Universidad del Azuay

Facultad de Administración

Escuela de Ingeniería de Sistemas

Seguridades en Comercio Electrónico

Trabajo de graduación previo a la obtención del título de Ingeniera en Sistemas

Autor: Daniela Molina

Director: Ing. Luis Calderón

Cuenca, Ecuador
2007

DEDICATORIA

Dedico la culminación de esta monografía a mi familia, por el amor, comprensión y apoyo que siempre me han brindado, a mis amigos, por darme la fuerza, confianza y valor necesarios para poder alcanzar esta gran meta.

AGRADECIMIENTOS

Quiero agradecer a Dios por haber puesto en mi camino a todas las personas que me han sabido guiar y hacer de mí lo que soy, a mis padres por su dedicación y amor, mis hermanos por ser mi apoyo y fuerza incondicionales, mis padrinos por estar siempre conmigo alentando mis pasos, mis tíos y primos por sus muestras de cariño, mis compañeros de trabajo por darme el tiempo necesario para cumplir con esta meta.

También quiero agradecer de una manera muy especial a mis profesores por su dedicación en las clases, por compartir su conocimiento conmigo y a muchos de ellos por llegar a ser un ejemplo a seguir.

Para finalizar quiero dar gracias a mis amigos, a todos y cada uno de ellos, por ser parte fundamental de mi vida y por estar conmigo cada instante de ella.

INDICE DE CONTENIDOS

INDICE DE ILUSTRACIONES Y CUADROS

RESUMEN

Hoy en día, las empresas se han visto en la necesidad de incursionar en el comercio electrónico para aprovechar las ventajas que este ofrece. Dentro de este contexto existe un sin numero de pros y contras especialmente en lo que se refiere a la seguridad en las transacciones que se realizan dentro del mismo, es por esto que en esta monografía he investigado el funcionamiento del protocolo SSL y los certificados digitales para incrementar la confianza de las transacciones electrónicas. Como una demostración práctica de lo investigado, se escribió una aplicación que simule el funcionamiento de un Web Banking utilizando como herramientas el servidor Web Apache y la base de datos MySQL.

ABSTRACT

Nowadays, companies have seen the need to approach e-commerce to benefit from the advantages that it offers. Within this context, there is a great number of pros and cons, especially regarding security in the transactions that are made through it. For this reason, this research work has investigated the functioning of the SSL protocol and the digital certificates to increase user's confidence on electronic transactions. As a practical demonstration of what has been researched, an application simulating Web Banking functioning was created, using the Apache Web Server and the database MySQL as tools.

INTRODUCCIÓN

Hoy en día todos dependemos de la información que generamos y mantenemos en nuestras computadoras y de una conexión física para comunicarnos, el avance que se ha tenido con las redes nos ha permitido solucionar problemas y hacer provecho de sistemas que nos ayudan a manipular la información. Empresas, organizaciones y cualquier persona que utiliza una computadora envía y recibe correos electrónicos, comparte información de manera local o a nivel mundial, realiza transacciones, ofrece servicios y encuentra soluciones a sus requerimientos, convirtiendo la información en algo muy preciado tanto para los usuarios como para los Hackers, es por eso que debemos tener una serie de precauciones para evitar que alguien no deseado indague en nuestra información y seamos presa fácil de extorsiones, fraudes y pérdidas irreparables.

En los últimos años, se ha producido el crecimiento de un nuevo tipo de comercio, el denominado comercio electrónico, que no es mas que un servicio de la tecnología que permite tener en nuestro domicilio una gran galería comercial por la que podemos pasear de forma fácil y rápida con el ratón, y todo ello sin movernos de casa, esto es posible gracias a la existencia de la gran red Internet, la cual da cobertura a millones de usuarios. Las ventajas del comercio electrónico son evidentes. El comprador puede ver de manera rápida todo el escaparate electrónico y no tiene que ir tienda por tienda en busca del producto deseado. Se optimiza también el tiempo de atención al cliente, que no tiene que esperar largas colas para ser atendido. Por su parte, el vendedor también se beneficia, puesto que puede ofertar sus productos sin necesidad de mostrarlos físicamente al comprador.

Pese a todas estas ventajas, también es cierto que este tipo de comercio presenta sus inconvenientes, el más importante es la falta de seguridad en los procesos de compraventa, es por esto que existe la necesidad del estudio y desarrollo de medidas de protección como la criptografía. Ésta proporciona al comercio electrónico las herramientas necesarias para garantizar, dado el caso, el carácter secreto de la

información intercambiada (confidencialidad), así como la no manipulación de la misma entre el origen y el destino (integridad).

