente se debe elegir diferente nombre de archivo y locación, además de diferente contraseña. El comando para la generación de estas llaves es "sec-key".

3. ***Configuración de la Base de Datos***: La base de datos que almacenará los Certificados debe ser configurada para que el Servidor de Certificados pueda hace uso de ella, la información que debe proveerse es la siguiente:
   a) Servidor de Base de Datos: Este es el nombre definido durante la instalación de la base de datos (ol_NombreDelaMaquina).
   b) Nombre de la base de Datos: Dar el nombre de la instancia de la base de datos que el Servidor de Certificados debe usar para su base de datos en el servidor especificado.
   c) Usuario de la Base de Datos: Dar el nombre del usuario que el Servidor de Certificados debe usar para obtener acceso a la base de datos. Este usuario debió haber sido creado en el grupo Informix-Admin y puede ser el sugerido "cmsdbusr"

4. ***Expedición del Certificado de Autoridad Certificadora***: En este paso se debe escoger un nombre para la Autoridad Certificadora, éste nombre permanecerá mientras dure la Autoridad Certificadora y no podrá ser cambiado bajo ninguna circunstancia. De hecho es muy importante que se esté seguro de la información provista en esta forma ya que no podrá ser modificada.

   La información que se debe proveer es la siguiente:
   a) *Nombre Común*: Es el nombre de la Autoridad Certificadora (Ejemplo: CERTIFICADORA LCE)
   b) *Unidad Organizacional*: Identifica el área o departamento dentro de la Organización (Ejemplo: Oficina de Certificación)
   c) *Organización*: Identifica a la Organización (Ejemplo: ITESM-CEM)
   d) *País*: Identifica al país (Ejemplo: MX)
   e) *Periodo de Vida*: Se debe especificar el periodo de vida del Certificado de la Autoridad Certificadora.

f) *Número de Serie Inicial*: Se debe indicar el número de serie a partir del cual se comenzarán a expedir los Certificados.

g) *Habilitar Extensiones X.509*: Es muy importante que si se desea una mayor compatibilidad con otros productos y aplicaciones, además si se tiene planeado incluir más políticas o campos a los Certificados, que se seleccione la casilla de Habilitar Extensiones X.509.

h) *Seleccionar el Algoritmo de Firma*: En este apartado se debe elegir el algoritmo que la Autoridad Certificadora utilizará para firmar los Certificados que expida. Se puede elegir entre MD5 con encripción RSA ó SHA-1 con encripción RSA.

5. ***Expedición del Certificado para comunicaciones SSL***: En este apartado se recolecta la información necesaria para expedirle al servidor su Certificado para mantener comunicaciones seguras. La información que se debe proveer para la expedición de dicho certificado es la siguiente:

   a) *Nombre Común*: Es el nombre del Servidor y que será utilizado en el Certificado expedido por esta Autoridad Certificadora para el uso de SSL de este Servidor. (Ejemplo: campus.cem.itesm.mx)

   b) *Unidad Organizacional*: Es el área o departamento dentro de la Organización. (Ejemplo: Oficina de Certificación)

   c) *Organización*: Describe a la Organización (Ejemplo: ITESM-CEM)

   d) *País*: Describe al país (Ejemplo: MX)

   e) *Periodo de Vida*: Es el periodo de vida del Certificado SSL para nuestro Servidor. Este periodo de vida no puede ser mayor al tiempo de vida de la Autoridad Certificadora.

6. ***Creación del Administrador***: En este paso se lleva a cabo la creación del administrador y su Certificado Digital. Éste será quien tenga todos los privilegios sobre la Autoridad Certificadora al presentar su Certificado cuando le sea requerido. La información que se debe proveer es la siguiente:

   a) *Nombre del usuario*: Este es el nombre del Administrador. (Ejemplo: Administrador)

b) *Nombre Común*: Es el nombre del Administrador. (Ejemplo: Administrador)

c) *Unidad Organizacional*: Es el área o departamento dentro de la Organización. (Ejemplo: Oficina de Certificación)

d) *Organización*: Describe a la Organización (Ejemplo: ITESM-CEM)

e) *País*: Describe al país (Ejemplo: MX)

f) *Tamaño de la llave*: Se debe elegir el tamaño de la llave. Por restricciones del Gobierno de los Estados Unidos, respecto a la exportación de criptografía en algunas versiones pudiera estar disponible únicamente el tamaño de 512 bits.

g) *Periodo de Vida*: Es el periodo de vida del Certificado de Administrador. Este periodo de vida no puede ser mayor al tiempo de vida de la Autoridad Certificadora.

Al enviar esta forma se generará una llave privada para el Administrador, es necesario dar una contraseña para proteger a la llave privada.

7. ***Importar el Certificado de Administrador***: Para que un Certificado Digital pueda ser utilizado, éste debe estar instalado en el navegador de Netscape. Es por ello que una vez creado el Administrador y su Certificado Digital, es necesario importar dicho Certificado al navegador, para poder tener acceso privilegiado al Servidor de Certificados.

   Se tiene que escoger la opción de Importar Certificado y el Certificado será automáticamente importado al navegador. Se tiene la opción de cambiarle el nombre y de poder ver el Certificado Digital. Una vez instalado el Certificado del Administrador la instalación y configuración del Servidor de Certificados ha concluido y está listo para poder ser utilizado.

6. Acceso al Servidor de Certificados

Al instalar el Servidor de Certificados, se instala un servidor web. El acceso al Servidor de Certificados se lleva a cabo vía web bajo el protocolo de comunicaciones seguras SSL y HTTP, es decir HTTPS. Para accesar al Servidor de Certificados se debe acceder al URL https://servidor.dominio desde cualquier

navegador (Ejemplo: https://nikita.cem.itesm.mx). Si se desea tener accceso al Servidor de Certificados como Administrador, se tendrá que acceder a éste desde el navegador, y en consecuencia desde la máquina donde se encuentra instalado el Certificado de Administrador.

7. Descripción del Servidor de Certificados Netscape

El Servidor de Certificados de Netscape, permite crear, firmar, y manejar Certificados Digitales. Los Certificados expedidos por el Servidor de Certificados de Netscape son del tipo X.509. Se puede usar el Servidor de Certificados como la base de software para la implantación de una Autoridad Certificadora. Algunas de las tareas más importantes que se pueden realzar con ayuda del Servidor de Certificados de Netscape son:

- Procesar Solicitudes de Certificados Digitales
- Expedir Certificados Digitaeles
- Establecer políticas de restricciones sobre los Certificados expedidos
- Revocar Certificados
- Mantener y publicar una lista de Certificados Revocados
- Buscar Certificados expedidos por este Servidor de Certificados
- Establecer Jerarquías de Autoridades Certificadoras
- Adecuar el Servidor de Certificados a los Procesos de Certificación de nuestra Autoridad Certificadora

El Servidor de Certificados de Netscape posee un mayor número de operaciones a las presentadas en esta sección. Presentaremos únicamente las funciones que por su naturaleza, resultan ser las más importantes. Una vez dominadas las funciones importantes, el ahondar en el resto de las funciones resultará más fácil.

7.1 Componentes del Servidor de Certificados Netscape

El Servidor de Certificados de Netscape, provee formas como interfaces para la realización de sus operaciones. Ya que estas operaciones son llevadas a cabo por

diferentes personas (Administrador, Operadores o Usuarios), el Servidor provee dos conjuntos de formas:

Operaciones públicas: Estas formas están diseñadas para uso público. Se pueden utilizar estas formas para solicitar Certificados, buscar Certificados Expedidos por esta Autoridad Certificadora y consultar la lista de Certificados revocados, entre otras.

Operaciones Privilegiadas: Estas formas están diseñadas para uso administrativo. Estas formas son usadas por el equipo de trabajo de la Oficina de Certificación para realizar tareas como procesar solicitudes de Certificados, revocar Certificados, etc.

Además se cuenta con el Administrador de Servidores de manera separada, para labores administrativas y manejo del Servidor.

8. Operación del Servidor de Certificados Netscape

El operar una infraestructura de Certificados Digitales, es una labor tradicionalmente difícil. Esto se debe básicamente a que la mayoría de los usuarios no tienen formación informática, y ésta es una cuestión que requiere de conocimientos informáticos profundos (criptografía, tecnologías de llave pública, seguridad computacional, etc.).

Es por ello que en esta sección trataremos el tema de, cómo operar el Servidor de Certificados de Netscape, de tal manera que quede al alcance de la comprensión de la mayoría de los usuarios. Esto no quiere decir que los conceptos presentados aquí sean sencillos, por lo que es necesario dominar los conceptos presentados en todos los capítulos anteriores.

El operar con el Servidor de Certificados, es labor de los usuarios, ya que incorporan los Certificados Digitales a su operación diaria. Por su parte, un Operador de la Autoridad Certificadora, lleva a cabo labores Administrativas sobre el Servidor de Certificados. Para tener acceso a las tareas de Operación, se deben seleccionar las

Opciones públicas después de hacer contacto con el Servidor de Certificados.

8.1 Solicitud de un Certificado Digital

Para solicitar un certificado personal se deben seguir los siguientes pasos:

1. Verificación de las condiciones previas a la solicitud de un certificado.

2. Enviar una solicitud de certificado a la Autoridad Certificadora.

8.1.1 Verificación de las condiciones previas a la solicitud de un certificado.

El Certificado se instalará en el Navegador desde el cual se solicitó el Certificado Digital y por consiguiente quedará instalado en la máquina desde la cual se llevo a cabo el proceso de solicitud.

Es por ello que el usuario debe asegurarse de que se encuentra corriendo su navegador Netscape en la máquina en la que quiere que el certificado sea instalado. Esto es debido a que durante el proceso de solicitud del certificado, la llave privada del usuario es generada y ésta permanece en la máquina desde la cual se envió la solicitud. Una vez recibido el certificado, éste se puede exportar e importar a otras computadoras.

8.1.2 Enviar una Solicitud de Certificado Digital

Para poder enviar una solicitud de Certificado Digital, es necesario llevar a cabo los siguientes pasos:

- Establecer una comunicación segura entre la Autoridad Certificadora y la máquina del usuario. Esto se logra mediante el uso del protocolo seguro https. Por ejemplo, "https: //nikita.cem.itesm.mx". Esta dirección nos llevará a la página principal de la Autoridad Certificadora.

- Al hacer contacto con la Autoridad Certificadora, ésta presentara su certificado digital que le acredita como tal ante su navegador. Este certificado no es válido, debido a que esta Autoridad aún no es reconocida por su navegador.

- Se deben leer cuidadosamente los cuadros de diálogo, éstos contienen información importante en materia de seguridad. Se deben seguir las instrucciones y elegir la opción "Aceptar el certificado por esta sesión" cuando le sea requerido.

- Después de aceptar el certificado, se ha establecido una comunicación segura entre la Autoridad Certificadora y la máquina del usuario (Se puede observar, como se ha cerrado el candado de la parte inferior izquierda del navegador).

- Se debe seleccionar la opción "Solicitar un Certificado Personal" del menú público, para desplegar la forma de solicitud de certificados.

- Llenar la forma de solicitud de Certificado con la información requerida y enviarla.

- Después de enviar la solicitud de Certificado, se genera un par de llaves. La parte privada permanece en el navegador y la parte publica se envía a la Autoridad Certificadora. Es muy importante proteger la llave privada con una contraseña.

- Si la solicitud fue llenada correctamente, el servidor de certificados de la Autoridad Certificadora desplegará una página confirmando que la petición ha sido recibida y se le ha asignado un número de referencia.

- Posteriormente la Autoridad Certificadora, acorde a sus Procesos de Certificación dará trámite a la solicitud.

Las llaves del usuario son generadas a la hora de solicitar un Certificado, sin importar si la solicitud será aceptada o no. La llave privada es guardada en la

máquina local del usuario y se almacena encriptada bajo una contraseña que el mismo usuario ingresa. Es de suma importancia cuidar esta llave con una contraseña, por lo que no hay que olvidar asignarle una.

8.2 Instalación de un Certificado Digital

En caso de que la Autoridad Certificadora haya comprobado la identidad del usuario y haya resuelto aprobar su solicitud de certificado, el usuario recibirá su certificado por correo electrónico, este mensaje también contiene las instrucciones de cómo importar el certificado a su navegador.

Para importar el certificado al navegador, sólo hace falta leer la sección "Importar este Certificado a su Navegador" del mensaje que se acaba de recibir, y seguir las instrucciones.

Se debe dar click en la dirección de web que ahí aparece bajo la leyenda "Usted puede recoger su Certificado en". Posteriormente, se debe seleccionar la opción "Importar este Certificado al Navegador".

Ya que la llave privada se generó desde el momento de la solicitud y ésta quedó en el navegador desde el cual se realizó la solicitud del Certificado, éste sólo podrá ser instalado en ese navegador. Si se trata de instalar el Certificado en una máquina diferente a la que se utilizó para solicitar el Certificado Digital, éste no podrá ser instalado, ya que al momento de su instalación, el programa busca la llave privada que hace juego con la llave pública que porta el Certificado.

Si se encuentra la llave privada para ese Certificado, el navegador confirmará su existencia, y la contraseña que protege a la llave privada será requerida. Se deben seguir cuidadosamente las instrucciones de los cuadros de dialogo para completar el proceso de instalación del certificado.

Por último, será recomendado que se salve el certificado, este paso puede ser saltado o si se desea se puede hacer un respaldo del Certificado Digital. Hay que tomar en

consideración que el poseer una copia del Certificado Digital pude servirnos en caso de pérdida del original, pero también puede resultar un peligro, ya que se puede extraviar.

Si se recibe el mensaje de que el certificado ha sido importado exitosamente, entonces el proceso concluyó satisfactoriamente.

Otra opción es buscar el Certificado en la pagina de la autoridad certificadora. Se debe escoger "Buscar Certificado" o "Listar Certificados" en la parte pública del Servidor de Certificados. Para encontrar el certificado, uno se puede ayudar de las formas que ahí se presentan. Una vez hallado el Certificado, se debe presionar "Detalles", para por último importar el certificado con la opción "Importar este Certificado al Navegador".

8.3 Aceptar la Autoridad Certificadora en el Navegador

El Aceptar a una Autoridad Certificadora, quiere decir que la estamos adoptando como nuestra Autoridad Certificadora. Para poder adoptar oficialmente y técnicamente a una Autoridad Certificadora la debemos aceptar como tal de la manera que se describe a continuación.

Se debe contactar a la Autoridad Certificadora de la manera habitual (Ejemplo: "https://nikita.cem.itesm.mx"). Dentro del apartado público hay que seleccionar "Aceptar Autoridad Certificadora".

Se tiene la opción de confiar únicamente en esta Autoridad Certificadora o confiar en todas las Autoridades que compartan la misma Autoridad Certificadora raíz. Se debe consultar al Administrador de la Autoridad Certificadora para saber que opción elegir. Una vez hecha la selección, se debe dar click en "Importar cadena de Certificación".

Se deben leer cuidadosamente los cuadros de diálogo, estos contienen información importante en materia de seguridad y seguir las instrucciones en pantalla. En este

punto el usuario está listo para utilizar su certificado.

8.4 Ver, Verificar, Borrar y Buscar un Certificado

Para poder ver un Certificado Digital, se debe acceder a la sección de seguridad del navegador, bajo el rubro de Certificados. Se puede tener acceso a los Certificados propios, a los de las personas, de los sitios web y de las Autoridades Certificadoras. Para poder verlo sólo basta oprimir la opción de ver y el Certificado será presentado.

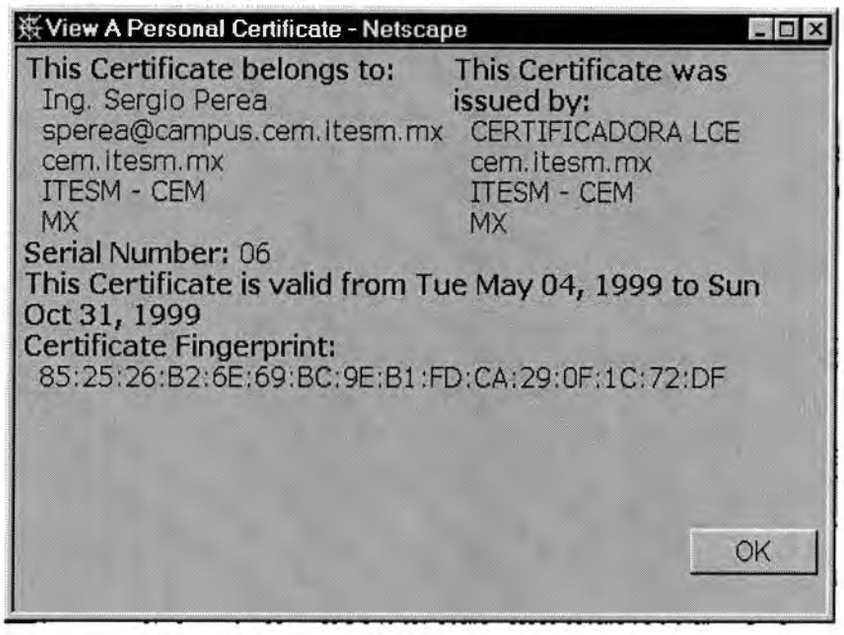

Figura 11: Ejemplo de un Certificado Digital de Netscape

El verificar un Certificado Digital consiste en ver si el Certificado Digital es válido para nuestro sistema en particular. Básicamente de lo que se trata es de ver si la Autoridad Certificadora que expidió dicho Certificado es reconocida por nuestro navegador. Para verificar un Certificado Digital sólo basta con oprimir la opción de verificar.

Si se desea borrar un Certificado Digital, lo único que se tiene que hacer es seleccionarlo y oprimir el botón de borrar.

Es muy probable que se llegue a tener duda de la procedencia de un Certificado o de la valides del mismo. Para este tipo de situaciones, el Servidor de Certificados de Netscape provee la publicación de la lista de Certificados Expedidos y Revocados.

Estas listas son de libre acceso a todos los usuarios. Para acceder a ellas se debe hacer contacto con la Autoridad Certificadora y dentro del menú de acciones públicas se puede escoger entre listar Certificados, Buscar Certificados o revisar la lista de Certificados Revocados. Las formas para buscar Certificados se explican por si mismas y son muy fáciles de llenar para poder acotar la búsqueda.

8.5 Cómo firmar Digitalmente un Mensaje

En la forma de edición de un nuevo mensaje en Netscape aparecen tres pestañas: la primera es la lista de receptores del mensaje; la segunda es un clip, que sirve para incluir archivos en anexo al mensaje, y la última nos presenta una serie de opciones, seleccionar "firmado".

El destinatario del correo recibirá en la esquina superior derecha del mensaje una firma digital, que es el Certificado del remitente del mensaje. El recipiente debe analizar la firma digital que le llegó adjunta al mensaje. De ésta manera si la firma es válida, quiere decir que el remitente del mensaje es en realidad quien dice ser.

También se puede configurar el Navegador para que firme de manera automática los mensajes antes de enviarlos.

Hay que tomar en cuenta que si el receptor no reconoce a la misma Autoridad Certificadora que el emisor, aparecerá una firma inválida. Aún así es posible ver el certificado y comprobar la procedencia de éste.

8.6 Cómo encriptar un Mensaje

En la forma de edición de un nuevo mensaje en Netscape aparecen tres pestañas: la primera es la lista de receptores del mensaje; la segunda es un clip, que sirve para incluir archivos en anexo al mensaje, y la última nos presenta una serie de opciones, seleccionar "encriptado".

Para poder enviar un mensaje encriptado, el emisor debe poseer la llave pública del receptor del mensaje, ya que al encriptar el mensaje con esa llave, el destinatario del

mensaje será el único que podrá leerlo, ya que él es el único que posee la otra llave que hace juego con la llave que encriptó el mensaje, es decir su llave privada. La llave pública se encuentra en el certificado del receptor. Si no se posee el certificado del receptor, el mensaje no podrá ser encriptado; sin embargo si podrá ser enviado.

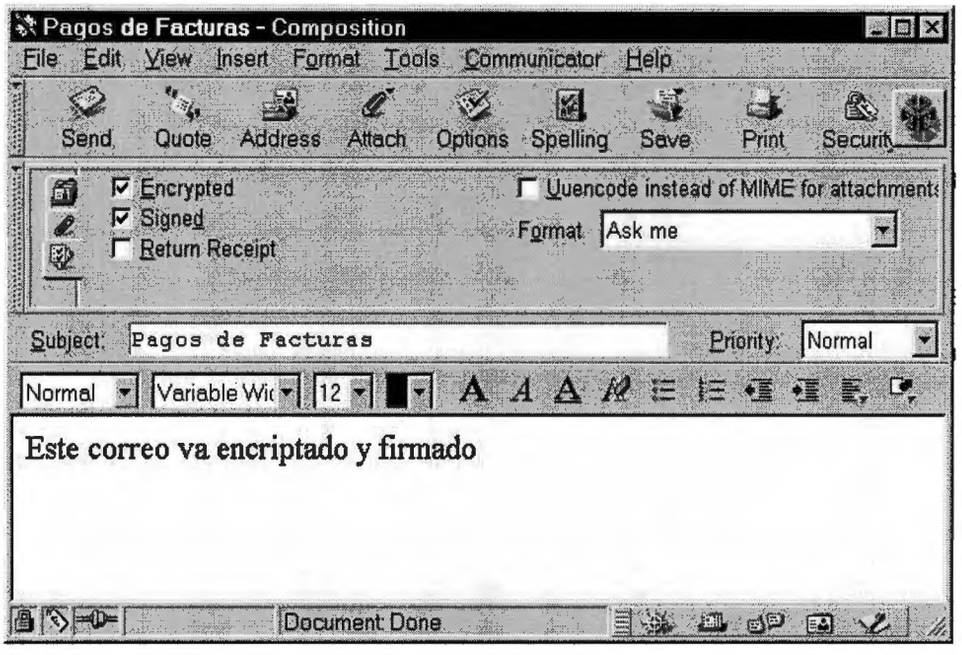

Figura 12: Ejemplo de cómo firmar y encriptar un mensaje.

8.7 ¿Cómo leer un Mensaje encriptado?

Para poder leer un correo encriptado, es necesario que se ingrese la contraseña que protege a la llave privada y entonces el mensaje podrá ser leído, de otra manera aparecerá un mensaje totalmente en blanco.

Es posible que la configuración del sistema de contraseñas de su Netscape le permita ver el mensaje encriptado directamente (ver configurar sistema de contraseñas).

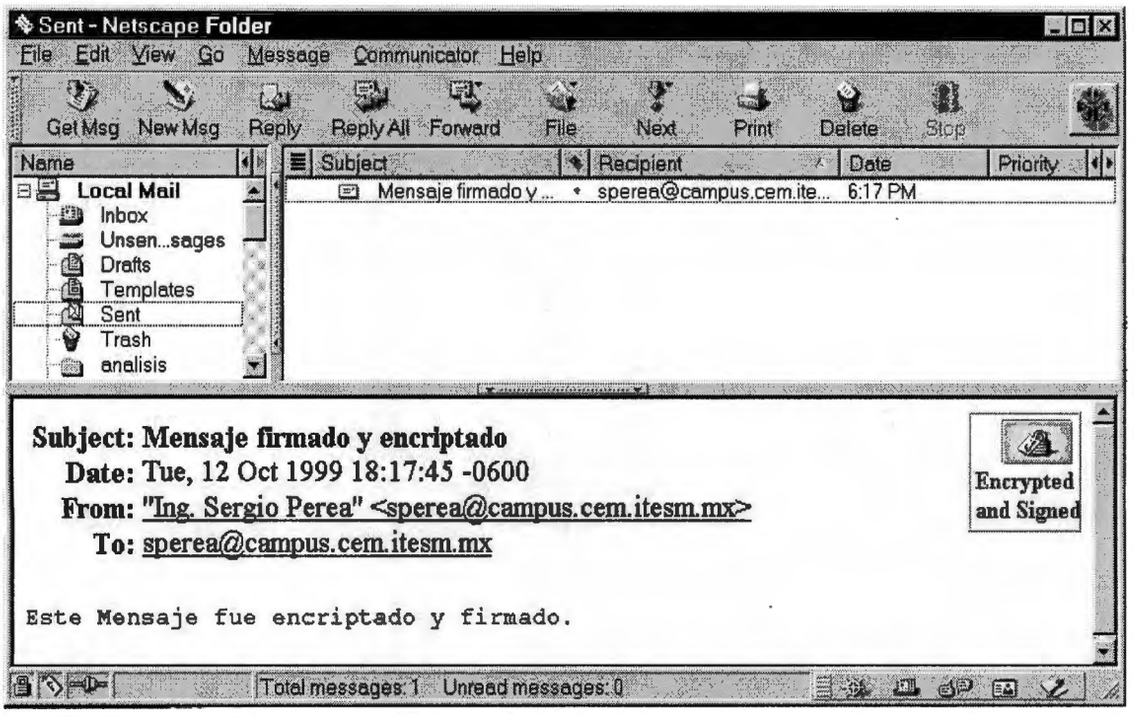

Figura 13: Mensaje firmado y encriptado

8.8 Intercambio de llaves

Para hacer posible el intercambio de mensajes encriptados, es necesario poseer los certificados de los receptores. Cuando usted recibe un mensaje firmado, el certificado incluido se instala automáticamente en el navegador. Desde ese momento usted puede comenzar a intercambiar mensajes encriptados con esa persona.

Una buena práctica dentro de la organización sería intercambiar mensajes firmados para que los certificados de los demás se instalen en nuestro navegador y así tener la posibilidad de intercambiar mensajes encriptados con todos.

8.9 Protección del Certificado Digital

8.9.1 Porqué se debe Proteger el Certificado Digital

El Certificado Digital hace las veces de nuestra firma manuscrita. Esto quiere decir que debemos responder por cualquier instancia firmada digitalmente con nuestro Certificado, de la misma manera que se debe responder ante un Documento firmado a mano por nosotros.

Es por ello que debemos proteger nuestro Certificado Digital para que éste no caiga en manos de terceros que hagan mal uso de él. Además debemos proteger su llave privada con una contraseña dentro de nuestro propio sistema.

El Certificado Digital queda instalado en el Navegador y su llave privada se guarda encriptada bajo una llave que ingresamos como contraseña.

8.10 Configuración del Sistema de Contraseñas

Cada vez que se utiliza el Certificado, la contraseña que lo protege es requerida. Esta configuración se puede cambiar en el apartado de seguridad de su navegador. En la sección de contraseñas (passwords). Se puede elegir entre ingresar la contraseña la primera vez que el certificado sea requerido, ingresarla cada vez que se requiera el Certificado o después de cierto tiempo de inactividad. El tiempo de inactividad puede ser establecido por el usuario y está dado en minutos.

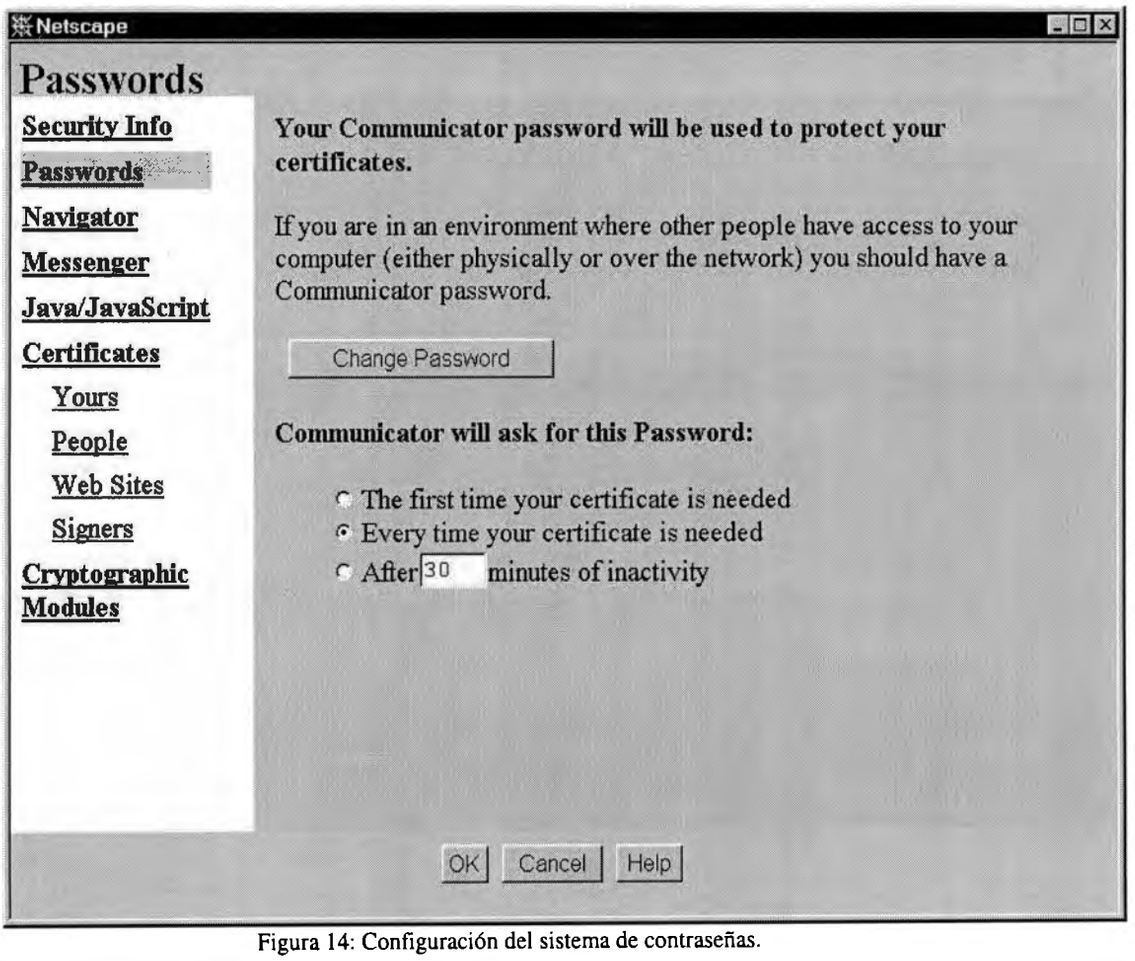

Figura 14: Configuración del sistema de contraseñas.

Se debe elegir el esquema de manejo de contraseñas que mejor ajuste a las necesidades del usuario. Hay que recordar que se puede cambiar este esquema y además se tiene la posibilidad de cambiar la contraseña cada vez que se desee.

8.10.1 Desventajas de la Configuración Automática del Sistema de Contraseñas

El programar de manera automática el requerimiento de la contraseña que protege a la llave privada del Certificado Digital, nos puede aliviar de ingresarla cada vez que el Certificado se utilice, pero es una arma de dos filos, ya que puede resultar muy peligroso.

Si se deja configurado el sistema de contraseñas para que ésta se requiera solamente la primera vez que se utilice el Certificado, y el equipo es de acceso a varios usuarios o se ha dejado abierto el navegador por accidente, una tercera persona con malas intenciones puede enviar un mensaje a nuestro nombre, y debido a la configuración del sistema, el mensaje saldrá firmado, lo que significa que tendremos que responder por dicho mensaje.

Lo mismo puede ocurrir si se programa para que se pida la contraseña después de cierto tiempo de inactividad. Lo mejor es dar la contraseña cada vez que el Certificado es usado, de esta manera uno no se expone.

8.11 Configuración del Sistema de Encripción y Firma de un Mensaje

En primera instancia cuando se desea firmar o encriptar un mensaje, uno puede elegir esas opciones directamente sobre el mensaje que se está editando. Estas opciones pueden configurarse de manera automática para que un mensaje salga firmado o encriptado sin que el usuario deba especificarlo en cada mensaje.

En el apartado de seguridad del navegador de Netscape, bajo el rubro de mensajero (messenger) se puede elegir el encriptar un mensaje, firmar un mensaje o firmar un mensaje de noticias de manera automática. Posteriormente se puede elegir de entre la lista de Certificados instalados en nuestro navegador (en caso de tener más de

uno) el Certificado predeterminado con el cuál serán firmados y/o encriptados los mensajes. Además se puede enviar el Certificado a un Directorio o cambiar las configuraciones del protocolo S/MIME.

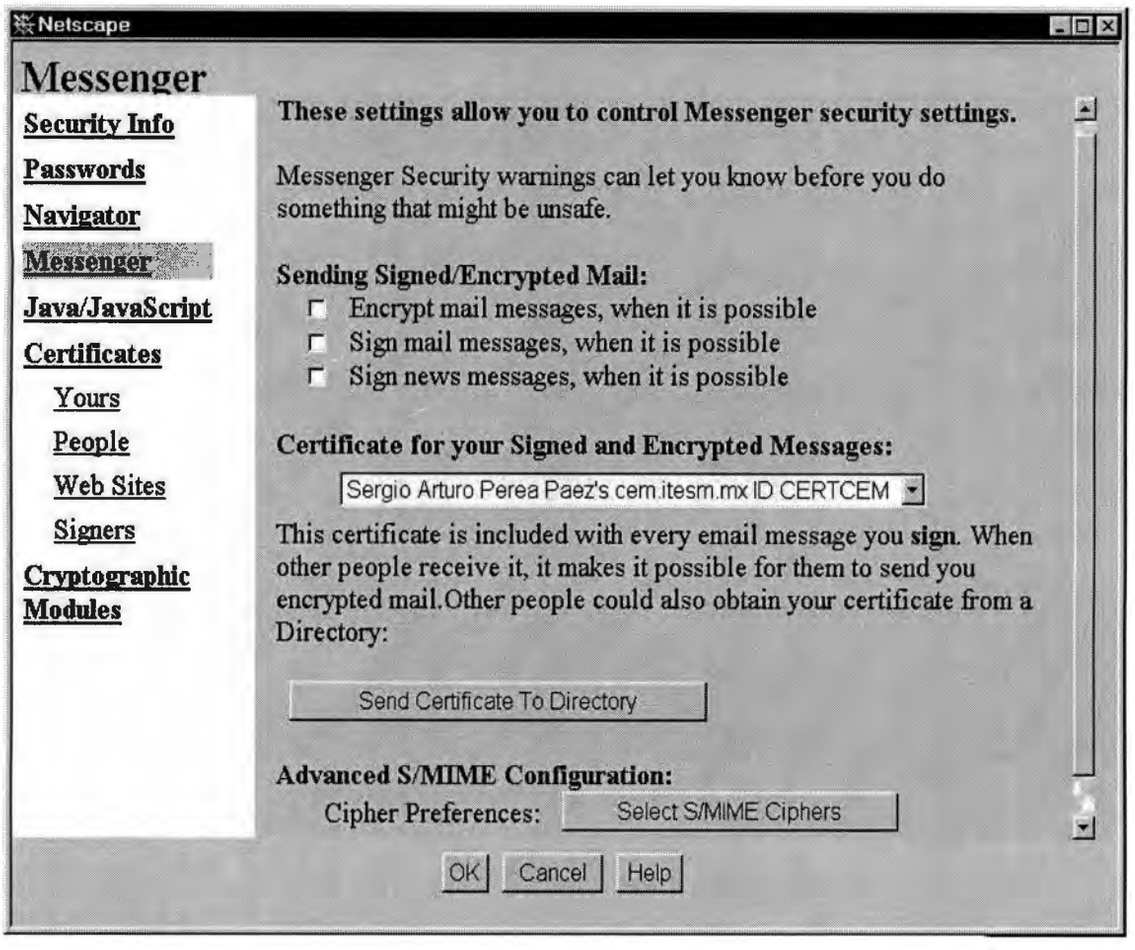

Figura 15: Configuración del sistema de encripción y firma de un mensaje.

8.11.1 Desventajas de la Automatización del Proceso de Firma y Encripción de un Mensaje.

La gran desventaja de este proceso, es que si alguien más tiene acceso a nuestro equipo, o por accidente se deja abierto el navegador, cualquier persona con malas intenciones puede enviar un mensaje a nuestro nombre aprovechando las circunstancias. Y ya que el mensaje salió firmado, éste puede ser tomado como oficial y poner en serias dificultades al dueño de la cuenta, ya que es él quien tendrá que responder por el mensaje enviado.

8.12 Comunicación Segura entre dos Entidades

Cuando dos entidades por la red se comunican de manera segura utilizando su Certificado Digital, ya sea mediante el protocolo SSL o encriptando mensajes entre ellas, la Autoridad Certificadora es una tercera parte que ya no forma parte del proceso, es decir, una vez que la Autoridad Certificadora ha expedido los Certificados, ésta permanece independiente de cualquier comunicación y uso que se les de a los mismos.

Ni siquiera la misma Autoridad Certificadora se puede enterar de las comunicaciones privadas de sus usuarios. Es más, la Autoridad Certificadora no triangula comunicación alguna entre dos puntos en la red.

8.13 Importar / Exportar un Certificado Digital

El Certificado Digital permanece instalado en el navegador, pero es posible que éste se pueda instalar en otro navegador. Para llevar un Certificado a una localidad diferente éste necesita ser exportado para posteriormente ser importado en su destino.

Para exportar un Certificado, se debe acceder al apartado de Seguridad del navegador, bajo el rubro de Certificados propios. A un costado de la lista de Certificados, aparecen las opciones de verlo, verificarlo, borrarlo y exportarlo. Se debe escoger exportarlo.

Después de haber elegido exportar el Certificado, la contraseña que lo protege será requerida. Posteriormente será requerida una nueva contraseña, y su confirmación, que será la llave bajo la cual se almacenará encriptado. Por último se elige la locación donde será exportado, ésta puede ser un directorio dentro del disco duro, un disco flexible, etc.

Para importar un Certificado, básicamente el proceso es el mismo, únicamente se debe elegir Importar Certificado en el apartado debajo de la lista de Certificados.

Posteriormente se debe ingresar la localidad donde se haya exportado el Certificado y se debe proporcionar la contraseña que lo protege, que es con la que fue exportado (si la contraseña es olvidada no habrá forma de importar el Certificado). Además se debe ingresar una nueva contraseña, y su confirmación, ya que ésta será la llave bajo la cual se almacenará encriptado.

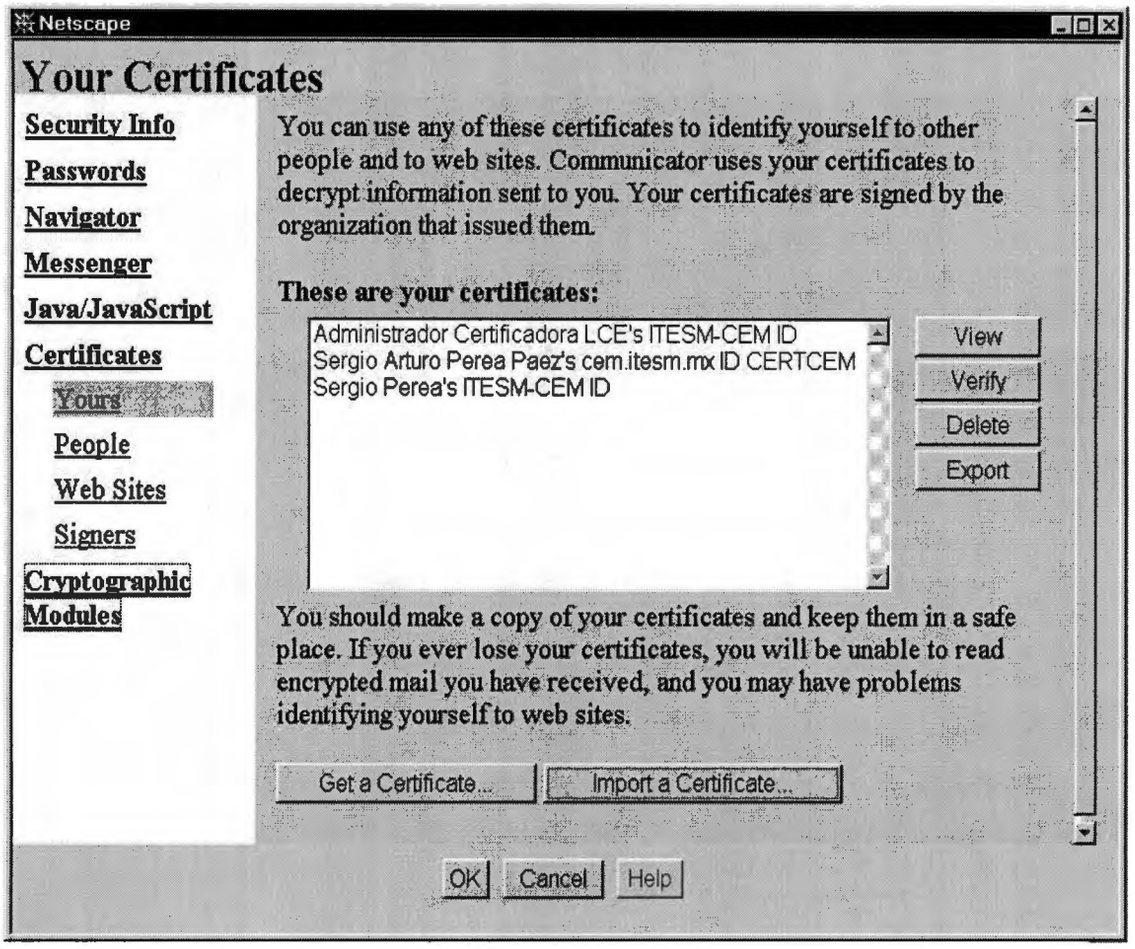

Figura 16: Importar un Certificado Digital. También se presentan las funciones para ver, verificar, borrar y exportar un Certificado.

9. La Confianza para Netscape

La parte de la validez de un Certificado Digital se la da que esté firmado por una Autoridad Certificadora confiable. En Netscape, tanto los usuarios como los administradores de los Servidores pueden decidir en qué Autoridades confiar y en cuáles no.

Si un navegador o Servidor de Netscape recibe un Certificado expedido por una

Autoridad Certificadora no confiable, el Certificado puede ser rechazado. Por otro lado, los Certificados expedidos por Autoridades Certificadoras confiables pueden ser automáticamente aceptados por el navegador o Servidor.

El aspecto de la confianza resulta ser de suma importancia, ya que existe el software para que cualquier persona con las habilidades técnicas necesarias levante su propia Autoridad Certificadora, pero eso no significa que sea una Autoridad Confiable.

La confianza en los sistemas Netscape funcionan de la siguiente manera. Cuándo un navegador establece una conexión SSL con un servidor seguro (como el Servidor de Certificados), el servidor envía su Certificado de Servidor al cliente. El navegador determina qué Autoridad Certificadora expidió el Certificado y busca en la base de datos el Certificado de Autoridad Certificadora de esta Autoridad.

Si el Certificado de Autoridad Certificadora se encuentra en la base de datos local y éste corresponde a una Autoridad Certificadora confiable, el navegador completa la conexión SSL. Si el Certificado de la Autoridad Certificadora no está en la base de datos, se busca una Autoridad Certificadora confiable en la cadena de certificación. Recordemos que las Autoridades Certificadoras se pueden Certificar entre sí, entonces lo que se busca es que dentro de toda esa cadena haya una Autoridad Certificadora Confiable (las cadenas de certificación son tratadas más adelante en este capítulo).

Si ninguna de las anteriores condiciones de confianza ocurrieron, el navegador presenta una serie de advertencias que ayudan al usuario a decidir si aceptar el Certificado o no y bajo qué terminos.

Se debe tener especial cuidado con el aspecto de la confianza, lo único que el usuario debe hacer para confiar en una Autoridad Certificadora, es Aceptar la Autoridad Certificadora, para lo cual importa su cadena de certificación. El importar la cadena de Certificación de una Autoridad Certificadora implica aceptarla a ella y a todas las Autoridades Certificadoras en las que ella confía, lo que nos impide decidir realmente en cual confiar o no.

10. Verificación de la firma Digital

Para indicar que un mensaje ha sido firmado digitalmente o encriptado, Netscape marca al mensaje con un recuadro en la esquina superior derecha indicando que el mensaje fue firmado o encriptado.

Si la Autoridad Certificadora que firma el Certificado presentado es una Autoridad Certificadora confiable (ver sección anterior) para Netscape, entonces la firma aparece como válida, de lo contrario aparecerá como firma inválida, en cualquiera de los casos el mensaje puede ser leído por el usuario.

El que la firma sea inválida puede indicar que la Autoridad Certificadora que firma el Certificado no es confiable o que el mensaje sufrió alguna alteración por su camino por la red o que fue falsificado. En este caso el mensaje debe ser desechado. Se debe contactar a la persona que aparece como remitente del mensaje para comprobar que haya sido ella quien envió ese mensaje y pedirle su re envío.

Es una buena costumbre verificar el Certificado que se nos presenta cuando nos llega un mensaje con firma. Una buena practica es darle doble click y analizar el Certificado para verificarlo.

11. Administración del Servidor de Certificados Netscape

Tradicionalmente, la implantación y el manejo de una infraestructura de Certificados Digitales, ha sido una tarea muy complicada. Así mismo resulta ser la tarea de administrar el Servidor de Certificados de Netscape. Para poder administrar esta herramienta, que es la base de software de nuestra Autoridad Certificadora, se deben dominar a la perfección todos los conceptos expresados en este trabajo.

La labor principal de Administración la lleva a cabo el Administrador de la Autoridad Certificadora, aunque éste puede apoyarse de su grupo de operadores para la realización de las labores administrativas.

Es necesario que las personas que llevarán a cabo las labores administrativas de la Autoridad Certificadora, estén lo suficientemente capacitadas técnicamente para poder manejar el Servidor de Certificados de Netscape. El Servidor de Certificados de Netscape cuenta con infinidad de funciones para un Administrador. En esta sección se presentarán únicamente aquellas que sean las más importantes, después de dominar estas funciones, el grupo administrativo será capaz de explorar y explotar las demás funciones.

En esta sección exploraremos la Administración del Servidor de Certificados de Netscape desde el punto de vista de la Administración de una Autoridad Certificadora y no desde el punto de vista de la administración de un paquete de software, ya que el Servidor de Certificados provee sus propias formas asignadas a funciones específicas y muchas de ellas se explican por sí solas. Es por ello que muchas de las tareas de administración únicamente serán descritas brevemente.

A continuación presentaremos las tareas que debe llevar a cabo la Administración de la Autoridad Certificadora, basándose en el uso del Servidor de Certificados de Netscape.

11.1 Funciones Administrativas

Algunas de las funciones Administrativas son:

- Configuración y manejo del Servidor
- Manejo del Servicio de Certificados
- Configuración de los parámetros del Servidor
- Establecimiento de las preferencias de seguridad
- Monitoreo del Servidor

Como ya lo mencionamos, estas no son todas las funciones administrativas, pero si son las más relevantes para poder funcionar con la Infraestructura de Certificación. A pesar de que estas son las funciones más relevantes, no todas serán explicadas, ya que el Servidor presenta formas asignadas a estas tareas, las cuales son muy fáciles de utilizar, y se explican por sí solas. En esta sección únicamente trataremos las

funciones más importantes.

Las funciones administrativas se pueden acceder, ya sea desde el Administrador de Servidores, o algunas desde el menú de funciones privilegiadas de la página principal de la Autoridad Certificadora. El grupo de funciones administrativas que se acceden a partir del menú privilegiado de la página principal de la Autoridad Certificadora son:

- Manejo de las Solicitudes de Certificado
- Revocación de Certificados
- Solicitud de un Certificado de Autoridad Certificadora

Para poder tener acceso a estas funciones, un Certificado de administración será requerido y éste debe estar instalado en el navegador desde el cual se desean acceder a las funciones privilegiadas.

11.1.1 Configuración y Manejo del Servidor de Certificados

Para llevar a cabo las tareas de manejo y configuración del Servidor de Certificados, se hace uso del Administrador de Servidores. También se hace uso del Servidor de Certificados para instalar otros Servidores de Certificados, para des instalar un Servidor de Certificados y para Prender y apagar el Servidor de Certificados. Una de las tareas más importantes es la de levantar o dar de baja el Servidor de Certificados (Prender y Apagar el Servidor).