Hoy en día existen diferentes protocolos como el SET (Secure Electronic Transaction) o el SSL (Secure Sockets Layer) que se ocupan de que este tipo de transacciones a través de redes informáticas sean lo más seguras posibles, así como los certificados digitales que son una carta de presentación en la Web pues contienen información como: dominio para el que se expidió, dueño del Certificado, domicilio del dueño y la fecha de validez del mismo, que fácilmente nos ayudará a saber si estamos o no en el sitio correcto.

CAPITULO 1: FUNDAMENTOS DE SEGURIDAD

1 Introducción

Las computadoras están cambiando al mundo y sus negocios, a veces muy rápidamente. Hoy, las empresas y las personas están comprando por medio de la red, usan números (dinero digital) para comprar lo que quieren en los sitios de comercio electrónico, trayendo esto tanto beneficios como problemas, pues la mayoría de estos compradores temen dar sus números de tarjetas de crédito a extraños, temiendo que su información personal o valiosa sea usada sin su consentimiento, la inseguridad, desde luego, es el riesgo más grande de usar dinero digital sobre Internet. A fin de fomentar el uso de los sistemas electrónicos se debe asegurar que la información no relacionada y personal no sea revelada innecesariamente.

1.2 Fundamentos de la Seguridad Digital

Hablar de seguridad en una organización, es tratar que ninguna persona haga cosas que la organización no quiere que haga, así podemos decir que la seguridad en computación se refiere a las disciplinas que protegen la integridad, confidencialidad y disponibilidad de los sistemas y activos de información, refiriéndonos específicamente a la protección de los sistemas de información contra el acceso no autorizado o las modificaciones a la información, brindando o no acceso a los diferentes usuarios, y las medidas necesarias para detectar, documentar y registrar tales amenazas.

La seguridad de la red va mas allá de la protección de los activos y los sistemas, también se refiere a la protección de las transacciones dentro y fuera de ella. Usando esta misma lógica, la seguridad del dinero digital es parte de la seguridad de la red. El mayor riesgo se encuentra durante la transmisión, los atacantes pueden robar el dinero codificado o los números de la tarjeta de crédito durante la transmisión y decodificar los numero para así usar el dinero digital para comprar en Internet o usar esta información para obtener datos más personales o sensitivos.

1.3 Objetivos de la Seguridad

- Asegurar la disponibilidad de cualquier servicio del sistema de seguridad digital para los usuarios cuando lo pidan.
- Asegurar la confidencialidad e integridad de la información transmitida por medio de redes públicas
- Asegurar la autentificación del poseedor de la tarjeta de crédito.
- Proveer protección contra ataques relacionados con el comercio electrónico.
- Tener mecanismos separados de privacidad para el intercambio de la información general y el intercambio de datos de pago.
- Asegurar que cualquier transacción, dinero digital o mensaje enviado llegue al destino apropiado.
- Asegurar que cualquier dinero digital, transacción o mensaje recibido sea exactamente el que fue enviado.
- Controlar el acceso a las computadoras y otras partes conexas. Esto significa terminales, switches, modems, gateways, bridges, routers e impresoras.
- Proteger la información en riesgo de ser vista, alterada o removida por una persona o dispositivo no autorizado.
- Tener un plan de recuperación si las vías de comunicación primarias y de respaldo fracasan.

1.4 Necesidad de la Seguridad

El acceso inseguro al sistema de comercio electrónico deja a los clientes y a los recursos corporativos muy vulnerables. La información propietaria puede ser robada. Las operaciones pueden ser saboteadas. Además los recursos como la fecha de la CPU, el espacio del disco y el ancho de banda de la red pueden ser consumidos por un usuario no autorizado. La carencia de un sistema de dinero digital seguro puede dar como resultado consecuencias serias para una compañía, incluyendo:

- Destrucción de datos.
- Exposición de información y fuentes propietarias.
- Acceso no autorizado a los recursos de la computadora.
- Pérdida de la confidencialidad y el secreto.
- Pérdida de la confianza del cliente.
- Información personal y financiera dañada, destruida o alterada.