11.1.1.1 Prendido y Apagado del Servidor de Certificados

Una de las tareas más transparentes de la administración, es la de levantar y apagar el Servidor. El Servidor se puede prender o apagar desde el Administrador de Servidores de Netscape y a esta tarea sólo puede tener acceso el Administrador o algún miembro del grupo administrativo autorizado por él. El Servidor de Certificados podrá funcionar únicamente si éste está prendido, al igual que el Servidor de la Base de Datos.

Para poder levantar el Servidor de la Base de Datos, es necesario hacerlo desde el "Command Center", del grupo de programas Informix y elegir la opción de dejarlo "en línea y disponible". Después se debe ejecutar el Administrador de Servidores de Netscape del grupo de programas Netscape y elegir el Servidor de Certificados. Aparecerá un interruptor, éste se debe mover de apagado a encendido.

Para apagar el servidor (shut down), se llevan a cabo los mismos pasos descritos anteriormente, sólo que el interruptor se debe pasar de prendido a apagado.

11.1.2 Manejo del Servicio de Certificados

Como Administrador del Servidor de Certificados, se pueden establecer ciertas configuraciones en el servicio de expedición. Por Ejemplo, se puede restringir el expedir ciertos Certificados, basándose en nombre del usuario o en su llave pública, se puede limitar el periodo de validez de los Certificados expedidos, se puede especificar el algoritmo usado para firmar los Certificados, además se puede controlar el acceso a las tareas administrativas y monitorear las acciones del cuerpo administrativo.

11.1.3 Configuración de los Parámetros del Servidor

A través del Administrador de Servidores, se pueden ver y ajustar los parámetros de configuración del Servidor de Certificados. Se puede observar el rendimiento del Servidor, cambiar las configuraciones de red, también se pueden recuperar configuraciones previas, de los archivos de respaldo de configuraciones. Para todas estas funciones se proveen formas para su uso y se encuentran perfectamente explicadas.

11.1.4 Establecimiento de los parámetros de Seguridad

Cuando el Servidor de Certificados es instalado, éste es configurado para trabajar usando el protocolo de comunicaciones seguras SSL. Mediante estas funciones se

pueden ajustar los parámetros de configuración de SSL. Por Ejemplo, se puede cambiar la locación de los archivos que contienen la llave privada, se puede cambiar la locación de los archivos que contienen el certificado, entre otras.

11.1.5 Monitoreo del Servidor

Usando el Administrador de Servidores, se puede tener acceso a los archivos de registro de actividades (logs). Estos archivos proveen información acerca del estado del Servidor y de posibles errores que pueden ocurrir.

11.2 Manejo de las Solicitudes de Certificados

Debemos recordar que detrás del procesamiento de una solicitud de Certificado Digital, se deben cumplir con los Procesos de Certificación establecidos en el capítulo "Autoridad Certificadora", para que éstos avalen al Certificado mismo.

El siguiente es el típico procedimiento para manejar las solicitudes de Certificados:

- Revisar la lista de solicitudes.
- Seleccionar una solicitud de la lista, y asignársela a sí mismo.
- Procesar la solicitud. Al procesarla se pueden llevar a cabo varias acciones
  - Probar la solicitud para asegurarse de que el Servidor de Certificados la considera una solicitud válida.
  - Expedir el Certificado.
  - Cancelar la solicitud (en caso de que el solicitante haya cometido un error al enviar la solicitud).
  - Rechazar la solicitud (Si la solicitud no es compatible con las políticas y Procesos de Certificación de la Autoridad Certificadora).
  - Regresar la solicitud a la lista de espera.

11.2.1 Listar las solicitudes de Certificado

Cuándo un usuario envía su solicitud de Certificado, ésta es formada en una cola. La

cola guarda si una solicitud se encuentra en los estados de: esperando, cancelada o rechazada. Un miembro del equipo de administración se asigna la solicitud a sí mismo para poder procesarla.

- Hacer contacto con la página principal de la Autoridad Certificadora (o con la página que contenga las formas adecuadas) y dirigirse al menú de funciones privilegiadas.
- Elegir "Listar solicitudes de Certificados", para tener acceso a la cola de solicitudes de Certificados y poder procesarlas.
- Elegir cuáles solicitudes se desean ver
  - Mostrar solicitudes en espera: Estas son solicitudes que no han sido procesadas aún.
  - Mostrar solicitudes canceladas: Estas con las solicitudes que han sido canceladas.
  - Mostrar solicitudes rechazadas: Estas son las solicitudes que no son compatibles con las políticas o los Procesos de Certificación de la Autoridad Certificadora.
  - Mostrar solicitudes completadas: Estas con las solicitudes para las cuales se han expedido sus respectivos Certificados Digitales.
- Escoger "Correr consulta"

11.2.2 Selección y Asignación de una solicitud

Para seleccionar una solicitud de la cola, se debe seleccionar el número de referencia de la solicitud. Este número se encuentra en la primera columna de la cola. Una vez seleccionada, la información detallada de la solicitud aparecerá.

Si se desea procesar la solicitud se debe seleccionar la liga "Asignármela a Mi" y cuando la forma vuelva a cargar, la solicitud quedará asignada. Si se cambia de opinión y se desea des asignar la solicitud y regresarla a la cola, hay que dirigirse al final de la página y elegir "Regresar esta solicitud a la cola de espera", de la lista de operaciones. Esta acción se puede llevar a cabo en cualquier estado de la solicitud (asignada, completada, cancelada o rehcazada), el regresarla a la cola nos permite

volver a expedir el Certificado en caso de que se requiera.

11.2.3 Expedición de Certificados

Debemos recordar que se debe expedir un Certificado una vez que se hayan cumplido al pie de la letra los Procesos de Certificación. Por otra parte, nunca se deben expedir Certificados sin que la Autoridad Certificadora se encuentre satisfecha con la identidad del solicitante. Una vez que la Autoridad Certificadora acorde a sus Procesos de Certificación ha decidido expedir el Certificado, se deben llevar a cabo los siguientes pasos:

- Verificar que la solicitud este correctamente asignada a la persona que la atenderá.

- Si se requiere cambiar el nombre del sujeto, se debe hacer en el campo de "Nombre del sujeto". Esta acción se debe hacer para evitar duplicados o corregir errores de escritura.

- Para sobre escribir el requerimiento de llave pública única, se debe marcar dicha opción. El expedir un Certificado Digital con la misma llave pública a dos sujetos diferentes, viola el modelo de autenticación. Normalmente el Servidor de Certificados checa las llaves de tal manera que un Certificado que tenga la misma llave que otro ya existente, pueda ser expedido sólo si pertenece a la misma entidad. Sin embargo, se puede sobrepasar esta protección de manera manual. Esto se debe hacer sólo si los dos nombres de sujetos corresponden a la misma entidad o si el Certificado fue generado con un nombre incorrecto.

- Para especificar el periodo de vida del Certificado se debe seleccionar el periodo del menú.

- Para sobre escribir la restricción de tener periodos de validez que caen exclusivamente en el rango de vida del Certificado de la Autoridad

Certificadora, se debe seleccionar "Sobre escribir restricción de tiempo de vida". De manera predeterminada, el periodo de vida de un Certificado debe caer en el rango de vida del Certificado de Autoridad Certificadora de la nuestra.

- Se puede especificar el tipo de Certificado que se expedirá

- También se puede especificar que el identificador de la llave de la autoridad y el identificador de la llave del sujeto sean incluidos en el Certificado. Estos identificadores pueden ser usados en situaciones donde la Autoridad Certificadora tiene más de una llave pública (Por ejemplo, si la Autoridad Certificadora necesita generar otra llave antes que la actual expire).

- Si se desea utilizar otro algoritmo de firma que no sea el predeterminado, MD5 con encripción RSA, se debe escoger una alternativa del menú que ofrece las siguientes opciones:
    - MD5, el cual genera un message digest de 128 bits
    - SHA-1, el cual genera un message digest de 160 bits

- Para verificar que la solicitud cumple con todos los requerimientos se puede elegir "Validar únicamente" del menú etiquetado como "Seleccione una Operación a Realizar sobre esta solicitud".

- Para expedir el Certificado, se debe escoger "Expedir este Certificado", del menú etiquetado como "Seleccione una Operación a Realizar sobre esta solicitud" y elegir "Llevar a cabo la operación seleccionada".

Si la expedición del Certificado fue exitosa, entonces aparecerá una forma con el Certificado expedido y las instrucciones para entregar éste a su solicitante. Para mandar por correo electrónico el Certificado expedido, sólo basta dirigirse a la liga asignada para ese fin. Otras opciones que se pueden elegir son las de Cancelar la solicitud, Rechazar la solicitud y regresar la solicitud a la cola de espera.

TABLA 2: Tipos de Certificados de Netscape

TIPO	DESCRIPCIÓN
Cliente SSL	Indica que el Certificado personal es utilizado para comunicaciones seguras con servidores mediante el protocolo SSL.
Servidor SSL	Indica que el Certificado de servidor es utilizado para comunicaciones seguras con clientes mediante el protocolo SSL.
Correo electrónico Seguro	Indica que el Certificado es utilizado por una aplicación de correo electrónico para la utilización de correo seguro.
Firma de objetos	Indica que el Certificado es utilizado para firmar objetos, como applets de Java y código de Java Scripts.
Autoridad Certificadora subordinada	Permite a la Autoridad Certificadora el expedir Certificados personales y de Servidores.
Autoridad Certificadora subordinada para firma de objetos ejecutables	Permite a la Autoridad Certificadora firmar y expedir Certificados de Objetos firmados. (Certificados para applets de Java y código de Java Scripts).

11.3 Revocación de Certificados

Es necesario revocar un Certificado Digital cuando:

- El dueño del Certificado ha cambiado de estatus y no tiene el derecho a usar más el Certificado.
- La llave privada del Certificado se ha comprometido.

Al revocar un Certificado, se debe notificar a los demás usuarios que un Certificado ya no es válido, con la finalidad de que éstos ya no lo acepten. Esta notificación se hace a través de una lista de Certificados Revocados, en la cual se inscriben todos los Certificados que han sido revocados y es de acceso libre a todos los usuarios. De hecho, es obligación del usuario el consultar dicha lista.

Para revocar un Certificado se deben seguir los siguientes pasos:

- Dirigirse a la página principal de la Autoridad Certificadora y acceder al menú de operaciones privilegiadas.
- Escoger "Revocar Certificados", para desplegar las formas para seleccionar los Certificados a revocar. En la forma de revocación de Certificados, se puede generar una lista con los Certificados que se desean revocar, mediante una búsqueda en base a varios criterios, como lo pueden ser: Revocar Certificados por nombre del usuario, revocar en base al número de serie, revocar de acuerdo al periodo de expedición o expiración (certificados que fueron expedidos o expiran en determinado periodo de tiempo), revocar los Certificados expedidos por determinada persona, etc.
- Después de haber ingresado el criterio de búsqueda se debe elegir "Mostrar los Certificados", para que éstos sean desplegados en pantalla.
- Se puede elegir entre revocar todos los Certificados desplegados en la lista o revocarlos individualmente.

Inmediatamente después de que un Certificado es revocado, éste es inscrito en la lista de Certificados Revocados de manera automática.

11.4 Cadenas de Autoridades Certificadoras

Como ya lo hemos estudiado, las Autoridades Certificadoras se pueden Certificar unas a otras. De esta manera se crea un lazo de confianza, ya que la Autoridad Certificadora que Certifica a otra Autoridad Certificadora está de acuerdo en los Procesos de Certificación de ésta. Y no sólo eso, sino que le tiene la suficiente confianza como para certificarla como una Autoridad Certificadora confiable. En el punto más alto de la cadena, habrá una Autoridad Certificadora que no está Certificada por nadie, o visto de otra manera, está siendo certificada por ella misma. A esta Autoridad Certificadora se le conoce como Autoridad Certificadora Raíz y es la que al final de cuentas Certifica a todas las demás en la cadena de certificación. La Cadena de Autoridades Certificadoras está organizada como una jerarquía en donde todas parten de la Autoridad Certificadora Raíz.

Desde el punto de vista del Servidor de Certificados de Netscape, una Autoridad Certificadora puede Certificar a otras, al expedirles un Certificado de Autoridad Certificadora, solamente que en este caso, se ve desde el punto de vista de poseer una Autoridad Certificadora esclava para delegar la tarea de expedir Certificados Digitales. A pesar del enfoque presentado por Netscape, Autoridades Certificadoras de distintas organizaciones se pueden Certificar unas con otras utilizando el mismo esquema. Básicamente una Cadena de certificación traza el camino desde las hojas hasta la Raíz, dentro de la jerarquía tipo árbol.

El certificado de la Autoridad Certificadora Raíz, se encuentra firmado por ella misma. Esto es, se encuentra firmado usando la llave privada correspondiente a la llave pública de su Certificado. Esta es una Autoridad Certificadora que se certifica a sí misma, por lo que hay que tener cuidado en verificar que este tipo de Autoridades Certificadoras sean realmente dignas de confianza.

11.4.1 ¿Cómo verifica Netscape las Cadenas de Certificación?

El proceso de verificación de una Cadena de Certificación consiste en asegurarse de que una Cadena dada esté bien formada, sea válida y esté firmada correctamente, además de verificar su confiabilidad. Netscape utiliza el siguiente procedimiento para formar y verificar una cadena dada, comenzando por el sujeto del Certificado (a quien se el expidió el Certificado Digital):

1. La fecha de expiración del Certificado es verificada, contra la fecha actual del sistema.
2. Se localiza el Certificado de la Autoridad Certificadora que expidió el Certificado a examinar. La fuente puede ser, tanto la base de datos local de quien lo verifica, como la Cadena de Certificación provista en el Certificado.
3. La firma digital del Certificado se verifica, usando la llave pública en el Certificado de la entidad que lo expidió.
4. Si el Certificado del usuario es confiable para quien lo verifica, en su base de datos local, la verificación se determina exitosa en este punto. De otra manera, el Certificado de quien expidió el Certificado a verificar, es revisado para verificar

que contenga la indicación de Autoridad Certificadora subordinada apropiada en las extensiones de X.509, y la verificación de la cadena regresa al paso 1 para comenzar otra vez, ahora con este nuevo Certificado.

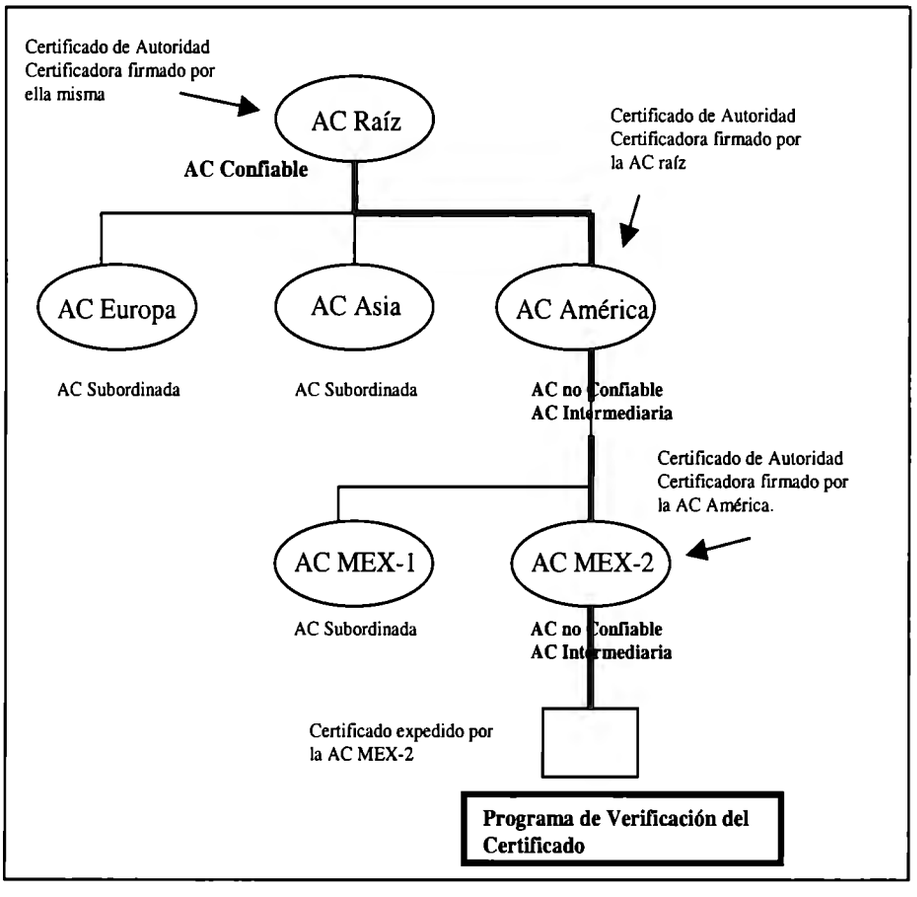

Figura 17: Verificación de un Certificado Digital

Es decir, la verificación de un Certificado Digital consiste en encontrar una Autoridad Certificadora confiable dentro de su cadena de certificación. Si dentro de la cadena presentada por el Certificado, no se haya alguna Autoridad Certificadora que sea confiable para el navegador local, la verificación falla, de otra forma la verificación resultará exitosa. De igual forma la verificación de un Certificado Digital fallará si éste expiró.

En caso de que la verificación falle, Netscape lo maneja de una manera muy especial. Por lo general se le da al usuario la oportunidad de aceptar un Certificado que ha expirado o cuya cadena de Certificación termina en una Autoridad Certificadora no confiable. El navegador presenta una serie de cuadros de diálogo para estos casos. El usuario puede aceptar el Certificado de manera temporal o definitiva. El usuario no puede aceptar Certificados para los cuales la verificación de

la firma de quien lo expidió haya fallado. Para el caso de los servidores de Netscape, los fallos en la verificación generalmente resultan en una falla en la autenticación.

11.5 Solicitud e Instalación de un Certificado de Autoridad Certificadora

Con el Servidor de Certificados de Netscape, se puede crear una jerarquía de Autoridades Certificadoras. Es decir, se provee la propiedad de que Autoridades Certificadoras se Certifiquen entre sí para formar una cadena de confianza entre Autoridades Certificadoras.

En el contexto del Servidor de Certificados de Netscape, este concepto está orientado a crear Autoridades Certificadoras subordinadas, para delegar el proceso de expedir Certificados.

Para solicitar un Certificado de Autoridad Certificadora se necesita generar una solicitud en la Autoridad Certificadora subordinada y entregar ésta a la Autoridad Certificadora servidora, la cual se encuentra arriba en la jerarquía.

El Administrador de la Autoridad Certificadora servidor, procesará la solicitud de Certificado y en caso de aceptarla, enviará el Certificado a su solicitante. Para generar la solicitud de Certificado de Autoridad Certificadora, se deben seguir los siguientes pasos:

- En el Administrador de Servidores, se debe escoger la opción de "Solicitar un Certificado de Autoridad Certificadora", que se encuentra en el apartado de Encripción. Entonces aparecerá la forma de petición del Certificado.
- Se debe ingresar la localización del archivo que contiene las llaves de la Autoridad Certificadora. Este es el archivo que contiene el par de llaves usado para firmar los Certificados
- En el campo de la contraseña, se debe ingresar la contraseña que protege la llave de la Autoridad Certificadora
- Si los datos son los correctos, elegir OK. Se deben salvar y aplicar los cambios. Cuando la forma es enviada, el servidor despliega la solicitud de

Certificado

- Se deberá copiar la sección acotada por las marcas "BEGIN" y "END", y ser guardada en un lugar seguro.

Los pasos para enviar la solicitud de Certificado de Autoridad Certificadora son los siguientes:

- Hacer contacto con la página principal Autoridad Certificadora servidora, la cual está arriba en la jerarquía.
- Se debe ingresar al menú de funciones privilegiadas
- Seleccionar la opción de "Solicitar Certificado de Autoridad Certificadora" para desplegar la forma de solicitud.
- La forma de solicitud pide la información necesaria para poder expedir el Certificado.
- En el área de texto, se debe pegar la solicitud de Certificado generada en el paso anterior.
- En la información del contacto, se debe ingresar la información que identifique al Administrador de la Autoridad Certificadora solicitante (nombre, teléfono, correo electrónico).
- En el campo de comentarios Adicionales, se puede ingresar información adicional acerca de la solicitud.
- Seleccionar "Enviar solicitud".

Después de haber solicitado el Certificado de Autoridad Certificadora, y después de haber recibido el nuevo Certificado por parte de la Autoridad Certificadora, se puede instalar el Certificado siguiendo los siguientes indicaciones.

Se debe acceder al Administrador de Servidores y escoger "Instalar Certificado" del apartado de "Encripción". Se debe escoger el tipo de Certificado a instalar, para este caso aplica la opción de "Certificado para la Autoridad Certificadora firmante en este servidor". Se debe, ya sea, indicar la localización exacta del archivo que contiene el Certificado o se debe pegar el Certificado codificado en el espacio provisto para ello. Se deben salvar y aplicar los cambios, además de detener y volver

a levantar el Servidor de Certificados.

11.5.1 Consideraciones en el cambio de la cadena de Certificación

Si antes de haber instalado el Certificado de Autoridad Certificadora, ya se habían expedido Certificados Digitales, éstos no contendrán la cadena de Certificación nueva y no serán reconocidos por los sistemas que la comparten. La única solución en este caso es revocar dichos Certificados y expedir nuevos, ya con la correcta cadena de Certificación.

11.6 Solicitud e Instalación de un Certificado de Servidor

Así como existen los Certificados personales, los Certificados para comunicaciones SSL y los Certificados para Autoridades Certificadoras, también existen los Certificados para Servidores. Un Servidor también puede tener su Certificado expedido por una Autoridad Certificadora confiable, para poder tener acceso a opciones privilegiadas, para autenticarse o para comunicaciones seguras utilizando el protocolo SSL, entre otras funciones.

El proceso para solicitar un Certificado para Servidor, es básicamente el mismo que el descrito para obtener un Certificado de Autoridad Certificadora. En primera instancia se tiene que generar la solicitud de Certificado para Servidor, esto se logra generando las llaves usando las herramientas provistas por el servidor. Si se trata de un Servidor Netscape, dentro del Administrador de Servidores se debe elegir "Generar llave" del apartado "Encripción". Una vez generado el par de llaves, se debe elegir la opción "Solicitar Certificado" y seguir las instrucciones.

Se debe ingresar una dirección de correo electrónico, a la cual será enviado el Certificado. Posteriormente la solicitud de Certificado es generada y mostrada en pantalla, no se debe olvidar copiarla y guardarla en un lugar seguro.

Para enviar la solicitud, es necesario hacer contacto con la página principal de la Autoridad Certificadora y escoger "Solicitar un Certificado de Servidor" del menú

público. Se deben llenar los datos requeridos y pegar la solicitud de Certificado generada con anterioridad. Posteriormente se debe enviar la solicitud para que ésta sea procesada.

Una vez enviada la solicitud y recibido el Certificado, éste se debe instalar de la siguiente manera:

- En el Administrador de Servidores del Servidor en el cual se instalará el Certificado de debe escoger "Instalar Certificado" del apartado "Encripción".
- Escoger "Este Servidor".
- Teclear un nombre para el Certificado.
- Existen dos maneras de cargar el Certificado
  - Salvar el correo electrónico que contiene el Certificado, usando "Salvar correo electrónico" y escribir la localización exacta de correo salvado en el campo apropiado.
  - Pegar el texto del correo comprendido entre -----BEGIN CERTIFICATE----- y ----- END CERTIFICATE -----, en el espacio asociado para ello.
- En el campo de Base de Datos de Certificados, escribir el nombre de la base de datos que maneja los Certificados.
- Salvar y aplicar los cambios. El servidor desencriptará el mensaje, extraerá el Certificado y lo salvará en la base de datos especificada.

11.7 Modificación de la Interfaz

El Servidor de Certificados de Netscape permite el modificar la interfaz predeterminada para llevar a cabo las funciones de su menú público y privilegiado. Estas formas están hechas en HTML y se pueden modificar para tener una apariencia diferente y para adecuarlas a los requerimientos de cada Organización.

Debido a que el proceso de operar con el Servidor de Certificados puede resultar complicado para la mayoría de los usuarios, se recomienda presentarles interfaces sencillas, amigables, con explicaciones claras y solicitando sólo la información necesaria. Para el caso de la información que resulte común para todos los usuarios,

es mejor no presentarla o presentar los campos llenos.

Para cambiar las interfaces, sólo hace falta substituir las antiguas formas por las nuevas. Es muy recomendable respaldar las formas antiguas para poder restituirlas en caso de fallo.

12. Desventajas del Servidor de Certificados de Netscape

Una desventaja del Servidor de Certificados es que, si bien la lista de Certificados Revocados se actualiza automáticamente cada vez que se revoca un Certificado, ésta por lo general no es consultada por los usuarios cada vez que reciben un Certificado Digital. Es por ello que se corre el riesgo de llegar a aceptar un Certificado ya no válido. La solución para este problema es que el navegador consulte de manera automática la lista de Certificados Revocados para verificar si el Certificado recibido aún es válido.

Otra gran desventaja se presenta a la hora de verificar un Certificado. La verificación será exitosa si la Autoridad Certificadora que expidió el Certificado es reconocida por el navegador local (su Certificado se encuentra en la base de datos local) o existe una Autoridad Certificadora confiable en la cadena de Certificación de la Autoridad Certificadora que expidió ese Certificado. El punto es que nunca se toma en cuenta a la Autoridad Certificadora para la verificación del Certificado, y hasta es probable que ésta ya no exista.

La solución para este problema es hacer la verificación del Certificado en línea, y directamente preguntar a la Autoridad Certificadora si ella expidió ese certificado. Ésta revisará sus bases de datos y sus firmas y verificará o no el Certificado presentado.

En el Servidor de Certificados de Netscape, nunca se toma en cuenta la Terminación de la Autoridad Certificadora. Por lo mismo no se trata el cómo se debe dar de baja y como debe ser el fin de la misma. La solución debe ser el proveer las funciones para la terminación de una Autoridad Certificadora y los medios para, en su caso,

delegar la responsabilidad y el manejo de los Certificados a otra Autoridad Certificadora.

13. Un poco de Conciencia de Seguridad

El Administrador debe hacer conscientes a sus usuarios de que tomen medidas de seguridad como:

- Proteger los Certificados con una contraseña.
- No dejar abierto el navegador.
- Al exportar un Certificado Digital, es necesario que éste sea cuidadosamente guardado en un lugar secreto en el disco duro, que no se encuentre accesible por red o en un disco flexible guardado bajo llave. La finalidad es que el Certificado no caiga en manos de terceros que puedan hacer mal uso de él.
- Establecer contraseñas seguras.
- No prestar el Certificado.
- No revelar las contraseñas.
- Etc.

Todo esto con la finalidad de contar con sistemas seguros, además al hacer al usuario responsable por todo lo que lleve su Certificado, se le obliga a aplicarle las medidas de seguridad adecuadas.

14. El papel del administrador

A lo largo de esta sección, se han expuesto algunas de las tareas que debe realizar el Administrador, de hecho el verdadero papel del Administrador es velar porque todo lo expresado en este trabajo de tesis se cumpla.

Es por ello que el Administrador debe dominar a la perfección todos los conceptos planteados a lo largo de este trabajo.

Capítulo 6

CASO DE ESTUDIO ITESM-CEM

En este capítulo se presenta el caso de estudio denominado: "Caso de estudio ITESM-CEM". Este trabajo sirve a varios propósitos:

- Resolver la problemática de certificación que está llevando a cabo la Dirección de Informática del ITESM-CEM.
- Servir de guía práctica para la implantación de una Infraestructura de Certificación en las organizaciones mexicanas.
- Ser una implementación práctica de toda la teoría expresada en esta tesis.

Una vez presentados los objetivos de esta sección, procederemos a la presentación del caso de estudio.

1. Planteamiento de la Problemática

Para poder implantar la administración de Certificados Digitales en el ITESM-CEM, debemos partir del principio que tenemos arriba 10,000 personas que pertenecen a la organización (entre alumnos, profesores y empleados). Todos ellos, como miembros activos de la organización, deben poseer un Certificado Digital para sus operaciones computacionales. El grave problema al que nos enfrentamos, es que la mayoría de los potenciales poseedores de Certificados Digitales no tienen formación informática. Esto significa que la mayoría tiene una vaga idea acerca de la seguridad computacional y por supuesto, no serían capaces de comprender los conceptos informáticos detrás de una infraestructura de Certificación.

El punto de partida para poder implantar la administración de Certificados Digitales, a nivel campus, es explicar al usuario en un lenguaje simple, cómo obtener y utilizar un Certificado Digital, así como las ventajas de utilizarlo. Sin olvidar el formarle un poco de conciencia en materia de seguridad computacional.

Los siguientes puntos, expresan algunos aspectos de la problemática específica del ITESM-CEM:

- Se suscitan demasiados casos de usurpación de la personalidad vía correo electrónico.
- Se practica el envío de correos ofensivos usurpando la personalidad del remitente.
- Demasiada carga de correo basura (cadenas, publicidad, falsas alarmas, etc.).
- No se tiene una manera de comprobar que el remitente envió un correo dado, por el cual se le inculpa.
- Se puede negar el haber enviado un mensaje dado.
- Las comunicaciones entre aplicaciones y bases de datos pasan por canales inseguros, sujetos a monitoreo.
- Etc.

Como nos podemos dar cuenta, estos problemas son los mismos a los ya planteados en capítulos anteriores, y son muy similares a los problemas que experimentan muchas de las organizaciones en México y en el mundo.

Estos problemas pueden ser reducidos utilizando como herramienta los Certificados Digitales y su respectiva Autoridad Certificadora. Pero más allá de resolver los problemas planteados, también se requiere contar con comunicaciones seguras que nos provean de las siguientes características:

- Confiabilidad: La confiablilidad tiene que ver con que el mensaje enviado sea exactamente el recibido. En otras palabras, que su contenido no haya sido alterado en su trayecto por la red.
- Privacidad: La privacidad tiene que ver con que un mensaje no pueda ser visto mas que por su destinatario original y está muy relacionado a las técnicas criptográficas.

Por ejemplo, si existen comunicaciones confiables y privadas, un profesor puede enviar un examen a través de la red, con la confianza de que va a llegar sin alteraciones y de que nadie fue capaz de leerlo en su trayecto por la red.

En primera instancia, la implantación de una infraestructura de certificación nos permitirá resolver en gran medida los problemas planteados, pero su utilización e integración en la operación diaria abrirá un panorama muy amplio de aplicaciones:

- Reportar calificaciones.
- Transmitir información confidencial.
- Enviar tareas.
- Enviar recibo de nómina por correo electrónico.
- Enviar comunicados oficiales.
- Enviar información encriptada.

- Cursos rediseñados.
- Comunicación confidencial entre administradores de sistemas.
- Manejo de firmas digitales.
- Etc.

2. Consideraciones Técnicas

Debido al uso tan amplio de los productos Netscape, los cuales se han convertido en un estándar, en materia de navegadores y correo electrónico dentro del Instituto, este caso de estudio está parcialmente orientado al uso del Servidor de Certificados Netscape, como base operacional de software de la Autoridad Certificadora del ITESM-CEM. Aunque se procurará realizar los planteamientos de tal manera que se puedan implementar, independientemente de la plataforma de software.

Todo alumno inscrito en el ITESM-CEM tiene responsabilidades para con el Instituto, así mismo, tiene derecho a todos los servicios que éste ofrece. Para que una persona sea considerada como alumno del ITESM-CEM, debe ser reconocida como tal ante la Dirección de Servicios Escolares, quienes se encargarán de proveer de la lista de alumnos inscritos a la Dirección de Informática para la generación de sus servicios computacionales.

Como parte de los servicios computacionales, todo alumno tiene una cuenta de correo electrónico provista por el ITESM-CEM, su uso debe ser de carácter oficial para todo asunto que al Instituto se refiera.

Así mismo la Oficina de Recursos Humanos del ITESM-CEM, deberá proveer la lista del personal activo a la Dirección de Informática para la generación de sus servicios computacionales. Uno de los servicios computacionales es la cuenta de correo electrónico, que del mismo modo que los alumnos, debe ser de uso oficial para todos los asuntos relacionados con el Instituto.

3. La Oficina de Certificación del ITESM-CEM

Para poder implantar el manejo de Certificados Digitales en el ITESM-CEM, se debe establecer una Oficina de Certificación o Departamento de Certificación, dependiente del Departamento de Seguridad Computacional de la Dirección de Informática. Esto es debido a la gran carga de trabajo que implica tener a cargo la infraestructura de Certificación de una organización tan grande. Se estima que la Oficina de Certificación del ITESM-CEM manejará arriba de diez mil Certificados Digitales.

3.1 Organización Jerárquica de la Oficina de Certificación del ITESM-CEM

La Oficina de Certificación debe quedar a cargo de un Administrador, esta persona será el responsable en jefe de la Autoridad Certificadora. Básicamente la función del Administrador es la de asegurarse que los Procesos de Certificación se lleven a cabo de manera exitosa. Dichos procesos serán descritos uno a uno y de manera detallada más adelante en este capítulo.

Algunas de las tareas más importantes que debe realizar el Administrador de la Autoridad Certificadora del ITESM-CEM son:

- Montar la Autoridad Certificadora
- Conformar su equipo de trabajo
- Dirigir la Autoridad Certificadora
- Implantar los Procesos de Certificación
- Planear el ciclo de vida de la Autoridad Certificadora

También debemos recordar que es responsabilidad del Administrador, el aumentar el conjunto de Procesos de Certificación conforme las necesidades del ITESM-CEM lo demanden.

Para poder cumplir con todas sus responsabilidades, el Administrador deberá apoyarse de su grupo de operadores. Los operadores de la Autoridad Certificadora tendrán como tarea, el apoyar al Administrador en los Procesos de Certificación. Se deberá nombrar a un operador como Suplente del Administrador, y éste tomará su lugar en caso de ausencia. Dicho operador deberá ser el más capacitado dentro del grupo de operadores y deberá dominar la mayoría de los procesos.

Acorde a las necesidades de Certificación del ITESM-CEM, se requerirá de un Staff base conformado por un Administrador y cinco operadores. Esto sin perder de vista que es mejor el contar con mayor personal. Debido a la naturaleza de las actividades de la Autoridad Certificadora, únicamente personal autorizado por la Oficina de Certificación podrá realizar actividades relacionadas con la certificación. El personal deberá firmar un contrato de buen uso sobre la información de seguridad que manejen, así como de las llaves y Certificados ajenos, acorde al código de ética y valores del ITESM-CEM.

Es posible reforzar el equipo de trabajo de la oficina de Certificación con personal de mucha confianza, debido a la naturaleza de las actividades que desempeñará.

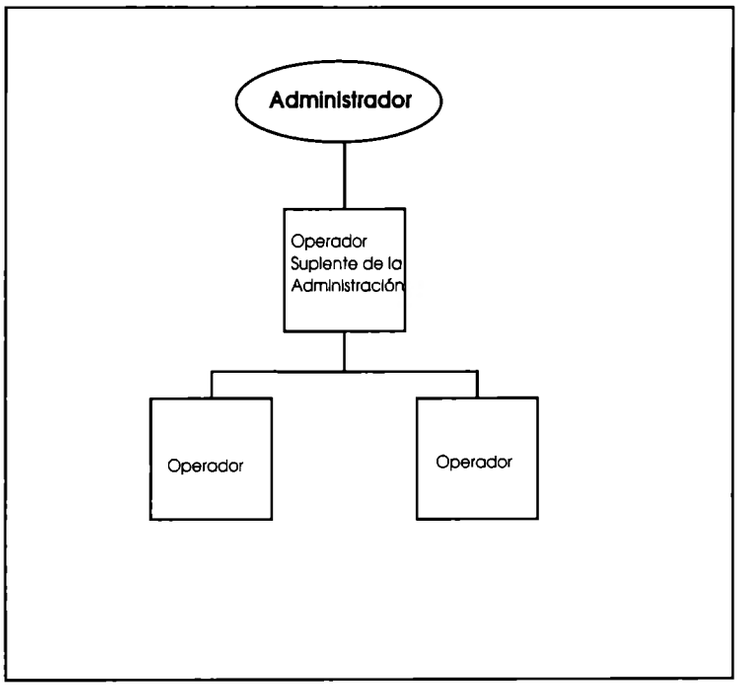

Figura 18: Organización jerárquica de la Oficina de Certificación del ITESM-CEM

Algunas de las tareas de los operadores de la Oficina de Certificación pueden ser: Emisión de Certificados Digitales, atender las solicitudes de Certificado, comprobación de la identidad de un solicitante, rechazo de una solicitud de Certificado, notificación de rechazo de una solicitud, entrega del Certificado Digital, instalación del Certificado, capacitación a usuarios, revocación de Certificados, notificación de baja de un Certificado, mantenimiento a la lista de Certificados expedidos, mantenimiento a la lista de Certificados revocados, renovación de un Certificado Digital, interacción entre Autoridades Certificadoras, entre otras.

4. Expedición de Certificados en el ITESM-CEM

La expedición de Certificados Digitales es la tarea medular de una Autoridad Certificadora. En el caso del ITESM-CEM, este proceso se torna especialmente particular debido al gran tamaño de la Organización y a la heterogeneidad de los usuarios.

La mayoría de los Procesos de Certificación son los mismos para todos los casos, pero debido a la heterogeneidad de los miembros del ITESM-CEM, en su caso, se hará la distinción entre los procesos que apliquen a los alumnos y los que apliquen a Profesores y empleados.

5. ¿A quién se le debe expedir un Certificado Digital dentro del ITESM-CEM?

Se le debe expedir un Certificado Digital a todo miembro activo del ITESM-CEM. Se considerará como miembro activo, a toda persona que caiga dentro de una de las categorías siguientes:

- Alumno
- Profesor

- Empleado Administrativo

6. Requisitos para obtener un Certificado Digital

Los requisitos para poder tener un Certificado Digital aplican a únicamente a los alumnos, y se resumen en el siguiente punto:

- Para que un alumno pueda poseer un Certificado Digital, deberá estar inscrito en el Instituto y estar cursando por lo menos una materia.

Para que un Profesor o empleado administrativo pueda obtener un Certificado Digital, no existe restricción alguna, de hecho para ellos es una obligación tramitarlo, poseerlo y utilizarlo.

7. ¿Quiénes están obligados a poseer un Certificado Digital?

Todo miembro activo del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Estado de México deberá tramitar, poseer y utilizar su Certificado Digital, bajo los lineamientos que marca el Departamento de Seguridad Computacional a través de su Oficina de Certificación.

Dichos lineamientos son parte de los Procesos de Certificación de la Autoridad Certificadora del ITESM-CEM y son los planteados en este capítulo.

8. Emisión de Certificados Digitales por parte de la Autoridad Certificadora del ITESM-CEM

La emisión de Certificados Digitales por parte de la Autoridad Certificadora del ITESM-CEM, se puede llevar a cabo de dos formas:

1. La Autoridad Certificadora del ITESM-CEM puede emitir los Certificados Digitales de los usuarios y posteriormente entregarlos (Emisión por parte de la Autoridad Certificadora).

2. El Usuario puede llevar a cabo el proceso convencional de solicitar su Certificado Digital ante la Oficina de Certificación del Campus Estado de México, esperar la resolución de ésta y recibir e instalar su Certificado Digital (Proceso convencional).

8.1 Emisión por parte de la Autoridad Certificadora

La emisión de los Certificados por parte de la Autoridad Certificadora del ITESM-CEM, consiste en que la Oficina de Certificación emita los Certificados Digitales de sus usuarios, para posteriormente entregárselos. Este Proceso omite el paso en el que el usuario solicita su Certificado Digital. Esta práctica nos asegura principalmente, que el usuario tendrá su Certificado Digital, ya que nosotros mismos le estamos proveyendo del mismo.

En primera instancia, la Dirección de Servicios Escolares y la Oficina de Recursos humanos del ITESM-CEM, deben proveer a la Oficina de Certificación de la Dirección de Informática, una lista en la que se incluya todo miembro activo del ITESM-CEM, como medio de comprobación de que realmente una persona es miembro del Instituto. Es decir, es un alumno inscrito en algún programa académico, cobra por nómina, etc.

Esta lista será consultada por los miembros de la Oficina de Certificación del ITESM-CEM para expedirle un Certificado Digital a quien esté inscrito en ella. El proceso de emitir el Certificado Digital por parte de la Autoridad Certificadora utilizando el Servidor de Certificados de Netscape consiste de los siguientes pasos:

- Solicitar el Certificado Digital a nombre del usuario sujeto del Certificado.

- Emitir el Certificado Digital al usuario.
- Importar el Certificado Digital.

Para este proceso el Servidor de Certificados deberá estar instalado y corriendo en un servidor determinado, y las tareas de solicitar, emitir e importar el Certificado Digital del usuario deberán llevarse a cabo desde las máquinas cliente de los operadores, en conexión directa con el Servidor de Certificados. Es por ello que si contamos con mayores recursos (técnicos y humanos), mayor será el avance en la emisión de Certificados Digitales.

El Solicitar el Certificado Digital, consiste en llenar la forma de solicitud de Certificado Digital a nombre del usuario (sujeto del Certificado). Para facilitar esta labor, se debe proveer al operador que la llenará, de una interfaz diseñada de tal manera que éste llene solamente la información que varía entre Certificado y Certificado.

Al enviar la solicitud, se genera el par de llaves correspondientes. La parte privada se queda residente en la máquina desde la cual se envía la solicitud. Es por ello que es importante que a la hora de importar el Certificado, se haga la misma máquina desde la cual se envió la solicitud.

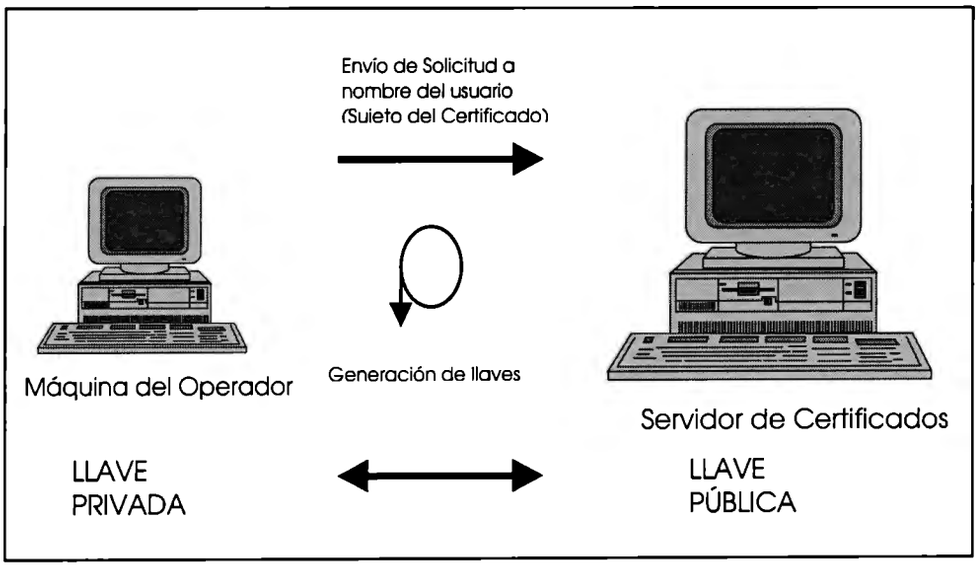

Figura 19: Solicitud de Certificado por parte del operador y estado de las llaves

La fase de Emitir el Certificado Digital, consiste en verificar la lista de solicitudes de Certificado en espera, tomar la solicitud enviada por el mismo operador, y emitir el Certificado Digital. Las opciones como el periodo de vida del Certificado, uso del Certificado, algoritmo de firma, etc. Serán establecidos por el Administrador.

Una vez que el Certificado ha sido emitido, éste se debe importar al navegador desde el cual se envió la solicitud de Certificado Digital. Esto se debe hacer dando click en el apartado de "Importar este Certificado al navegador" que se muestra inmediatamente después de haberlo expedido o desde el apartado de "detalles" después de haber buscado el Certificado. Posteriormente se debe escoger guardar el Certificado ("guardar como"). En ese momento será requerida la contraseña que protege a los Certificados del navegador local, y se requerirá una contraseña para el Certificado a ser importado. Una opción puede ser el colocar como contraseña del Certificado, la matrícula o el número de nomina del sujeto del Certificado. Debido a que esta es una contraseña muy débil, se le debe recordar al usuario que la debe cambiar al momento de instalar su Certificado Digital en su navegador.

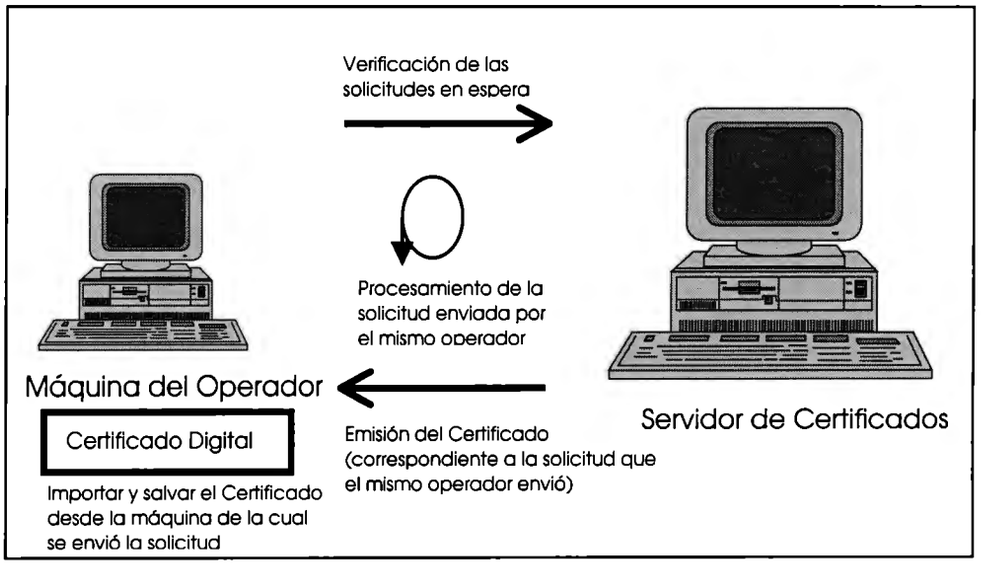

Figura 20: Procesamiento de la solicitud enviada por el operador.

8.2 Técnicas de Expedición de Certificados por parte de la Autoridad Certificadora

Existen varias técnicas para expedir los Certificados sin la intervención del usuario. Las técnicas dependen básicamente de los recursos (humanos y tecnológicos) con los que se cuenta, además del orden en el que se realizarán las tareas correspondientes. La finalidad es aprovechar al máximo todos los recursos con los que se cuenta, optimizar el proceso y hacerlo en el menor tiempo posible.

Se puede elegir entre las siguientes técnicas:

- Realizar el proceso de solicitar el Certificado Digital por parte del operador, para después emitir el mismo Certificado solicitado anteriormente, y por último importar ese Certificado. Es decir, realizar las tareas de solicitar, emitir e importar en ese orden por cada Certificado.

- Primero solicitar todos los Certificados de los usuarios, para posteriormente expedir los certificados e importarlos.

- Solicitar todos los Certificados de los usuarios, después expedir todos los Certificados para posteriormente importar todos los Certificados.

- Solicitar y procesar las solicitudes concurrentemente. Mientras unos operadores se dedican a solicitar, otros se dedican a procesar las solicitudes. Entre más equipos y más personas trabajen bajo esta técnica, se podrán expedir más Certificados en menor tiempo. Este factor es muy importante, si tomamos en cuenta que se trata de una organización que manejará arriba de diez mil Certificados Digitales.