1.5 Servicios de Seguridad

La seguridad en un ambiente de comercio electrónico esta estrechamente ligada a la confiabilidad e involucra las siguientes partes:

Confidencialidad: Su propósito es asegurar que las transacciones no sean visualizadas por grupos no autorizados, es decir, proteger los datos transmitidos en la red, por ejemplo, usando encriptación.

Integridad: Su función es proteger los datos o transacciones de alteraciones no autorizadas. El enfoque mas útil y directo es la protección total. Un servicio de integridad orientado a la conexión que trata con un flujo de mensajes asegura que los mensajes son recibidos como fueron enviados, sin duplicación, inserción, modificación ni reorganización. La destrucción de datos también es cubierta por este servicio. De esta forma, el servicio de integridad orientado a la conexión dirige las modificaciones del flujo de mensajes así como la negación del servicio.

No Repudio: Su propósito primario es proteger las comunicaciones de la acción de otros usuarios legítimos más que de atacantes desconocidos. Este servicio no elimina el rechazo, ni previene a una parte de rechazar el reclamo de otra, funciona para asegurar la disponibilidad de evidencia irrefutable de tal forma que se apoye a la resolución rápida de cualquier tipo de desacuerdo.

Autenticación: Estos servicios proveen la certeza de la identidad de una persona o entidad. Esto significa que cuando un reclamo es hecho por una identidad particular, este servicio proveerá un medio para confirmar si el reclamo es correcto o no. Las contraseñas son un medio bien conocido para proveer autenticación.

Control de Acceso: Es la capacidad para limitar o controlar el acceso a los sistemas y aplicaciones por medio de enlaces de comunicaciones. El controlar acceso incluye el uso, modificación, revelación, destrucción y emisión de comandos no autorizados.

1.6 Dinero Digital y Privacidad

Cuando se hacen compras por Internet, con la tarjeta de crédito (dinero digital), la información detallada va a una base de datos, y estos registros pueden llegar a constituir un expediente de la persona, estos efectos pueden revelar no solo información financiera, sino también datos de sus compras, a donde viaja y con quien se comunica. Esta información sensitiva puede hurtarse o ser accedida sin autorización durante la transmisión de la misma, desde el banco, la compañía de tarjetas de crédito, el sistema de pago digital o cualquier institución que enlace estos registros de diferentes fuentes, infringiendo así la privacidad personal.

El dinero electrónico en su forma digital esta surgiendo como la moneda más valiosa de la Edad de la Información, volviéndose cada vez más confidencial. Los archivos y mensajes se crean en las computadoras, se almacenan en discos y son enviados sobre enlaces de comunicación, pero los datos son más valiosos que los medios utilizados para su creación y envío, es por esto que la propiedad cibernética afronta diversos tipos de exposiciones a causa de los derechos a la privacidad. Los sistemas de dinero electrónico deben cumplir todos los requisitos de los servicios de seguridad por lo tanto tienen exactamente las mismas funciones que las monedas y los billetes. Se utilizan diversas tecnologías para implementarlos:

- **Números firmados**. La entidad financiera emite unos números aleatorios y los firma con su clave privada. Estos números están registrados en la base de datos de la entidad, su valía depende de la longitud del número y se pueden fraccionar cambiándolos en la misma. Los usuarios los piden por la red a la entidad a cambio de un cargo a su cuenta o tarjeta y los utilizan cuando creen conveniente. El sistema DigiCash trabaja con este tipo de dinero electrónico.
- **Monederos electrónicos**. Son tarjetas con un chip donde se almacenan cantidades de dinero que previamente se han descontado de una cuenta. El poseedor de la tarjeta posee el dinero de forma anónima y los puede gastar cuando y de la forma que quiera. Estos sistemas ya se utilizan en las compras físicas, pero para Internet se deberían construir ordenadores con lectores adecuados.

1.7 El valor de los datos y la protección a la privacidad

Aunque los bytes de datos carecen de cualquier valor directo cuando se escribieron en el medio de almacenamiento, el valor de un solo dato puede costar un millón de veces mas que el medio en el que esta almacenado. El valor del dato debería incluir también el dinero invertido en el almacenamiento y retención de los datos y cualquier valor potencial del dato en el mercado. Además las organizaciones deberían incluir el tiempo para reunirlos. Por lo tanto el valor puede ser ilimitado.