Una opción más para la expedición de Certificados por parte de la Autoridad Certificadora, es la de automatizar el proceso de expedición de Certificados por parte del Servidor de Certificados de Netscape. Mediante un programa de auto verificación se puede lograr que el Servidor de Certificados que recibe una solicitud, la procese de manera automática y expida el Certificado.

Una ventaja es que se podría ganar tiempo ya que el paso de expedir el Certificado de manera manual es hecho de manera automática, pero en realidad es el único paso que se ahorra ya que los pasos correspondientes a la solicitud e importación del Certificado se siguen llevando a cabo, así que realmente la ganancia no es muy significativa.

Una gran desventaja es que el dejar que un programa procese de manera automática todas las solicitudes, es muy peligroso ya que significa aceptar todas las solicitudes sin siquiera comprobar la identidad del solicitante. Simplemente se pierde el sentido de la Autoridad Certificadora ya que cualquiera podría sacar un Certificado a nombre de otra persona y cometer ilícitos a su nombre.

Es altamente recomendable que si se va a utilizar un programa de auto verificación para expedir los Certificados de forma automática, se cierre todo acceso externo a la Autoridad Certificadora, mientras se lleva a cabo ese proceso.

En realidad el equipo de la Oficina de Certificación puede elegir la técnica que mejor le ajuste o inventar una propia, el objetivo es optimizar el proceso de expedición de Certificados por parte de la Autoridad certificadora.

8.3 Recursos y tiempo requerido

El tiempo promedio de expedición de un Certificado Digital para una persona que domina el Servidor de Certificados de Netscape es de dos minutos, esto es, una sola persona en una sola máquina. Si tomamos en cuenta que se requieren expedir

aproximadamente diez mil Certificados Digitales, entonces necesitamos 333 horas hombre para poder expedir todos los Certificados Digitales.

A una sola persona, en su jornada de trabajo normal de 8 horas diarias y dedicada enteramente a esa tarea, le tomaría aproximadamente 50 días el expedir los diez mil Certificados Digitales.

Si contáramos con el doble de recursos, es decir dos personas y dos equipos de cómputo, los diez mil Certificados se expedirían en aproximadamente 25 días. Es por ello que si contamos con un equipo de 5 personas, en teoría los diez mil Certificados quedarían listos en 10 días. Esto es considerando un poco de holgura en el proceso y tomando en cuenta que los miembros de la Oficina de Certificación deben atender también otras tareas de los Procesos de Certificación

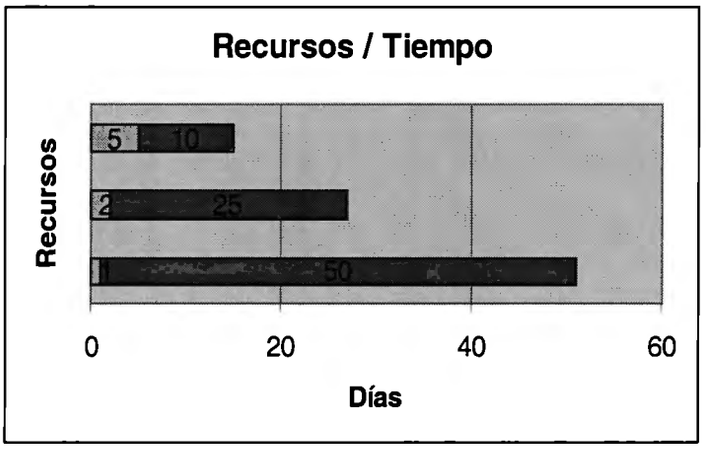

Figura 21: Recursos y tiempo requeridos para la expedición de 10 mil Certificados Digitales
(Los recursos están dados en personas y su respectivo equipo de cómputo y el tiempo en días)

8.4 Proceso Convencional

El llamado proceso convencional básicamente consiste en los siguientes pasos:

- Solicitud de Certificado Digital por parte del usuario
- Procesamiento de la solicitud de Certificado digital por parte de la autoridad Certificadora

- Entrega del Certificado Digital al usuario
- Instalación del Certificado Digital en la máquina del usuario

Como podemos ver, este es el proceso que se ha manejado a lo largo de este trabajo y el cual está descrito en los capítulos "Autoridad Certificadora" y "Servidor de Certificados Netscape". Es la manera usual de tramitar un Certificado Digital ante una Autoridad Certificadora.

8.5 Comparación entre ambas técnicas de emisión de Certificados

Existen dos maneras de expedir Certificados Digitales a los usuarios: el proceso convencional o la expedición por parte de la Autoridad Certificadora.

La ventaja del proceso convencional, es que se estaría llevando a cabo el proceso cual debe ser, además la Autoridad Certificadora no tendría que estar enviando las solicitudes de Certificado, papel que en teoría no le corresponde.

Una gran desventaja, es que debido a la heterogeneidad de los usuarios dentro del ITESM-CEM, no todos están interesados en poseer un Certificado Digital, o no le dan la importancia adecuada a este aspecto de la seguridad computacional. Además para algunos usuarios puede ser muy complicado entender para qué le sirve un Certificado Digital y cómo usarlo, además de cómo solicitarlo. Para estos casos la solución puede ser la capacitación y/o el expedirles el Certificado directamente en la oficina de Certificación.

La expedición de los Certificados Digitales por parte de la Autoridad Certificadora, tiene algunas desventajas, comenzando porque la Autoridad Certificadora realiza tareas que no le corresponden (solicitar un Certificado Digital) y representa una inmensa carga de trabajo. Sin embargo, puede ser necesario para introducir esta nueva tecnología y librar la resistencia inherente de los usuarios al cambio.

Las ventajas son que se asegura que el usuario posea un Certificado Digital, con lo que se conseguiría certificar a toda la comunidad del Campus Estado de México. De esta manera se le podría exigir al usuario el utilizar su Certificado Digital. Además de que se requiere de menor capacitación para los usuarios

9. Emisión de Certificados Digitales para toda la comunidad de ITESM-CEM

A este respecto se pueden utilizar innumerables técnicas para Certificar a toda la comunidad del CEM. En esta sección se presentaran varias alternativas que ayudarán a la labor de certificación, o en su caso, sentarán las bases para obtener una nueva que mejor ajuste a las necesidades de certificación del ITESM-CEM, muchas de estas técnicas son dependientes de los recursos con los que se cuenta y el tiempo en el que se requiere llevar a cabo la Certificación.

A continuación presentaremos dos técnicas de certificación: Certificación Masiva y Certificación Convencional. Ambas técnicas serán planteadas, para posteriormente sugerir la técnica ideal para certificar a toda la comunidad del ITESM-CEM.

9.1 Certificación Masiva

La certificación masiva consiste en expedir los cerca de diez mil Certificados Digitales, por medio de la Autoridad Certificadora. Como pudimos verlo con anterioridad, éste proceso puede tomar aproximadamente 10 días en llevarse a cabo, contando con los recursos humanos y computacionales adecuados.

El proceso de la certificación masiva depende de montar un equipo de trabajo enteramente dedicado a la expedición de Certificados Digitales durante los 10 días, la meta es entonces, expedir aproximadamente 1000 certificados por día. Si contáramos

con un equipo de 5 personas, la meta sería expedir 200 certificados diariamente por persona.

La técnica de certificación masiva no es imposible, pero requiere de una larga jornada de arduo trabajo, y muy probablemente de reforzar el equipo de trabajo de la Oficina de Certificación con empleados de mucha confianza, debido a la naturaleza del trabajo que llevarán a cabo.

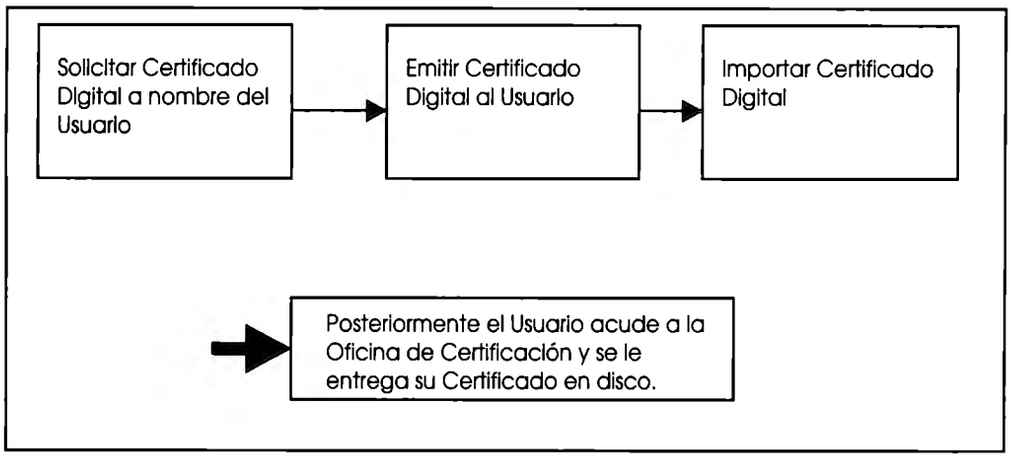

Figura 22: Certificación Masiva

Es muy importante tomar en cuenta que para levar a cabo la certificación masiva se requiere contar con un equipo de cómputo por cada persona trabajando en la expedición de Certificados Digitales, lo que aumenta los requerimientos de recursos.

La técnica de certificación masiva es muy útil si se requiere certificar a toda la comunidad del CEM en un corto lapso de tiempo.

9.2 Certificación convencional

La certificación convencional, es el Proceso tradicional para tramitar un Certificado Digital. En él, la Autoridad Certificadora del ITESM-CEM, debe proveer una interfaz para la solicitud de Certificados Digitales a sus usuarios. Si trabajamos bajo el Servidor de Certificados de Netscape, se debe proveer una interfaz diferente a la original, la cual

contenga únicamente las opciones de "Solicitar el Certificado Digital" y la de "Aceptar la Autoridad Certificadora". Esto es con la finalidad de evitar complicaciones a los usuarios. Además no se deben pedir datos que sean comunes a todos los Certificados, es mejor que los campos aparezcan ya llenos.

Después de haber solicitado el Certificado Digital, el usuario debe esperar la resolución por parte de la Autoridad Certificadora y su Certificado le será entregado vía correo electrónico, no sin antes llevarse a cabo los procesos de comprobación de la identidad del solicitante.

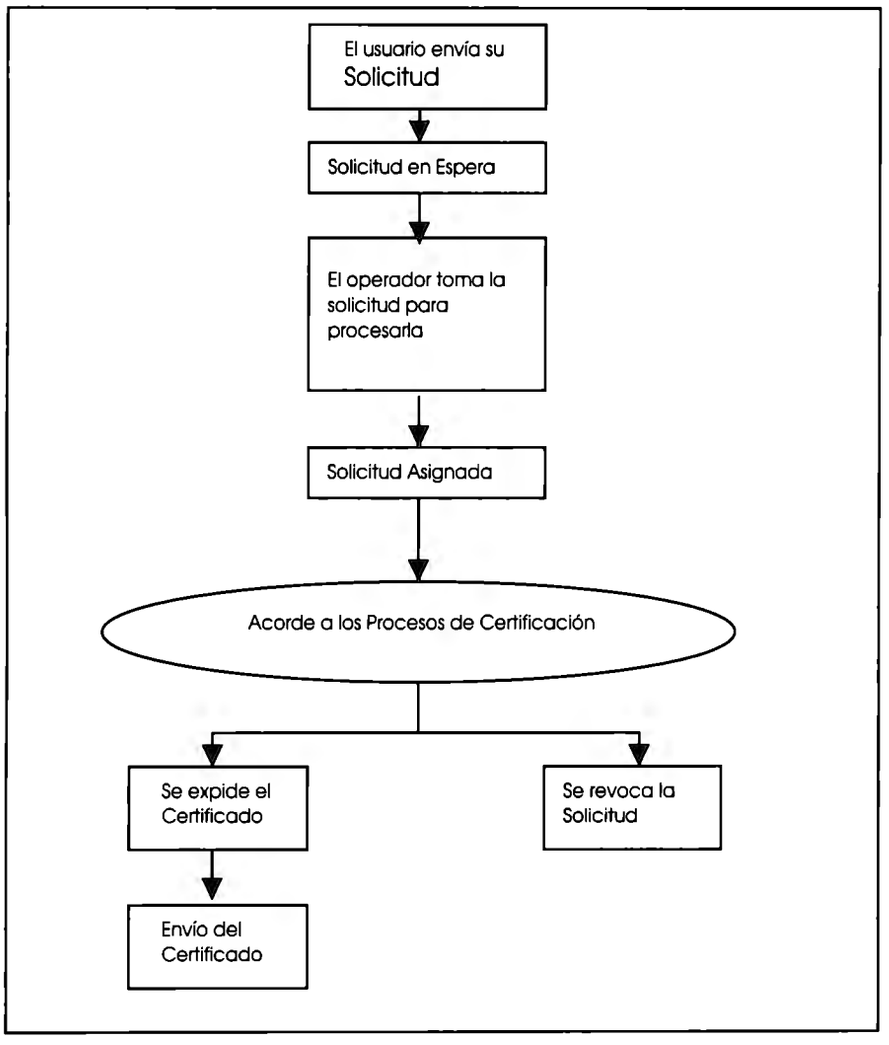

Figura 23: Certificación Convencional

9.3 Técnica de Certificación para el ITESM-CEM

Para certificar a toda la comunidad del ITESM-CEM, debemos tomar en cuenta varios factores, el principal es que es un número muy grande de certificados los que se deben expedir, cerca de diez mil; además la gran parte de la población del ITESM-CEM no tiene formación informática.

El hecho de que gran parte de la población no tenga formación informática, afecta significativamente que el proceso convencional de certificación se lleve a cabo, debido a los siguientes factores:

- El usuario no tiene conciencia de la seguridad computacional
- El usuario puede encontrar difícil el solicitar un Certificado Digital y no solicitarlo
- El usuario puede encontrar difícil el instalar su Certificado Digital
- El usuario puede ignorar las recomendaciones de tramitar un Certificado Digital
- El usuario puede preferir que el Certificado le sea entregado en mano

Por su parte, para la Autoridad Certificadora del ITESM-CEM resultaría demasiado complejo el llevar a cabo todo el ciclo convencional para tramitar el Certificado, debido a que además de recibir las diez mil solicitudes de Certificado, tendría que llevar a cabo las diez mil comprobaciones de la identidad del solicitante (ver "Comprobación de la identidad de un solicitante" en el capítulo "Autoridad Certificadora").

Supongamos que en el mejor de los casos, el proceso de verificación de la identidad del solicitante tomara 3 días hábiles en llevarse a cabo, y que la Oficina de Certificación es capaz de procesar 50 certificados por día. En este caso se requerirían más de 200 días naturales para poder concluir con el proceso. Esto es más de dos semestres convencionales de 16 semanas.

Este proceso funcionaría únicamente si la Oficina de Certificación tuviera los recursos suficientes para expedir 50 Certificados por día y tuviera en efecto, mínimo las 50 solicitudes para procesar día a día. Esto significaría que toda la comunidad del CEM participara enviando su solicitud oportunamente y no hubiera retraso, siguiendo el proceso al pié de la letra.

Es por ello que se propone como estrategia de certificación para el ITESM-CEM, la certificación masiva. Ésta permitirá que la Oficina de Certificación del CEM se asegure que todo miembro activo de la organización posee su Certificado Digital, ya que ella misma le esta proveyendo de él. Además de ser un proceso que se lleva a cabo en menor tiempo y bajo absoluto control de la Autoridad Certificadora. Se ahorra el proceso de comprobar la identidad del solicitante, ya que se expedirán certificados digitales únicamente a personas autorizadas por la Dirección de Servicios Escolares y la Oficina de Recursos humanos del ITESM-CEM, además de que la Autoridad Certificadora puede estar segura de que nadie solicitó un Certificado a nombre de otra persona. Es un proceso repetitivo y automatizado, el cual no representa mucha dificultad, la dificultad radica en el volumen de Certificados a manejar.

Mediante esta técnica lograremos certificar a toda la comunidad del ITESM-CEM actual. Para la certificación de quienes hayan quedado fuera de la certificación masiva, se utilizará la certificación convencional. Este tipo de certificación será utilizada de forma alternativa.

10. Campos de un Certificado Digital

El Certificado Digital debe contener la información necesaria para poder identificar a su portador. Los campos que debe contener el Certificado Digital para los miembros del ITESM-CEM son los siguientes:

- Rectoría
- Campus
- Dirección / División
- Departamento
- Función
- Datos Personales
- Nivel de Seguridad

El campo función, se refiere al papel de la persona sujeto del Certificado dentro del ITESM-CEM, ese campo puede ser llenado con una de las cuatro categorías siguientes: Profesor, alumno, empleado administrativo o directivo.

Adicionalmente, se puede incluir el Nivel de seguridad, éste será establecido y otorgado a los diversos usuarios por el departamento de seguridad computacional de acuerdo a la política de seguridad del ITESM-CEM. No debemos perder de vista que la función principal de un Certificado Digital es la de identificar a un usuario, ya el nivel de seguridad y los privilegios de los que éste goza, son responsabilidad de la aplicación que acepta el Certificado Digital, pero dicho nivel de seguridad también puede ser incluido en el Certificado.

Los datos personales incluyen la siguiente información: Nombre completo, login, correo electrónico, unidad organizacional, organización, país y teléfono.

Para poder implementar estos campos, se debe hacer uso de las extensiones X.509. Estas extensiones se deben programar para que dichos campos sean incluidos en el Certificado Digital emitido. Este proceso, está descrito más adelante en este capítulo.

11. Solicitud de un Certificado Digital

La solicitud de un Certificado Digital aplica básicamente a la técnica de certificación convencional. El proceso de solicitar un Certificado Digital mediante los procesos

convencionales, consiste básicamente en que la Autoridad Certificadora del ITESM-CEM provea una interfaz a los usuarios para la solicitud de un Certificado.

Utilizando el servidor de Certificados de Netscape, la interfaz para solicitar el Certificado es de acceso vía web y debe presentar formas para ser llenadas por el usuario. Las formas deben ser distintas a las originales, ya que éstas pueden causar confusión a los usuarios debido a la complejidad y número de funciones presentadas.

La forma a llenar por el usuario debe pedir información del usuario como: Nombre completo, login, correo electrónico, unidad organizacional, organización, país y teléfono. Adicionalmente se puede proveer al solicitante de un espacio para enviar algunos comentarios a la Oficina de Certificación.

Se entiende por unidad organizacional el área o departamento dentro de la jerarquía organizacional. En el caso de teléfono se debe ingresar el teléfono de oficina (en caso de ser empleados) o el teléfono particular (en caso de ser alumnos).

Para el caso en que existan campos que sean comunes a todo el mundo, como es el caso de la organización (ITESM-CEM), éstos deben estar previamente llenados para evitar que el usuario pierda tiempo llenándolos y evitar que los llene incorrectamente.

Además la forma debe contener las instrucciones de llenado y la descripción de cada campo a llenar. Se debe incluir un teléfono y/o dirección de correo electrónico para poder contactar a la Oficina de Certificación, en caso de requerir asistencia técnica.

Cabe la posibilidad de que una persona solicite un Certificado a nombre de otra, para evitar que se le expida el Certificado a dicho impostor, se debe llevar a cabo el proceso de comprobación de la identidad del solicitante. Este tipo de fraude se evita utilizando la técnica de expedición de Certificados por parte de la Autoridad Certificadora utilizada en la certificación masiva.

12. Comprobación de la identidad de un Solicitante

Para el caso específico del ITESM-CEM, la tarea de comprobar la identidad de un solicitante se ve aliviada debido a que todo miembro activo de la organización ha pasado previamente por un proceso de inscripción o reclutamiento que ya ha comprobado su identidad.

Es por ello que para comprobar que un solicitante es en efecto miembro activo del ITESM-CEM, se tiene que consultar a la Dirección de Servicios Escolares o a la Oficina de Recursos humanos. Se debe solicitar a estas oficinas, la información general que nos permita comprobar la identidad del solicitante. Esta información puede ser, dirección, teléfono, área en la que labora, si tiene algún impedimento para hace uso de los servicios informáticos, etc.

El siguiente paso es hablar directamente con el solicitante para verificar que en efecto haya sido él quien envió la solicitud de Certificado Digital. Este proceso se puede llevar a cabo ya sea contactándole vía telefónica, o visitándole directamente en su oficina dentro del ITESM-CEM.

Si llegara a haber inconsistencia entre la información provista por el solicitante y la provista por la Dirección de Servicios Escolares o la Oficina de Recursos humanos del ITESM-CEM, la solicitud debe ser rechazada debido a que la comprobación de la identidad del solicitante falló (ver sección siguiente).

13. Rechazo de una Solicitud de Certificado Digital

Existe la posibilidad de que una solicitud enviada por un usuario sea rechazada. Los motivos de rechazo de solicitud pueden ser los siguientes:

- No se pudo comprobar la identidad del solicitante
- El solicitante no es miembro del ITESM-CEM
- La solicitud fue llenada de manera incorrecta
- El solicitante no cumple con las políticas de seguridad del ITESM-CEM
- Inconsistencia entre los datos provistos por el usuario y los provistos por la Oficina de Recursos Humanos o por la Dirección de Servicios Escolares.

En el caso de que una solicitud haya sido rechazada, se debe documentar el hecho para tener un registro de eventos.

13.1 Notificación de Rechazo de una Solicitud de Certificado Digital

En el caso de que una solicitud haya sido rechazada debido a que ésta fue llenada de forma incorrecta por parte del usuario, el operador de la Oficina de Certificación debe notificarlo al usuario para que envíe de nuevo su solicitud.

Si la identidad del usuario no pudo ser comprobada, la solicitud debe ser rechazada de inmediato y notificarlo vía correo electrónico al solicitante. De la misma manera, se debe comunicar el rechazo de la solicitud a un miembro externo al ITESM-CEM que haya solicitado un Certificado Digital.

Para el caso en que el usuario no cumpla con las políticas de seguridad del ITESM-CEM, por ejemplo, si perdió el derecho a utilizar su Certificado Digital o si es considerada una persona peligrosa, etc. Se le debe notificar del rechazo de su solicitud y de las razones.

Es muy importante que todos los rechazos y sus motivos sean documentados para referencias futuras.

14. Entrega del Certificado Digital

Para que un miembro del ITESM-CEM obtenga su Certificado Digital, tiene que dirigirse personalmente a la Oficina de Certificación para recogerlo. El Certificado (que fue emitido de manera masiva) será entregado en disco al usuario, así mismo se le entregará la contraseña que lo protege.

Es muy importante que el usuario proteja su Certificado con una contraseña distinta a la que se le ha entregado en la Oficina de Certificación, de tal manera que sea él la única persona que la conozca, y por lo tanto, que sea la única persona que tenga acceso a la llave privada del Certificado Digital.

Bajo ninguna circunstancia se entregarán Certificados a otra persona que no sea el titular del Certificado (sujeto del Certificado).

En esta etapa se podrá solicitar al usuario que se comprometa a dar buen uso de su Certificado, mediante la firma de una carta compromiso.

15. Instalación y cambio de contraseña del Certificado

Una vez entregado el Certificado, éste deberá ser instalado en el navegador del usuario. Para poder instalar el Certificado en el navegador, se debe seguir el procedimiento de Importar el Certificado un Certificado Digital, explicado en el capítulo "Servidor de Certificados de Netscape".

En este proceso, será requerida la contraseña que protege al Certificado y será requerida una nueva contraseña para importarlo, es en este punto en el que se debe cambiar la contraseña para el Certificado.

15.1 Instalación del Certificado en la máquina del usuario por parte del personal de la Dirección de Informática

El instalar el Certificado Digital directamente en las máquinas de trabajo de los usuarios es una labor que resultaría titánica, ya que no solamente consistiría en el proceso de importar el Certificado Digital, sino que implica también el desplazamiento del personal de la Oficina de Certificación a la oficina del usuario. O en su caso, implicaría tener una fila interminable de alumnos esperando a que su Certificado sea instalado en su computadora personal.

El importar un Certificado Digital a una máquina cliente es un proceso que toma en promedio 20 segundos, por lo que el trabajar con 10000 Certificados Digitales nos tomaría aproximadamente 56 horas hombre. Esto sin contar el tiempo invertido en desplazarse a la oficina del usuario y el tiempo que tarda el usuario en tener su máquina lista para el proceso.

Este proceso se puede llevar a cabo como una segunda etapa después de la emisión de los Certificados Digitales de manera masiva. Para completar la instalación de los 10000 Certificados Digitales, contando con nuestro equipo de trabajo de cinco personas, requeriríamos aproximadamente una semana de trabajo dedicada a la instalación.

Realmente esta técnica no es muy recomendable, ya que puede verse afectada por diversos factores externos. Ya que habría que ajustarse a las agendas de los usuarios, y los desplazamientos del personal de la Oficina de Certificación retrasan mucho el proceso.

Es por ello que se recomienda esta técnica si algún usuario experimenta problemas al instalar su Certificado Digital en su máquina de trabajo, y a manera de asistencia técnica, el personal de la Oficina de Certificación de la Dirección de Informática, tenga que instalar el Certificado Digital directamente en la máquina del usuario.

El proceso de importar un Certificado Digital, esta descrito en el capítulo "Servidor de Certificados Netscape".

16. Aceptar Autoridad Certificadora del ITESM-CEM

Para que todo el esquema de utilización de Certificados Digitales pueda funcionar, los usuarios deben aceptar la Autoridad Certificadora del ITESM-CEM como su Autoridad Certificadora. Esto quiere decir que la están adoptando como tal, por lo que su navegador recibirá como válidos a todos los Certificados Digitales que hayan sido expedidos por dicha Autoridad Certificadora.

La Oficina de Certificación debe proveer de una interfaz accesible vía web, que presente un apartado para aceptar la Autoridad Certificadora y que éste proceso sea tan sencillo como dar un click. Al utilizar el Servidor de Certificados de Netscape, el proveer de esta interfaz es muy sencillo.

17. Capacitación a Usuarios

El departamento de seguridad computacional de la Dirección de Informática, debe organizar diversas sesiones de capacitación en materia de Certificados Digitales para la comunidad del ITESM-CEM. Estas sesiones tienen como objetivo el informar al usuario en un lenguaje al alcance de su comprensión, el significado, utilización y utilidad de un Certificado Digital. Así mismo, se busca concientizar a los usuarios en materia de seguridad computacional y que encuentren en los Certificados Digitales, una solución a problemas comunes en materia de seguridad computacional.

En primera instancia se debe trabajar a niveles de primera y segunda línea, además de dirección de carrera. Ellos serán quienes se encarguen de transmitir la concientización y de invitar a la gente a su cargo a la obtención y uso del Certificado Digital.

Se debe reforzar la capacitación con un folleto informativo en materia de Certificados Digitales. Este folleto contendrá la información de cómo obtener, instalar y utilizar el Certificado Digital, así como la información básica de para qué sirve un Certificado Digital, cómo funciona, etc.

De igual manera se debe incluir tanto en la capacitación como en el folleto informativo, las condiciones de uso, obligaciones y responsabilidades, así como una guía de buen uso del Certificado Digital.

18. Uso del Certificado Digital

Las aplicaciones de los Certificados Digitales son muy amplias, de hecho el uso de los Certificados se puede extender tanto como la imaginación de los usuarios pueda alcanzar. Nos podemos hacer preguntas como: ¿Qué nos asegura que los Avisos Generales en efecto los envió la oficina de comunicación?, ¿Quién nos asegura que los comunicados de dirección de carrera realmente provienen del director de carrera?, ¿Cómo sabemos si realmente algún profesor o alumno envió un correo ofensivo a otro profesor o alumno?, ¿Cómo compruebo que yo no envié algún mensaje?, ¿Cómo proteger de espías la información que viaja por la red?, ¿Cómo se sabe que una indicación de niveles altos, realmente proviene de la persona que aparece como remitente?, etc.

Todos estos problemas y muchos otros pueden ser resueltos mediante la utilización de Certificados Digitales. El utilizar un Certificado Digital significa tomar medidas de seguridad que serán benéficas para todos.

Mediante el uso del Certificado Digital, podemos explotar las características de Firma Digital y encripción de la información. Algunos ejemplos de uso del Certificado son:

Firma Digital

- Ordenes del jefe a sus empleados
- Memorándums
- Comunicados Oficiales
- Avisos de la Dirección
- Avisos Oficiales de Otras áreas
- Mensajes de interacción con nuestros clientes (facturas, cotizaciones, etc.)
- Peticiones de información entre áreas
- Interacción entre áreas ó departamentos
- Información de rutina entre los miembros de la Organización
- Envío de tareas firmadas
- Memorándums de salida o traslado de equipo o material
- Memorándums de préstamo de material
- Comunicación entre administradores de sistemas

Encripción

- Comunicación entre Directivos
- Información Confidencial
- Contratos
- Manejo de cifras e información confidencial (sueldos, estados contables, estados de cuenta, etc.)
- Reporte de Calificaciones
- Comunicación entre administradores de sistemas

Además podemos explotar la característica de autenticación mediante el Certificado Digital.

19. Tiempo de vida de un Certificado

Un aspecto muy importante a tomar en cuenta, es el tiempo de vida que tendrán los Certificados expedidos por la Autoridad Certificadora. Como los Certificados serán expedidos de manera masiva, todos expirarán por las mismas fechas. Esto sería un grave problema ya que se tendrían que renovar los cerca de diez mil Certificados expedidos, por lo que ahora tendríamos una renovación masiva.

Para evitar el problema de una renovación masiva, se podrían fijar diferentes periodos de vida para los diferentes Certificados, pero esto retrasaría el proceso de certificación masiva, así que no resulta ser una alternativa viable.

En teoría el tiempo máximo que se utilizará un Certificado Digital es de nueve semestres, que es la duración de una carrera profesional completa en el ITESM-CEM. Es por ello que se fijará el periodo de vida de todos los Certificados en nueve semestres, esto nos asegura que no habrá problemas de renovación masiva y que el usuario tendrá su Certificado Digital mientras sea miembro activo del ITESM-CEM. Para el caso de las personas que abandonen la Institución por cualquier causa, su Certificado será revocado aunque éste no haya expirado aún.

20. Responsabilidades y Obligaciones del Usuario

De la misma manera que una persona se responsabiliza por los documentos que tengan estampados su firma, un usuario es responsable de todo mensaje que vaya firmado con su Certificado Digital. El usuario deberá responder por el contenido de los mensajes firmados digitalmente por él.

Esto obliga al usuario a hacer buen uso de su Certificado Digital y a procurarle medidas de seguridad, algunas de las obligaciones y responsabilidades del usuario son:

- El usuario es el único responsable de su Certificado Digital
- El usuario tiene la responsabilidad de cuidar que sólo él tenga acceso a la llave privada de su Certificado Digital
- El usuario debe proteger la llave privada de su Certificado Digital con una contraseña
- El usuario no debe revelar la contraseña que protege a su Certificado Digital
- El usuario no debe prestar su Certificado Digital
- El usuario debe cambiar su contraseña periódicamente
- El usuario debe reportar inmediatamente a la Oficina de Certificación si sospecha que su llave privada ha sido expuesta.
- Todo Administrador de equipos computacionales debe poseer y utilizar su Certificado Digital de manera obligatoria.

21. Intercambio de llaves

A lo largo de este trabajo de tesis, se han tratado dos tipos de intercambio de llaves: Intercambio directo entre usuarios y Uso de un Servidor de Directorio.

Al utilizar los Certificados de Netscape, la primera técnica es la más sencilla e inmediata, ya que sólo basta con enviar un mensaje firmado con el Certificado Digital al usuario que se desea lo posea, y al recibirlo automáticamente se instalará en su navegador Netscape. Bajo esta técnica yo le puedo enviar mi Certificado Digital exclusivamente a las personas que deseo lo posean.

Una gran ventaja de esta técnica de intercambio de llaves es que no se necesita una infraestructura adicional, ni de montar servidores adicionales para que funcione, de hecho es una función natural de los navegadores Netscape, es por ello que es la más conveniente.

En cuanto al Servidor de Directorio, que trabaja bajo el principio de llavero público, se requiere de montar la infraestructura de Directorio adicional, pero es compatible con el Servidor de Certificados de Netscape. El manejo de un Servidor de Directorio esta fuera del alcance de este trabajo. Aunque es una estrategia del sistema ITESM el contar con la infraestructura de directorios.

22. Utilización del Certificado Digital en una máquina pública

Para poder utilizar el Certificado Digital desde una máquina pública, como lo pueden ser las maquinas ubicadas en los Laboratorios de Cómputo Especializado y en las salas generales de computadoras, se requiere portar el Certificado en disco flexible.

Para poder guardar el Certificado Digital en un disco flexible, es necesario exportarlo de la manera convencional descrita en el capítulo "Servidor de Certificados Netscape" y darle como destino de la exportación el disco flexible.

Una vez guardado el Certificado en disco, éste puede ser llevado a cualquier lugar y podrá ser instalado en cualquier máquina. El proceso para importar un Certificado esta descrito en el capítulo "Servidor de Certificados Netscape".

Aunque no es posible utilizar el Certificado Digital de una persona si no se cuenta con la contraseña que protege a la llave privada, es obligación del usuario el borrar su Certificado Digital de una máquina pública después de usarlo.

23. Revocación de un Certificados

Un Certificado debe ser revocado si alguna de la siguientes condiciones se cumple:

- La llave del usuario se ha puesto en peligro
- El usuario no pertenece más al ITESM-CEM como miembro activo

- El usuario perdió los derechos a utilizar su Certificado Digital
- El usuario fue suspendido temporalmente del ITESM-CEM

El usuario puede perder su derecho a utilizar su Certificado Digital si ha infringido las políticas del ITESM-CEM y se ha hecho acreedor a una sanción o ha perdido el derecho a utilizar los servicios informáticos.

Para que la Oficina de Certificación pueda estar al tanto de los usuarios cuyos Certificados se deben revocar, debe estar informada por parte de las demás áreas del ITESM-CEM sobre el estado que guardan los alumnos y empleados.

24. Notificación de baja de un Certificado

La Oficina de Certificación tiene la obligación de notificar a los usuarios de la revocación de un Certificado Digital. En primer lugar se debe notificar al dueño del Certificado de la baja de su certificado y de las razones que causaron la revocación, este proceso se debe documentar para referencias futuras.

Otro aspecto a cuidar es que los demás usuarios estén enterados de que un certificado ha sido revocado para que ya no lo acepten más. La manera más transparente de hacerlo es mediante la lista de Certificados Revocados, la cual debe estar accesible a todo el mundo. Una desventaja de dicha lista, es que no todo el mundo acostumbra revisarla, por lo que la Oficina de Certificación debe enviar semanalmente por correo electrónico a toda la comunidad, los Certificados que han sido revocados.

25. La lista de Certificados Expedidos y Revocados

Las listas tanto de Certificados revocados, como de Certificados expedidos, se mantienen actualizadas de manera automática utilizando el Servidor de Certificados Netscape.

Sólo basta que los usuarios visiten la página principal de la Autoridad Certificadora y consulten dichas listas en el apartado de operaciones públicas.

26. Renovación de un Certificado Digital

En el caso de que el Certificado de un usuario llegara a expirar, el usuario puede solicitar la renovación de su Certificado Digital directamente en la Oficina de Certificación. Para este fin, la Oficina de Certificación debe proveer de formas de solicitud de renovación de Certificado, la cual deberá ser llenada por el usuario.

Trabajando con el Servidor de Certificados de Netscape, la renovación se lleva a cabo de la siguiente manera:

- Se debe acceder al menú de operaciones privilegiadas
- Se deben listar las solicitudes de Certificados ya procesadas
- Se debe localizar la solicitud de la persona indicada
- Se expide de nuevo el Certificado Digital

Ya que se expidió el Certificado Digital, éste se puede enviar vía correo electrónico al solicitante.

27. Responsabilidad de la Autoridad Certificadora del ITESM-CEM

Los Certificados expedidos por la Autoridad Certificadora del ITESM-CEM son para uso interno al sistema Tecnológico de Monterrey y la Autoridad Certificadora únicamente los expide para reconocer a alguien como miembro de la organización y para su uso dentro de la misma. Nunca se expiden los Certificados para operaciones monetarias ni para asuntos ajenos al Instituto.

Debido a que para Certificar a al comunidad del ITESM-CEM se utilizará la técnica de certificación masiva, los Certificados y su llave privada quedarán en poder de la Autoridad Certificadora, lo que la convierte en un blanco de ataques. Es por ello que los Certificados se tienen que importar a un Servidor que será desconectado de red después que la certificación masiva termine y permanecerá aislado en un cuarto de acceso restringido por medidas de seguridad.

La Autoridad Certificadora del ITESM-CEM tiene la responsabilidad de salvaguardar la seguridad de dichos Certificados y de solamente acceder a ellos en caso de que se requieran entregar al usuario. Todo el equipo de la Oficina de Certificación debe tener absoluto respeto y cuidado por los Certificados ahí guardados ya que son su entera responsabilidad.

El guardar los Certificados Digitales nos permitirá reponerlo en caso de que se requiera sin necesidad de dar por perdidos los mensajes que ya se tenían.

28. Interacción entre Autoridades Certificadoras

Se puede pensar formar una jerarquía de Autoridades Certificadoras para todo el sistema ITESM. Se puede partir de una Autoridad Certificadora rectora y sus Autoridades Certificadoras esclavas en cada campus del sistema, formando así una cadena de Autoridades Certificadoras a nivel nacional.

El implementar una cadena de certificación a nivel nacional es un proyecto ambicioso pero a su vez realizable. El contar con este esquema a nivel nacional nos permitiría explotar las ventajas de los Certificados Digitales, inclusive con otros campus del sistema. Por ejemplo, se podría intercambiar información encriptada entre personas de diferentes campus y por supuesto se podrían reconocer las firmas digitales de todos los miembros del Sistema ITESM.

29. Proyección a futuro

Al montar una infraestructura de Certificación robusta y al estar siempre a la vanguardia en cuestiones tecnológicas, una vez que se haya madurado la infraestructura de certificación del ITESM-CEM, el Instituto podría proyectarse como una Autoridad Certificadora comercial, que pudiese vender Certificados Digitales con un respaldo confiable a empresas y personas que lo requieran.

Aparte de ser una fuente de ingresos para el ITESM-CEM, al ser una Autoridad Certificadora a nivel nacional, se apoya a las organizaciones que no pueden contar con su propia infraestructura de certificación y el ITESM-CEM ganaría mayor presencia en la industria mexicana.

30. Caso Extensiones X.509 (Implementación de extensiones de Certificado)

Como ya lo hemos hecho notar a lo largo de este trabajo de tesis, la tecnología de Certificados Digitales no es muy popular aún. La impopularidad de esta tecnología se debe básicamente a la dificultad para su implantación, administración y operación. Para poder manejar este tipo de tecnologías se requiere de conocimientos en materia de criptografía, sistemas criptográficos de llave pública, Certificados Digitales, Autoridades Certificadoras y por supuesto, conocimientos de seguridad computacional y redes de computadoras.

Se podría pensar entonces que solamente personas con grandes habilidades técnicas pueden manejar sin problema estas tecnologías. Pues realmente esta inferencia no está lejos de la realidad. Es objetivo de esta tesis, el acercar este tipo de tecnologías a las personas y organizaciones.

Un Certificado Digital contiene la información de su dueño y de la Autoridad Certificadora que lo expidió. La información que del sujeto del Certificado se provee por lo general es: Nombre del usuario, dirección de correo electrónico, unidad organizacional, organización y país.

Las organizaciones y personas que manejan Certificados Digitales, por lo general lo hacen en su forma original, es decir, utilizan el Certificado Digital con sus campos y formato originales. De hecho resulta muy raro el recibir un Certificado Digital que contenga campos y formato distintos al original.

Pero la información original del Certificado puede resultar insuficiente para los requerimientos de una organización. Como lo vimos en la sección "Campos de un Certificado", los requerimientos del Departamento de Seguridad Computacional del ITESM-CEM son que el Certificado Digital incluya campos como: Rectoría, campus, dirección/división, departamento, función, datos personales, nivel de seguridad, etc.

Entonces resultaría deseable poder incorporar más campos al Certificado Digital, para poder adecuar su funcionalidad a los requerimientos de seguridad de una organización en particular.

A partir de la versión 3 de X.509, es posible hacer uso de las extensiones de certificado, mediante las cuales se pueden añadir campos extras al Certificado o fijar una política para el mismo. De hecho las extensiones son campos extras del Certificado Digital que se pueden interpretar al gusto de quien las implementa.

El implementar las extensiones X.509 para que sean incluidas en los Certificados que se expiden, debe consistir en la modificación o configuración del software de emisión de Certificados para que dichas extensiones sean incluidas en sus Certificados.

El implementar dichas extensiones en el Servidor de Certificados de Netscape, de tal manera que éstas sean incluidas en los Certificados expedidos, es una tarea difícil, pero la presentaremos de tal manera que quede al alcance de todos los administradores de sistemas de cómputo.

Desde el momento de la instalación, como se describe en el capítulo "El Servidor de Certificados Netscape", se debe indicar si se desean habilitar las extensiones X.509. También se pude elegir habilitarlas desde el Administrador de Servidores, bajo el rubro de configuraciones del sistema.

El Servidor de Certificados mantiene un registro de extensiones de Certificado que asocia los nombres de las extensiones con los identificadores de objeto y tipos de implementación. Cuando se inicia el Servidor de Certificados, éste llena el registro con una serie de extensiones predeterminadas y con cualquier extensión definida en el objeto CMSConfig del archivo obj.conf. Si se desea añadir extensiones propias, se deben especificar en dicho objeto. Para poder localizar el archivo obj.conf, se puede utilizar el programa de buscar archivos de Windows. La búsqueda deberá arrojar dos archivos llamados obj,conf, ambos deben modificarse.

30.1 Tipos de implementación

Los tipos de implementación definen el tipo de dato de la extensión, algunos de los tipos son:

- **AsnInteger**: Este tipo maneja valores enteros
- **AsnIA5String**: Este tipo maneja valores de cadena de caracteres
- **AsnOctetString**: Este tipo maneja valores de cadena de octetos

30.2 Añadir extensiones propias

Como ya lo pudimos ver, para el caso del ITESM-CEM, necesitamos añadir los campos de Rectoría, campus, dirección/división, departamento, función y nivel de seguridad, a los Certificados emitidos por la Autoridad Certificadora del ITESM-CEM. Para poder hacerlo, se debe añadir el siguiente código al objeto CMSConfig del archivo obj.conf por cada extensión deseada.

```
Service fn="cms-set-config" element="defineCertExtension"
  type="<tipo>" name="<nombre_de_extension>"  oid="<identificador_de_objeto>"
  critical="[si|no]" default="<valor_predeterminado>"
```

Donde:

<tipo> Es el tipo de implementación para la extensión, es decir, el tipo de la extensión. El tipo de la extensión puede ser AsnInteger, AsnIA5String o AsnOctectString.

<nombre_de_extension> Es el nombre de la extensión. Este nombre es desplegado cuando se verifican los detalles de un Certificado.

<identificador_de_objeto> Es el objeto identificador de la extensión. El identificador de objeto debe ser especificado en notación numérica separada por puntos (ejemplo, 2.16.840.1.113730.199). El identificador de objeto que se seleccione puede ser inventado, pero se recomienda que se sigan las reglas ISO para definir identificadores de objeto de tal manera que el nombre de la extensión y su identificador sean únicos.

Critical, especifica si la extensión es crítica al Certificado o no. En general se recomienda hacer las extensiones no críticas para que el Certificado sea aceptado por otras aplicaciones, ya que estas aplicaciones pueden no entender la extensión.

<valor_predeterminado> Es el valor predeterminado de la extensión.

En la ilustración, se muestra como se han añadido las extensiones de Rectoría, campus, división, departamento, función y nivel de seguridad al registro de extensiones.

```
<Object name="CMSConfig">
Service fn="cms-set-config" installStep="finish" signatureAlgorithm="1.2.840.113549.1.1.4"
adminCertSerial="3"
Service fn="cms-set-config" logfile="D:/Netscape/Server/cms-arqui15/logs/cms.log" minLogLevel="info"
Service fn="cms-set-config" user="" mode="normal" element="runMode"
Service fn="cms-set-config" maxCount="100" element="query"
Service fn="cms-set-config" allowMD5Signing="yes" keyfile="D:/Netscape/Server/cms-
arqui15/config/CASigningKey.db"
Service user="informix" fn="cms-set-config" server="ol_arqui15" db="cmsdb" env="D:/informix"
type="INFORMIX"
Service IssuerName="CN=Certificadora LCE, OU=cem.itesm.mx, O=ITESM-CEM, C=MX" fn="cms-set-
config"
Service fn="cms-set-config" element="certExtensions" enabled="yes"

Service fn="cms-set-config" element="defineCertExtension"
        type="AsnIA5String" name="Rectoria"

        oid="2.16.840.1.113730.1.94" critical="no" default="ZONA_SUR"
Service fn="cms-set-config" element="defineCertExtension"
        type="AsnIA5String" name="Campus"
        oid="2.16.840.1.113730.1.95" critical="no" default="CEM"

Service fn="cms-set-config" element="defineCertExtension"
        type="AsnIA5String" name="Division"
        oid="2.16.840.1.113730.1.96" critical="no" default="DI"

Service fn="cms-set-config" element="defineCertExtension"
        type="AsnIA5String" name="Departamento"
        oid="2.16.840.1.113730.1.97" critical="no" default="Seguridad"

Service fn="cms-set-config" element="defineCertExtension"
        type="AsnIA5String" name="Funcion"
        oid="2.16.840.1.113730.1.98" critical="no" default="Administrativo"

Service fn="cms-set-config" element="defineCertExtension"
        type="AsnIA5String" name="NivelSeguridad"
        oid="2.16.840.1.113730.1.99" critical="no" default="6"
</Object>
```

Figura 24: Adición de nuevas extensiones. (Se presenta el fragmento del archivo obj.conf a ser modificado.)

Las extensiones agregadas son del tipo cadena de caracteres y se les ha asignado un valor predeterminado. Éste será el valor que tomarán en caso de que no les sea cambiado a la hora de expedir el Certificado Digital.

Par finalizar el proceso, se debe acceder al Administrador de Servidores para configurar nuestro Servidor de Certificados. Se debe seleccionar "aplicar", para aplicar los cambios

hechos, posteriormente se debe elegir "cargar los archivos de configuración", ya que hemos modificado uno. En este punto no es necesario apagar y volver a encender el Servidor de Certificados.

30.3 Especificar extensiones en las formas de expedición de Certificado

Para asegurarse de que las extensiones propias definidas sean incluidas en los Certificados expedidos, éstas se deben incluir en la forma para emitir Certificados Digitales. Para hacer esta configuración, se debe editar la forma HTML para expedir Certificados.

Debido a que la forma para expedir Certificados se genera dinámicamente, acorde a los parámetros enviados en la solicitud de Certificado, el archivo a modificar para incluir las extensiones es un template de Java script. El nombre del archivo es processCSR.template.