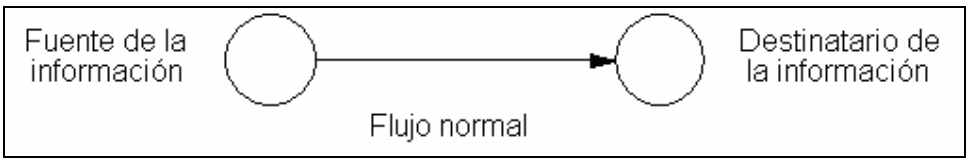
Los buenos modales y las leyes protegen la privacidad de los datos electrónicos. Es simplemente una falta de respeto leer el correo o los datos sensitivos de otros, así como el dinero digital o el número de la tarjeta de crédito. La inseguridad del correo electrónico ha sido un problema desde que el primer e-mail fue intercambiado. Un número asombroso de personas han visto sus mensajes leídos por otros a los cuales no eran destinados. La encriptación es una manera de poner fin a este problema de una vez por todas. Si las organizaciones están por implementar los conceptos de comercio electrónico, deben evaluar las amenazas y vulnerabilidades.

2 Amenazas y vulnerabilidades

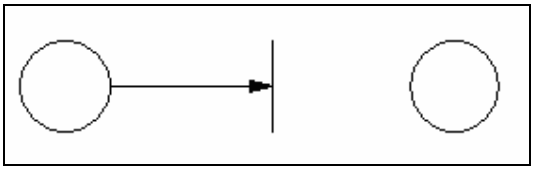
Las amenazas son potenciales para causar daño pero no son una debilidad específica, un ataque no es más que la realización de una amenaza, en cambio una vulnerabilidad se da cuando un sistema es susceptible de ser atacado. Así podemos decir que una amenaza es la intención concreta de explotar las vulnerabilidades de un sistema.

2.1 Amenazas

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad. La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, siendo el diseñador del sistema de seguridad el que debe especificar los servicios y mecanismos de seguridad necesarios. Las cuatro categorías generales de amenazas o ataques son las siguientes:

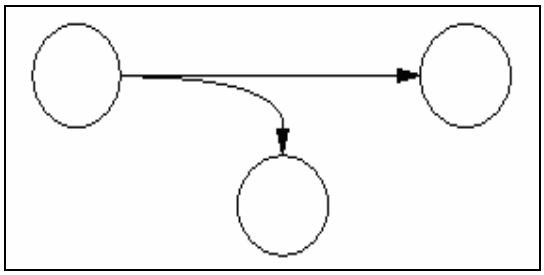


1. **Interrupción**: Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad, ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.



1.2.1 Ataque de Interrupción

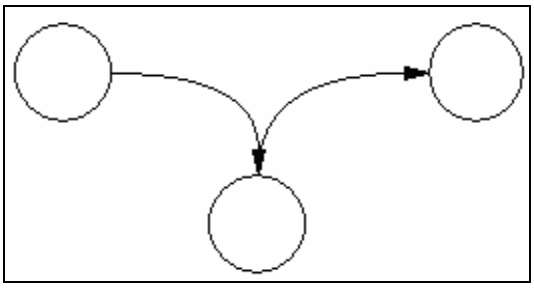
2. **Intercepción**: Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad, la entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son interceptar una línea para obtener datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para descubrir la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).



1.2.2 Ataque de Intercepción

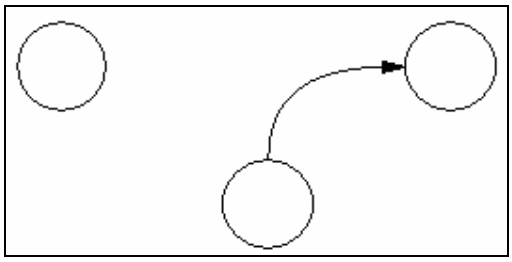
3. **Modificación**: Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad, ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para

que funcione de forma diferente o modificar el contenido de mensajes que están siendo transferidos por la red.



1.2.3 Ataque de Modificación

4. **Fabricación**: Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad, ejemplos de este ataque son la inserción de mensajes ilegítimos en una red o añadir registros a un archivo.