Por ejemplo, supongamos que se requiere incluir la extensión "Campus" en los Certificados expedidos. Se debe añadir una entrada en la forma de expedición de Certificados para dicha extensión:

Para permitir que el operador especifique el valor de la extensión, se debe usar un tipo de entrada (como texto) que le permita especificar un valor:

```
<INPUT TYPE=TEXT NAME="Campus">
```

Si se desea que la extensión siempre tome su valor predeterminado, se puede usar una entrada oculta:

```
<INPUT TYPE=HIDDEN NAME="Campus">
```

```
if (result.header.certExtsEnabled == 'yes') {
   document.writeln('<h3> Extensions </h3>');
   document.writeln('<p>');
   document.writeln('<h4><a href="javascript:help(\'/docs/issue.htm#issueCertificateType\')" ' +
            'onMouseOver="return helpstatus(\'Click for help ' +
            'on certificate types \')" ' +
            'onMouseOut="return helpstatus(\'\')">',
            'Netscape Certificate Type (Usage)</a>',
            '</h4>');
document.writeln('Enable for the following usage:', '<br>');
  var clientcert = ""; var servercert = ""; var cacert = ""; var emailcert = "";
   If (result.header.csrCertType == 'client') { clientcert = "CHECKED";
   If ((result.header.subject.indexOf("E=") >= 0) || (result.header.subject.indexOf("MAIL=") >= 0)) {
            emailcert = "CHECKED"; }
   } else if (result.header.csrCertType == 'server') {servercert = "CHECKED";}
   else If (result.header.csrCertType == 'ca') {cacert = "CHECKED"; }
   document.writeln('<INPUT TYPE=CHECKBOX ' + clientcert + ' ' + servercert + ' NAME="certTypeSSLClient" VALUE="yes">', ' SSL
Client');
   document.writeln('<INPUT TYPE=CHECKBOX ' + servercert + ' NAME="certTypeSSLServer" VALUE="yes">', ' SSL Server');
   document.writeln('<INPUT TYPE=CHECKBOX ' + emailcert + ' NAME="certTypeEmail" VALUE="yes">',' Secure E-mail');
   document.writeln('<INPUT TYPE=CHECKBOX NAME="certTypeObjSigning" VALUE="yes">', ' Object Signing');
   document.writeln('<p>');
   if (result.header.csrCertType == "ca") {
      document.writeln('<INPUT TYPE=CHECKBOX CHECKED NAME="certTypeSSLCA" VALUE="yes">', ' Subordinate SSL CA');
      document.writeln('<br>');
      document.writeln('<INPUT TYPE=CHECKBOX CHECKED NAME="certTypeEmailCA" VALUE="yes">', ' Subordinate Email CA');
      document.writeln('<br>');
      document.writeln('<INPUT TYPE=CHECKBOX NAME="certTypeObjSigningCA" VALUE="yes">', ' Subordinate CA'); }
   document.writeln('<p>');
   document.writeln('<h4><a href="javascript:help(\'/docs/issue.htm#issueKeyIdentifiers\')" ' + 'onMouseOver="return
helpstatus(\'Click for help ' +
            'on key identifiers\')" ' + 'onMouseOut="return helpstatus(\'\')">', 'Key Identifiers', '</a></h4>');
   document.writeln('<INPUT TYPE=CHECKBOX CHECKED NAME="AuthorityKeyIdentifier" VALUE="">');
   document.writeln('Include Authority Key Identifier','<br>');
   document.writeln('<INPUT TYPE=CHECKBOX ' + cacert + ' NAME="SubjectKeyIdentifier" VALUE="">');
   document.writeln('Include Subject Key Identifier', '<br>');
   document.writeln('<p>');

   document.writeln('Rectoria: ZONA SUR', '<br>');
   document.writeln('<INPUT TYPE=HIDDEN NAME="Rectoria">');
   document.writeln('<p>');

   document.writeln('Campus: CEM', '<br>');
   document.writeln('<INPUT TYPE=HIDDEN NAME="Campus">');
   document.writeln('<p>');

   document.writeln('Direccion/Division', '<br>');
   document.writeln('<INPUT TYPE=TEXT NAME="Division">');
   document.writeln('<p>');

   document.writeln('Departamento', '<br>');
   document.writeln('<INPUT TYPE=TEXT NAME="Departamento">');
   document.writeln('<p>');

   document.writeln('Funcion (Profesor | Alumno | Administrativo | Directivo)', '<br>');
   document.writeln('<INPUT TYPE=TEXT NAME="Funcion">');
```

Figura 25: Adición de extensiones en la forma de emisión de Certificado (Modificación del archivo processCSR.template)

En la ilustración podemos ver cómo se especifican las nuevas extensiones para que sean incluidas en los Certificados a expedir, algunas de ellas serán usadas con su valor predeterminado (rectoría y campus), ya que estos campos no varían entre Certificado y Certificado. Otras extensiones pueden ser llenadas al momento de expedir el Certificado

Digital (dirección/división, departamento, función y nivel de seguridad), ya que se espera que dichas características varíen acorde al sujeto del Certificado.

Una vez que se hayan hecho estas modificaciones, se debe apagar y volver a prender el Servidor de Certificados. A partir de ahora, la forma para emitir Certificados incluirá las extensiones especificadas.

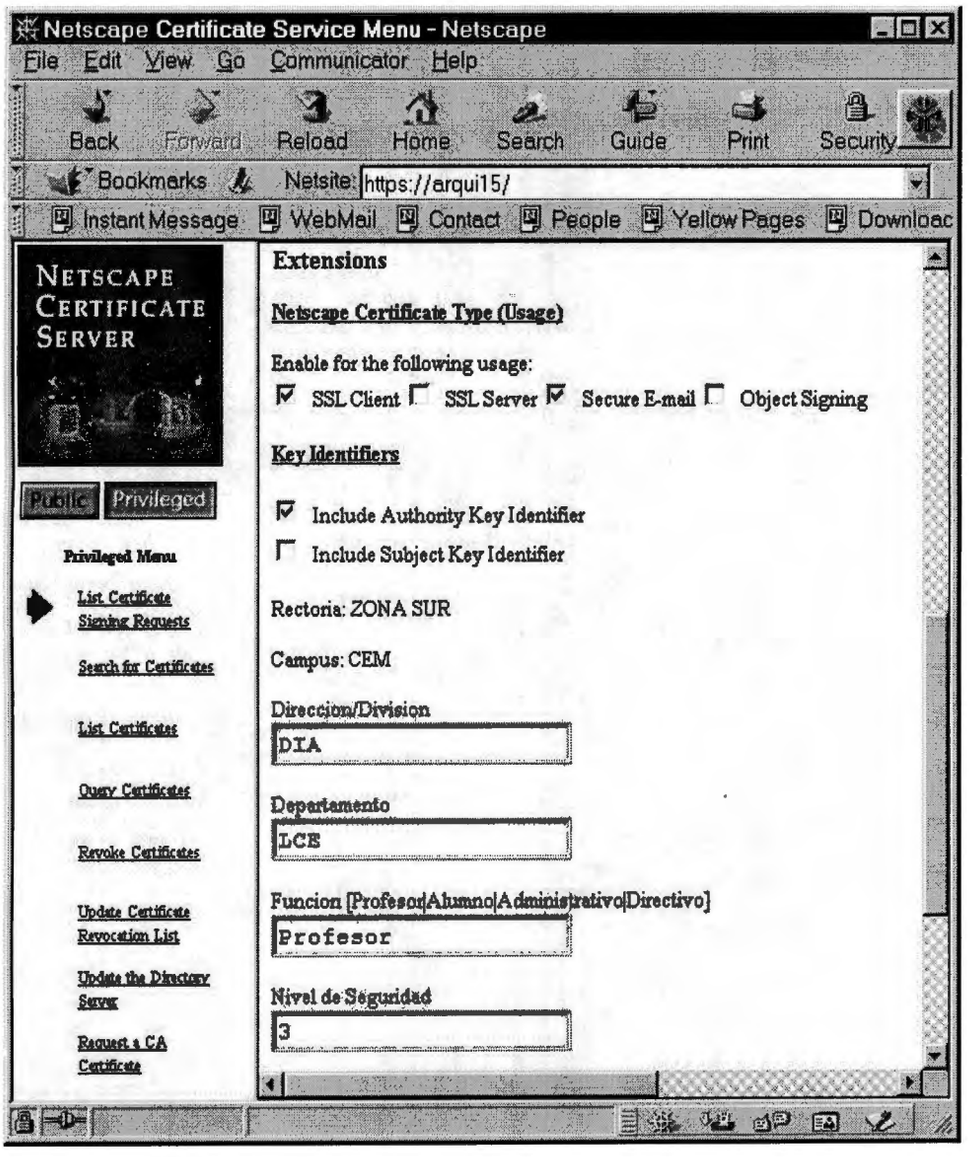

Figura 26: Forma de emisión de un Certificado con extensiones

Para poder especificar Políticas de Certificado (explicadas en el capítulo "Autoridad Certificadora"), se debe añadir una extensión de la misma manera como lo hemos hecho para aumentar un campo al Certificado Digital, sólo que ésta será interpretada como política por las aplicaciones que reciban el Certificado Digital.

En la figura 25 se muestra finalmente el Certificado Digital emitido incluyendo extensiones, estas extensiones representan los campos de Rectoría, campus, dirección/división, departamento, función y nivel de seguridad del Certificado Digital para uso dentro del ITESM-CEM.

30.4 Interpretación de las extensiones X.509

Como ya lo hemos estudiado, a los Certificados Digitales se les pueden añadir extensiones que funcionan como campos extras, en caso de que los campos estándar de un Certificado Digital no sean los suficientes o adecuados para una organización en particular. También las extensiones se pueden interpretar como Políticas de Certificado (ver capítulo "Autoridad Certificadora").

Es ahora responsabilidad de las aplicaciones que reciben el Certificado Digital reconocer e interpretar las extensiones. Es por ello que las aplicaciones que vayan a hacer uso de Certificados con extensiones, deben estar programadas para aceptarlas e interpretarlas de manera adecuada.

Un ejemplo es el uso del campo "nivel de seguridad" añadido a los Certificados Digitales para el ITESM-CEM. Una utilidad puede ser que un usuario se autentique en un servidor usando su Certificado Digital, el Servidor debe leer su nivel de seguridad y acorde a ello, otorgarle sus privilegios adecuados. Si es un nivel de seguridad alto, le serán otorgados privilegios de administrador, si por el contrario, el nivel de seguridad es bajo, se le otorgarán privilegios de usuario.

Pero toda esta tarea ya está fuera del alcance de la Autoridad Certificadora, es responsabilidad de los administradores de los sistemas, configurar las aplicaciones para que éstas puedan trabajar con los Certificados Digitales que incluyen extensiones.

```
The server issued the following certificate

  Certificate:
    Data:
      Version: v3 (0x2)
      Serial Number: 13 (0xd)
      Signature Algorithm: PKCS #1 MD5 With RSA Encryption
      Issuer: CN=Certificadora LCE, OU=cem.itesm.mx, O=ITESM-CEM, C=MX
      Validity:
        Not Before: Sat Nov 06 15:53:25 1999
        Not  After: Thu May 04 15:53:25 2000
      Subject: E=sperea@campus.cem.itesm.mx, CN=Sergio Perea, UID=sperea, OU=cem.itesm.mx, O=ITESM-
CEM, C=MX
      Subject Public Key Info:
        Algorithm: PKCS #1 RSA Encryption
        Public Key:
          Modulus:
            00:ae:59:de:c1:1d:19:b6:f1:e1:1b:a0:5c:47:a2:5b:dd:b5:
            e1:a7:3b:b5:97:43:be:89:99:4c:84:2b:17:dd:e0:a8:a4:10:
            5f:99:61:c3:d4:ea:08:de:72:7f:e9:7b:0e:7e:ad:fd:14:8f:
            80:0f:cc:bd:7c:2e:a3:ef:5f:52:45
          Public Exponent: 65537 (0x10001)
      Extensions:
        Identifier: Division
          Critical: no
          Value: DIA
        Identifier: Departamento
          Critical: no
          Value: LCE
        Identifier: Certificate Type
          Critical: no
          Certified Usage:
            SSL Client
            Secure E-mail
        Identifier: Funcion
          Critical: no
          Value: Profesor
        Identifier: NivelSeguridad
          Critical: no
          Value: 3
        Identifier: Authority Key Identifier
          Critical: no
          Key Identifier:
            a2:1b:da:15:80:56:8a:29:4d:dc:20:a8:55:79:e8:ad:a9:21:
            7f:2c
        Identifier: Rectoria
          Critical: no
          Value: ZONA_SUR
        Identifier: Campus
          Critical: no
          Value: CEM
    Signature:
      Algorithm: PKCS #1 MD5 With RSA Encryption
      Signature:
        b0:a3:17:b2:45:1a:05:c0:8c:a9:f4:e0:e0:be:4d:22:7e:bf:07:f4:e9:
        03:d3:f3:05:8e:7d:aa:ae:3b:26:74:e0:8f:db:8f:cf:fe:44:4d:07:1e:
```

Figura 27: Certificado Digital con extensiones

31. Aplicaciones futuras

Como ya lo hemos estudiado a lo largo de este trabajo de tesis, las aplicaciones de los Certificados Digitales son tan amplias como la imaginación de quien los maneja. Los Certificados son herramientas de seguridad versátiles que nos permiten explotar características cómo la privacidad, integridad y confidencialidad de la información, así como la autenticación.

Basados en estas características, se tienen planeadas algunas aplicaciones futuras de los Certificados Digitales dentro del ITESM-CEM, éstas incluyen:

- Manejo del correo electrónico seguro.
- Utilizar el Certificado Digital como medio de autenticación a los servicios de cómputo del ITESM-CEM.
- Incluir el Certificado Digital dentro de la Credencial Inteligente (portabilidad del Certificado Digital).
- Realizar la autenticación a los servicios de cómputo del campus, utilizando el Certificado Digital incluido en la Credencial Inteligente (se requiere de un lector).
- Utilizar el Certificado Digital como medio de autenticación y para establecer comunicaciones seguras en comercio electrónico para llevar a cabo tareas como: Pago de colegiatura, compras, interacción con clientes y proveedores, etc.
- Utilizar el Certificado Digital como medio de autenticación y para establecer una comunicación segura con los servidores del campus para tareas como: Inscripciones, reservado de equipo de cómputo, materias rediseñadas, etc.
- Incorporar el uso del Certificado Digital en la operación diaria del ITESM-CEM.

Estas son sólo algunas de las tareas en las que se puede utilizar el Certificado Digital, pero no hay que perder de vista que las aplicaciones de los Certificados son muy extensas.

Capítulo 7

TRABAJO PRÁCTICO,

Implantación de una Autoridad Certificadora y manejo de Certificados Digitales en el Departamento de Ciencias Computacionales de ITESM-CEM.

1. Presentación del Trabajo Práctico

A manera de laboratorio, y con la finalidad de obtener gran parte de los resultados expresados en este trabajo de tesis, se implementó una Autoridad Certificadora para el Departamento de Ciencias Computacionales del ITESM-CEM. El contar con esta Autoridad Certificadora nos permitió implementar el manejo de Certificados Digitales dentro del Departamento de Ciencias Computacionales.

Se comenzó levantando una Autoridad Certificadora apoyándose de la plataforma de software del Servidor de Certificados de Netscape. Además se organizó una sesión de capacitación en materia de Certificados Digitales para todos los miembros del departamento, para posteriormente trabajar bajo la infraestructura de certificación montada.

2. Planeación

Con la finalidad de apoyar los trabajos de tesis sobre Certificados Digitales y Autoridades Certificadoras, se decidió emprender un trabajo práctico para poder obtener de la experiencia, resultados a expresarse en este trabajo de tesis.

Se decidió montar una infraestructura de Certificación de manera independiente dentro del Departamento de Ciencias Computacionales del ITESM-CEM. Para poder montar dicha infraestructura de Certificación, se decidió utilizar la plataforma de software del Servidor de Certificados de Netscape.

Se escogió dicha plataforma de software debido al uso tan amplio que tienen los nevagadores Netscape dentro del ITESM-CEM. Su uso es tan amplio, que son la plataforma estándar de navegación y correo electrónico.

El Servidor de Certificados se montó en un Servidor de las siguientes características:

- HP LH-Pro NetServer
- Dos Procesadores Pentuim Pro
- 128 MB de memoria RAM
- 13 GB de Disco Duro
- Plataforma operativa Servidor Windows NT

Dicho Servidor se ubica dentro de las instalaciones del Laboratorio de Cómputo Especializado de Arquitectura del ITESM-CEM. Este laboratorio cuenta con una LAN a 100 mbps, la cual se encuentra conectada al backbone de fibra óptica del campus.

La instalación del Servidor de Certificados de Netscape se llevó a cabo acorde al procedimiento descrito el capítulo "El Servidor de Certificados Netscape". Posteriormente se procedió a la revisión del correcto funcionamiento y configuración del Servidor de Certificados de Netscape, procedimientos también descritos en el capítulo "El Servidor de Certificados Netscape".

3. Estudio del Servidor de Certificados de Netscape

Para la instalación de la infraestructura de software de la Autoridad Certificadora del Departamento de Ciencias Computacionales, se obtuvo una versión de prueba del Servidor de Certificados de Netscape versión 1.01. Posterior a su instalación, se inició la fase de estudio de funcionamiento del Servidor de Certificados de Netscape. El resultado de esa fase de instalación y exploración del Servidor de Certificados de Netscape es lo expresado en el capítulo "El Servidor de Certificados Netscape", que trata acerca de la instalación, configuración, administración y operación de una infraestructura de certificación utilizando el Servidor de Certificados de Netscape.

Una de las fases más relevante del estudio del Servidor de Certificados de Netscape, es la de expedición de Certificados Digitales. Se hizo el estudio de las funciones que el software presentaba para el trámite, emisión, instalación y uso de un Certificado Digital, para su presentación a los usuarios de la Autoridad Certificadora. Para tal fin se expidieron Certificados de prueba, se instalaron y se hizo uso de sus propiedades como firma digital y encripción de mensajes.

Otra fase muy importante del estudio del Servidor de Certificados Netscape, fue el incorporar un mayor número de campos al Certificado Digital. Esto permitiría darle una mayor funcionalidad a los Certificados Digitales expedidos y poder adecuarlos a necesidades específicas. Para llevar a cabo esta tarea, se echó mano de las extensiones X.509, las cuales representan importantes dificultades para poder implementarse.

4. Preparación de una Página Informativa

Debido a la novedad del proceso, se instaló una página web (http://nivada.cem.itesm.mx/sperea) informativa para los usuarios de la Autoridad Certificadora del Departamento de Ciencias Computacionales. La página contiene la siguiente información:

- Introducción a los Certificados Digitales
- Cómo solicitar un Certificado Digital
- Cómo instalar un Certificado Digital
- Cómo aceptar la Autoridad Certificadora
- Cómo firmar un mensaje
- Cómo encriptar un mensaje
- Cómo leer un mensaje encriptado
- Cómo llevar a cabo el intercambio de llaves
- Cómo configurar el sistema de contraseñas

La finalidad de esta página era la de proveer de la información necesaria al usuario para poder tramitar y utilizar su Certificado Digital.

5. Capacitación

Una vez montada la infraestructura de software y hecha la página informativa, se llevó a cabo una sesión de capacitación para los usuarios del Departamento de Ciencias Computacionales. En la sesión de se expusieron los siguientes temas:

- Sistemas criptográficos asimétricos
- Teoría de Certificados Digitales
- Manejo de Certificados Digitales usando el Servidor de Certificados de Netscape

En la sesión de Capacitación arrancó de manera oficial el laboratorio de implementar una infraestructura de certificación para el Departamento de Ciencias Computacionales.

6. Desarrollo del Proceso de Certificación

En total, se recibieron doce solicitudes de Certificado Digital, las cuales fueron procesadas y cuyo Certificado fue expedido con éxito. Las instrucciones de trámite, instalación y uso del Certificado Digital presentadas en la página de instrucciones

ayudaron a que el proceso se desarrollara sin dificultades, aunado a la formación informática de los miembros de este grupo.

El proceso para expedir el Certificado fue el siguiente:

- Recibir solicitud de Certificado Digital
- Expedir el Certificado Digital
- Enviar Certificado por correo electrónico

La instalación y uso del Certificado Digital quedaron en completa responsabilidad del usuario.

7. Cadenas de Autoridades Certificadoras

Como una parte importante del trabajo práctico, se implementó una cadena de Autoridades Certificadoras. Se tomó como Autoridad Certificadora raíz a la Autoridad Certificadora montada por la Dirección de Informática del ITESM-CEM (CERTCEM) y se tomo como Autoridad Certificadora hija a la Autoridad Certificadora de Ciencias Computacionales (CERTIFICADORA LCE, https://arqui15.cem.itesm.mx).

El procedimiento seguido para establecer la cadena de Certificación es el descrito en el capítulo "Servidor de Certificados Netscape", sección "Solicitud e instalación de un Certificado de Autoridad Certificadora".

El experimento dio resultados positivos, se logró que los Certificados Digitales de ambas fueran compatibles. Esto trajo dificultades técnicas ya que la cadena de Certificación se estableció después de que los Certificados correspondientes al Departamento de Ciencias Computacionales fueran expedidos, por lo que éstos no portaban la nueva cadena de certificación. Es por ello que se tuvieron que volver a expedir los Certificados para el departamento de Ciencias Computacionales.

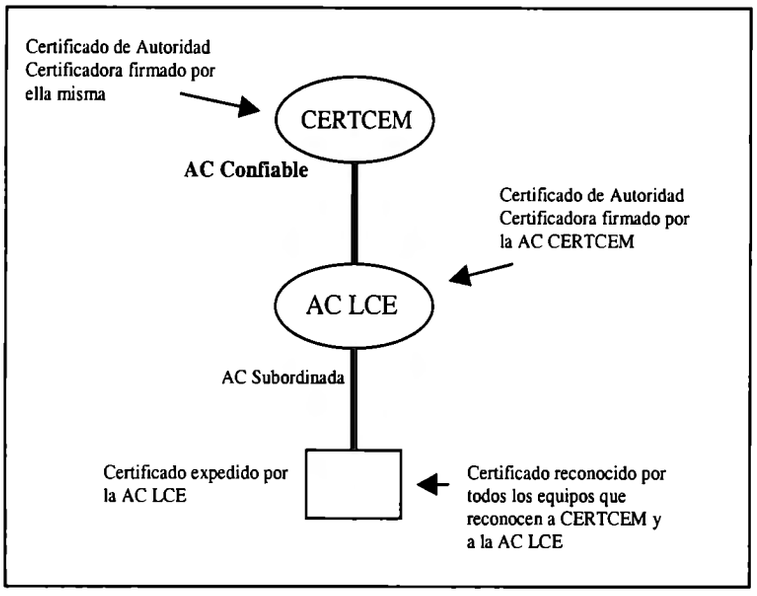

Figura 28: Cadena de certificación Trabajo práctico

8. Resultados Obtenidos del Trabajo Práctico

El trabajo práctico resultó fundamental para este trabajo de tesis, ya que gracias a él se pudieron obtener las bases para poder establecer el cómo montar, administrar y operar una Autoridad Certificadora, además de poder obtener el conocimiento para poder sugerir un esquema de certificación para toda la comunidad del ITESM-CEM.

Como ya lo estudiamos en capítulos anteriores, los Procesos de Certificación de una Autoridad Certificadora no están establecidos, en realidad dependen de cada Autoridad Certificadora. En base este trabajo práctico, se pudieron deducir los Procesos de Certificación expresados en esta tesis, y que se espera sirvan de guía para que las organizaciones mexicanas puedan implantar su propia infraestructura de Certificación.

RESULTADOS OBTENIDOS

Esta sección tiene por objetivo expresar las aportaciones que ha arrojado este trabajo de tesis.

Debido a la gran dificultad y a los conocimientos requeridos para poder implementar una Autoridad Certificadora, y en general una Infraestructura de Certificación, estas tecnologías se están desarrollando de manera muy lenta en México. Este trabajo acerca estas tecnologías a las personas y organizaciones para que puedan implementar su propia Infraestructura de Certificación, ya sea de manera independiente o dentro de una organización. En base a un trabajo práctico y a un caso real, se establecen los Procesos de Certificación de una Autoridad Certificadora.

Acorde a la definición del capítulo "Autoridad Certificadora", los Procesos de Certificación son el conjunto de funciones, políticas, tareas específicas,

procedimientos, etc. que gobiernan a una Autoridad Certificadora, son el alma de ésta. Estos procesos quedan fuera del alcance del estándar X.509 y no están definidos y no se sabe cuáles son éstos.

Con base en lo anterior, en este trabajo definimos las funciones de una Autoridad Certificadora, recursos necesarios, su organización jerárquica, la solicitud de un Certificado Digital, condiciones de aceptación o rechazo de una solicitud, la comprobación de la identidad de un solicitante, la expedición de Certificados, campos y formato de un Certificado Digital, métodos de entrega del Certificado, protección de la llave privada, intercambio de llaves públicas, condiciones y el proceso de revocación del Certificado Digital, definición del tiempo de vida de un Certificado Digital, uso de Certificados Digitales, renovación de un Certificado Digital, políticas del Certificado, responsabilidades de una Autoridad Certificadora, aplicación de la infraestructura de Certificación en una organización, administración de una Autoridad Certificadora, terminación de una Autoridad Certificadora, entre muchos otros puntos importantes. También se establecen las relaciones entre Autoridades Certificadoras y las Cadenas de Autoridades Certificadoras. Todas estas definiciones sirven de guía para la implantación de una infraestructura de Certificación.

Como ya lo hemos estudiado, el implantar una Autoridad Certificadora y su entorno, representa grandes dificultades, así mismo, las herramientas de software que apoyan dicha tarea. Es por ello que en este trabajo de tesis se presenta una herramienta de software como opción para montar sobre ella, una Infraestructura de Certificación. Esta herramienta es el Servidor de Certificados de Netscape, el cual es descrito paso a paso para su instalación, operación y administración. La presentación que del Servidor de Certificados se hace, esta diseñada para quedar al alcance de la mayoría de los administradores de sistemas. La implantación de una Infraestructura de Certificación se puede llevar a cabo utilizando el Servidor de Certificados de Netscape como plataforma operativa de software, más los Procesos de Certificación definidos anteriormente.

Como una de las aportaciones mas destacadas de este trabajo de tesis, tenemos la recomendación para la Certificación de la comunidad del ITESM-CEM,

administración y manejo de certificados a gran escala. Este trabajo de tesis aporta la definición de los Procesos de Certificación de la Autoridad Certificadora del ITESM-CEM. Algunos puntos destacados obtenidos son:

- Definición de la Organización jerárquica de la Autoridad Certificadora del ITESM-CEM.
- Se presentaron dos métodos de expedición de Certificados y se hizo un estudio comparativo entre los dos.
- Se obtuvo el método ideal para certificar a toda la comunidad del ITESM-CEM, presentando sus demandas en tiempos y recursos.
- Se presentaron los tiempos y recursos necesarios para llevar a cabo la certificación del ITESM-CEM.
- Se definieron las funciones y tareas de la Autoridad Certificadora del ITESM-CEM.
- Se definieron los campos que debe tener un Certificado Digital del ITESM-CEM, acorde a las necesidades del Departamento de Seguridad Computacional de la dirección de Informática.
- Se definió el proceso de entrega e instalación del Certificado Digital, presentando su estudio de demanda en tiempo y recursos.
- Se definieron procesos como: Solicitud de un Certificado Digital, comprobación de la identidad de un solicitante, condiciones y el proceso de rechazo de una solicitud de Certificado Digital, aceptación de la Autoridad Certificadora del ITESM-CEM, intercambio de llaves, condiciones y el proceso de revocación de un Certificado Digital, definición del tiempo de vida de un Certificado Digital para evitar una renovación masiva, entre mucho otros puntos importantes.
- Se definieron las responsabilidades de los usuarios, en cuanto a su Certificado Digital.
- Se planteó el uso que se le puede dar al Certificado Digital.
- Se presentó un caso real de cómo formar Cadenas de Autoridades Certificadoras, utilizando el Servidor de Certificados de Netscape.
- Además se planteó la proyección y aplicaciones futuras de la tecnología de Certificados Digitales dentro del ITESM-CEM.

- Este caso puede ser visto como una opción para la certificación a gran escala para las organizaciones grandes.

Otra importante aportación de esta tesis, es el "Caso extensiones X.509", donde se trata la implantación de las extensiones X.509 en los Certificados expedidos. Por lo general un Certificado Digital es utilizado en su formato y con sus campos originales, de hecho es muy raro recibir un Certificado con campos distintos a los originales. Como una opción para las organizaciones que deseen implantar mayor número de campos a un Certificado Digital o añadirle una política, se presenta de manera detallada cómo hacerlo utilizando el Servidor de Certificados de Netscape.

Como otra aportación de este trabajo de tesis, tenemos las recomendaciones de mejora que se hacen sobre el Servidor de Certificados Netscape.

Por último contamos con la presentación de capacitación a usuarios que se utilizo en el Departamento de Ciencias Computacionales del ITESM-CEM, la cual puede ser muy útil para la capacitación dentro de una organización. Dicha presentación se encuentra en http://nivada.cem.itesm.mx/sperea.

CONCLUSIONES

Como lo hemos podido estudiar a lo largo de este trabajo de tesis, el manejo de la Infraestructura de Certificados Digitales y su respectiva Autoridad Certificadora, es una solución en materia de seguridad computacional para las organizaciones en general. Este mecanismo aporta las características de autenticación, integridad y confidencialidad a nuestras redes.

La autenticación efectiva se da desde la perspectiva de que uno puede estar seguro que un mensaje en efecto proviene de la entidad que aparece como remitente. Además se añade la característica de integridad, ya que podemos descubrir si el mensaje fue alterado en su trayecto por la red. Y podemos hablar de confidencialidad, ya que podemos utilizar las bases de criptografía de llave pública para mandar y recibir mensajes encriptados.

El contar con estas características de seguridad en nuestra red nos permite realizar operaciones delicadas con mayor confianza. Tales operaciones incluyen las comunicaciones entre nuestras aplicaciones, comunicación entre servidores, el envío de información confidencial, transacciones que involucran dinero, la comunicación cotidiana entre usuarios, etc.

Pero el montar una infraestructura con tales características, tradicionalmente ha resultado ser una labor demasiado compleja. Este ha sido uno de los factores que han frenado el éxito de esta tecnología. Es por ello que como una aportación de este trabajo de tesis, se ofrece una guía completa para poder montar una infraestructura de Certificación. En este trabajo se plantea todo lo necesario para llevar a cabo esta tarea, desde la teoría que soporta a los conceptos generales, hasta las instrucciones detalladas de cómo montar, administrar y operar una Autoridad Certificadora y la implantación y operación con Certificados Digitales.

También son presentadas recomendaciones, que por la naturaleza del estándar X.509 quedan fuera de su alcance, tal es el caso de los Procesos de Certificación de una Autoridad Certificadora. En este trabajo de tesis se establecen Procesos de Certificación comunes, que pueden estandarizarse para las organizaciones mexicanas, los cuales pueden ser adoptados e implantados de manera transparente.

Además de presentar la teoría de cómo montar, operar y administrar una Infraestructura de Certificación, se presenta una herramienta de software que nos permite aplicar los conceptos teóricos planteados. Dicha herramienta es el Servidor de Certificados de Netscape, que es presentado en este trabajo como una opción para ser la base operacional de software de una Infraestructura de Certificación. Debido a la complejidad que representa el construir una Infraestructura de Certificación sobre el Servidor de Certificados de Netscape, se presenta una descripción a detalle y de manera simple de cómo instalarlo y administrarlo. Así como las recomendaciones para operar con Certificados Digitales bajo plataformas Netscape.

Otra aportación de este trabajo de tesis, es la recomendación para la Certificación de toda la comunidad del ITESM-CEM. Se ha desarrollado toda la logística y se han documentado los Procesos de Certificación que debe guardar la Autoridad

Certificadora del ITESM-CEM. Así mismo se presenta la recomendación para la administración y operación de su Autoridad Certificadora y el manejo de Certificados Digitales a gran escala (arriba de diez mil).

Debido a que el contar con una infraestructura de Certificación requiere de avanzados conocimientos técnicos en materia informática, además de resultar ser una tarea complicada, al contar con esta guía, las organizaciones mexicanas pueden adoptarla para implementar su propia Infraestructura de Certificación. Logrando también de esta manera, ahorrar costosas consultorías en la materia. Además de cubrir necesidades de seguridad, inherentes para el trabajo en red de hoy en día.

La gran mayoría de lo establecido en este trabajo de tesis, está soportado en un trabajo práctico realizado en el departamento de Ciencias Computacionales del ITESM-CEM, donde se implantó una Infraestructura de Certificación, que actualmente usan los profesores y apoyos académicos para sus comunicaciones internas.

Referencias y Bibliografía

[1] TÉLLEZ VALDES, JULIO, *Derecho Informático*. Serie Jurídico. McGraw-Hill, 1995.

[2] SARZANA, CARLOS, Criminalitá e Tecnología, Computer Crimes, Resegna Penitenziaria e Criminología., Roma Italia, 1979, Vol. 1, No. 1-2.

[3] ITU-T X.509, en http://www.itu.int; Es el estándar X.509.

[4] FREIER, ALAN O., *et al.* The SSL Protocol, Version 3.0. Internet Draft, Marzo 1996, p 1-26.

[5] RFC 2312, en http://www.imc.org/rfc2312; Especificación de S/MIME.

[6] PKCS-1, Laboratorios RSA, en http://www.rsa.com; Especificación del algoritmo RSA.

[7] STALLINGS, WILLIAM, *Network and Internetwork Security Principles and Practice*, Prentice Hall, New Jersey USA, 1995, p 268-276

[8] STALLINGS, WILLIAM, *Network and Internetwork Security Principles and Practice*, Prentice Hall, New Jersey USA, 1995, p 276-282

[9] ITU-T X.208, en http://www.itu.int; Especificación de ASN.1 (Abstract Syntax Notation One)

[10] ITU-T X.209, en http://www.itu.int; Especificación DER (Distinguished Encoding Rules)

[11] ITU-T X.520, en http://www.itu.int; Especificación de Nombres Distinguidos.

[12] *Netscape Certificate Server 1.0 evaluation guide*, Netscape communications corporation, 1998

Anexo A

El protocolo de Comunicaciones Seguras SSL

El protocolo SSL y los Certificados Digitales están íntimamente ligados, esto es debido a que actualmente SSL es el protocolo de seguridad más utilizado, que incorpora el uso de Certificados Digitales. Si bien es cierto que la aplicación más popularmente usada que implementa el uso de Certificados Digitales es SSL, no es la única. Cada programador tiene la libertad de hacer su propio protocolo y usar Certificados Digitales en él, o implementar el uso de Certificados Digitales en sus aplicaciones.

Debido al estrecho lazo que existe entre los Certificados Digitales y SSL, no podemos dejar de presentar este protocolo en este trabajo. La presentación que de SSL se hace en este anexo es con la finalidad de conocer el protocolo de manera general, el sólo estudio de este protocolo requeriría trabajos posteriores.

1. SSL (Secure Sockets Layer)

Al transmitir información a través de la red, un punto fundamental de interés en seguridad es la privacidad de la información y la confiabilidad de la misma. Es decir, nos interesa que la información que mandamos por la red no pueda ser vista por nadie más (o en su defecto, que ésta sea ininteligible para quien llegue a verla), ya que por lo general dicha información es privada. Además debemos estar seguros de que la información es confiable, en el aspecto de que ésta no haya sido alterada en su viaje por la red.

SSL es un protocolo de seguridad que provee privacidad en comunicaciones sobre Internet. La meta principal de SSL es la de proveer privacidad y confiabilidad entre dos aplicaciones comunicantes. SSL se compone de dos capas, una de bajo nivel llamada "SSL Record Protocol", que va situada arriba de algún protocolo de transporte confiable como lo puede ser TCP, y es usada para encapsular varios protocolos de más alto nivel. Uno de esos protocolos es el "SSL Handshake Protocol" el cual permite al cliente y al servidor autenticarse mutuamente y negociar un algoritmo de encriptación y una llave criptográfica, antes de que el protocolo de la aplicación transmita su primer byte de datos. SSL es un protocolo independiente de la aplicación.

Las tres propiedades básicas de SSL son:

- La conexión es privada: La encripción es usada después de un handshake inicial para definir una llave secreta, se utiliza criptografía simétrica (DES, RC4, etc.)

- Las identidades de los entes comunicantes pueden ser autenticadas mediante criptografía asimétrica, o de llave pública (RSA, Certificados Digitales, etc.)

- La conexión es confiable: El transporte del mensaje incluye el chequeo de su integridad (SHA, MD5, etc.). En otras palabras, nos sirve para verificar que el mensaje recibido es exactamente el mismo que se ha enviado.

Las metas de SSL son:

1. Seguridad Criptográfica: Establecer una conexión segura entre dos partes

2. Interoperabilidad: Programadores independientes pueden desarrollar aplicaciones que usen SSL, las cuales deben ser capaces de intercambiar parámetros criptográficos sin la necesidad de conocer el código de la otra parte.

3. Extensibilidad: SSL permite que nuevos métodos de encripción puedan ser incorporados cuando se requiera, con esto se consigue prevenir la necesidad de crear un nuevo protocolo y con ello la incorporación de posibles nuevas debilidades y también evitar la necesidad de implementar una nueva librería de seguridad.

4. Eficiencia relativa: Debido a que las operaciones de criptografía suelen ser muy demandantes en CPU, particularmente las de llave pública, SSL incorpora un esquema opcional de cache de sesión para reducir el numero de conexiones que se necesitan para establecer la sesión. Además SSL hace especial énfasis en reducir la actividad sobre la red.

SSL es un protocolo por capas. En cada capa los mensajes deben incluir campos de longitud, descripción y contenido. SSL toma los mensajes a ser transmitidos, fragmenta los datos en bloques manejables, opcionalmente comprime los datos, aplica los mecanismos para el chequeo de la integridad del mensaje, encripta y transmite los resultados. Los datos recibidos son desencriptados, verificados, descomprimidos y ensamblados para ser entregados a los clientes de niveles más altos.

2. Estados de Sesión y Conexión

SSL es un protocolo cuyo comportamiento depende del estado en el que se encuentre. Es responsabilidad del protocolo de Handshake de SSL, el coordinar los estados entre el cliente y el servidor.

Los estados de sesión en los que se puede encontrar el protocolo incluyen los siguientes elementos:

- Identificador de sesión: Una secuencia de bytes arbitraria escogida por el servidor para identificar una sesión recuperable o activa.
- Certificado Digital: El Certificado Digital X.509 de las entidades comunicantes. Este elemento puede ser nulo.
- Método de Compresión: El algoritmo usado para comprimir los datos antes de la encripción.
- Especificaciones de Cifrado: Especifica el algoritmo simétrico de encripción (ninguno, DES, etc.), así como el algoritmo MAC (MD5 o SHA).
- Llave Maestra: Secreto compartido de 48 bytes entre el cliente y el servidor.
- Es recuperable: Una bandera que indica si una sesión puede ser usada para iniciar nuevas conexiones.

Los estados de conexión incluyen los siguientes elementos:

- Secuencias aleatorias de cliente y servidor: Son secuencias de bytes escogidas por el cliente y el servidor para cada conexión.
- Llave de escritura MAC del servidor: El secreto usado en operaciones MAC sobre datos escritos por el servidor.
- Llave de escritura MAC del cliente: El secreto usado en operaciones MAC sobre datos escritos por el cliente.
- Llave de escritura del servidor: La llave de cifrado para el algoritmo simétrico utilizado para encriptar datos por el servidor y desencriptarlos por el cliente.
- Llave de escritura del cliente: La llave de cifrado para el algoritmo simétrico para encriptar datos por el cliente y desencriptarlos por el servidor.

- Números de secuencia: Cada parte mantiene secuencias separadas de mensajes recibidos y transmitidos para cada conexión.

3. SSL Record Layer

La capa SSL *Record Layer* recibe datos de capas superiores en bloques no vacíos de tamaño variable. Esta capa fragmenta la información en registros SSL de texto plano con un tamaño máximo de 2^{14} bytes. Todos los registros son comprimidos usando el algoritmo pactado, por lo general existe un algoritmo de compresión activo. El algoritmo de compresión transforma a la estructura SSL de texto plano en una estructura SSL comprimida.

Una vez que el *handshake* se ha completado, las dos partes han compartido llaves secretas, las cuales son usadas para encriptar los registros y computar los códigos de autenticación de Mensaje (MACs). Las técnicas utilizadas para realizar la encripción y las operaciones MAC se encuentran definidas en las especificaciones de cifrado (*cambio_spec_cifrado*). Las operaciones de MAC y encripción, transforman una estructura SSL comprimida en una estructura SSL de texto cifrado. Las funciones de desencripción realizan la operación inversa. Las transmisiones también incluyen un número de secuencia de tal manera que mensajes perdidos, alterados o extras, son detectados.

4. El protocolo de Cambio de Especificaciones de Cifrado

El mensaje de cambio de especificaciones de cifrado (*cambio_spec_cifrado)* es enviado tanto por el cliente como por el servidor para notificarle a la otra parte que los registros subsecuentes serán protegidos bajo las recientemente negociadas especificaciones de cifrado y llaves.

5. SSL Handshake protocol

Este protocolo es usado para negociar los atributos de seguridad de una sesión. Provee sus mensajes a la SSL Record Layer donde éstos son encapsulados dentro de una o más estructuras SSL de texto plano, las cuales son procesadas y transmitidas.

Los parámetros criptográficos para la sesión son producidos por este protocolo. Cuando un cliente y un servidor SSL comienzan a comunicarse acuerdan una versión del protocolo, seleccionan los algoritmos criptográficos, opcionalmente se autentican mutuamente, y utilizan técnicas de llave pública para generar llaves secretas compartidas. El protocolo de *handshake* se lleva a cabo de la siguiente manera:

El cliente manda un mensaje de ***hola_cliente***, al cual el servidor debe responder con un mensaje de ***hola_servidor***. Los mensajes de ***hola cliente*** y ***servidor*** establecen los siguientes atributos: versión del protocolo, identificador de la sesión, especificación de cifrado y método de compresión. Adicionalmente dos valores aleatorios son generados e intercambiados, uno para el cliente y otro para el servidor.

Después de los mensajes de ***hola***, el servidor mandará su Certificado Digital si es que éste va a ser autenticado. Adicionalmente un mensaje de intercambio de llave (***intercambio_llave_servidor***) debe ser enviado por el servidor (sólo si él no tiene certificado). Si el servidor es autenticado, éste debe pedir su certificado al cliente.

Ahora el servidor mandará un mensaje de ***hola_servidor_hecho***, indicando que la fase de mensajes ***hola*** ha terminado. El servidor ahora espera por una respuesta del cliente.

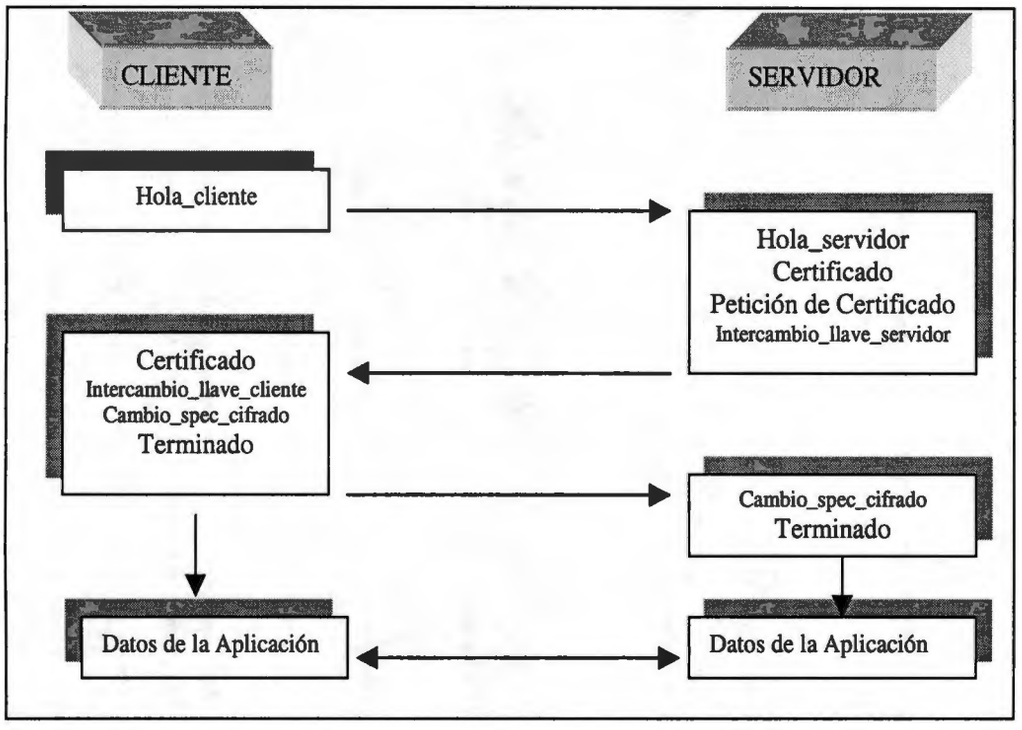

Figura A29: SSL Handshake Protocol

Si el servidor mandó una solicitud de Certificado Digital, el cliente debe mandarlo o mandar una alerta en caso de no poseer alguno. En este punto se manda el mensaje de *intercambio_llave_cliente* y el contenido de ese mensaje dependerá del algoritmo de llave pública negociado en la fase previa.

En este punto un mensaje de *cambio_spec_cifrado* (cambio de especificaciones de cifrado) es mandado por el cliente, inmediatamente después el cliente manda el mensaje de *terminado* bajo los nuevos algoritmos, llaves y secretos. En respuesta el servidor va a mandar su propio mensaje de *cambio_spec_cifrado* y también manda su mensaje de *terminado* bajo las nuevas especificaciones de cifrado. En este momento el *handshake* está completo y el cliente y el servidor pueden comenzar a intercambiar datos de la aplicación.

Cuando el cliente y el servido deciden reanudar una sesión previa o duplicar una sesión existente (en lugar de negociar nuevos parámetros de seguridad) los mensajes fluyen como se indica a continuación:

El cliente manda un ***hola_cliente*** utilizando el identificador de la sesión a ser reanudada. Entonces el servidor consulta el número de sesión en cache. Si la encuentra, entonces el servidor manda un mensaje de ***hola_servidor*** con el mismo valor de identificador de sesión. En este punto ambos deben mandar el mensaje de ***cambio_spec_cifrado*** para establecer los nuevos parámetros de seguridad y proceden de inmediato a ***terminado***, es aquí donde se comienzan a intercambiar datos de la aplicación.

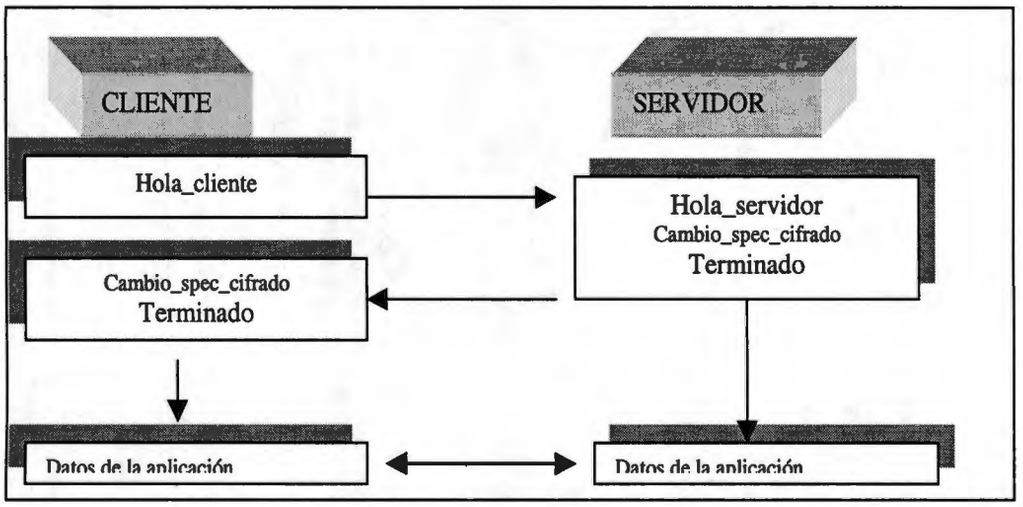

Figura A30: Reanudación de una sesión SSL previa

Si el número de sesión no es encontrado en cache, el servidor genera un nuevo identificador de sesión y se vuelve a llevar a cabo todo el protocolo.