1.2.4 Ataque de Fabricación

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación. Estos ataques son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos, sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad**: El intruso se hace pasar por una entidad diferente. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo al individuo acceder a una serie de recursos privilegiados, como robar la contraseña de una cuenta.
- **Reactuación**: Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- **Modificación de mensajes**: Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
- **Degradación fraudulenta del servicio**: Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes ilegítimos. Entre estos ataques se encuentran los de **denegación de servicio**, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

2.2 Vulnerabilidad

Desde el momento en que se ingresan los números de dinero digital en una computadora hasta el momento que llega al último destino, puede ser interceptado y leído durante la transmisión, esta puede ser dividida en cinco pasos y cada uno de ellos tiene diferentes vulnerabilidades:

- El dinero digital almacenado en la computadora del remitente: el dinero digital que se crea y envía a menudo es almacenado en su computadora o en el disco, si este no está encriptado, es vulnerable a ser comprometido por alguien que tenga acceso a los mismos.
- En transmisión: la vulnerabilidad principal en este paso es la interferencia, los atacantes pueden intervenir en la transmisión de datos sensitivos y dinero digital.
- En el buzón de correo del receptor: una vez que el dinero digital es recibido, la transacción es almacenada en una porción del disco duro, es decir, un buzón del correo electrónico, este puede estar en una computadora remota o en el disco

duro propio del receptor. Se requiere de una contraseña para acceder a la transacción, por lo tanto, es importante encriptar y manejar las contraseñas de forma que se evite su conocimiento.

- Clasificado por el sistema de correo electrónico para propósitos administrativos: la mayoría de los sistemas de comercio electrónico y de dinero digital purgan las transacciones anteriores después de un tiempo específico, pero también hacen copias de respaldo con propósito de facturación o en caso de que falle el sistema. Si los atacantes acceden a estos archivos, una gran cantidad de información personal será revelada, incluyendo con quien se comunica, que compra y donde esta.
- Análisis del tráfico: aunque los atacantes no intercepten las transacciones pueden aprender mucho sobre ellas haciendo un análisis del tráfico.

3. Mecanismos de seguridad

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información, los más importantes son:

- **Intercambio de autenticación**: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.
- **Cifrado**: garantiza que la información no es legible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar, mediante un proceso, un texto normal en un texto cifrado.
- **Integridad de datos**: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

- **Firma digital**: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.
- **Control de acceso**: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas.
- **Tráfico de relleno**: consiste en enviar tráfico ilegítimo junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
- **Control de encaminamiento**: permite enviar información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en alguna ruta.
- **Unicidad**: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los estos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.

- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

4. Seguridad en el comercio electrónico

Los requisitos comerciales a los cuales se enfrentan hoy las organizaciones, demandan que éstas conozcan y manejen los aspectos de la seguridad de la información corporativa, esto implica que entiendan como proteger su presencia dentro de Internet, incluyendo sus sitios Web. También se espera que la organización proporcione adecuados niveles de seguridad especializada para apoyar y promover nuevas iniciativas de comercio electrónico.

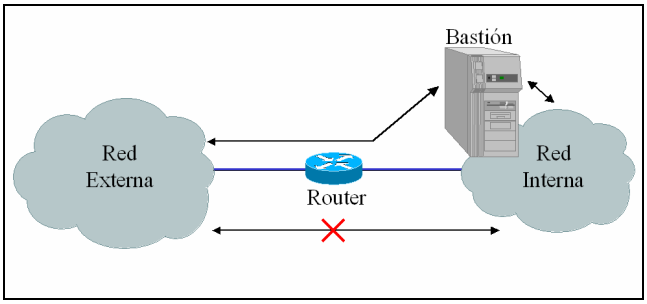
Las soluciones automatizadas se tornan más complejas. Muchas veces conllevan un prolongado tiempo para su correcta implementación. Por lo cual, la tecnología para protección de la información debe ir avanzando de la misma manera, ya que todos estos cambios hacen que se incrementen las amenazas y vulnerabilidades a las que se exponen las organizaciones que utilicen estas nuevas formas de hacer negocios. Atender este desafío involucra realizar una compleja revisión de aspectos técnicos como:

- Mantener una configuración apropiada del firewall para asegurar integridad y privacidad de las comunicaciones entre su organización y otras a lo largo de las redes no-seguras como la Internet.
- Colocar estratégicamente software de detección de intrusos para complementar la configuración del firewall.
- Una adecuada política de recursos humanos que logre retener a las personas con las habilidades técnicas necesarias para los aspectos de la seguridad del ambiente Web.
- Monitorear continuamente la evolución de la tecnología de seguridad de información, productos y servicios que se ofrecen y su potencial para satisfacer sus necesidades comerciales y ver como encajan en su infraestructura técnica.
- Evaluar los mecanismos de acceso, de autentificación y de encriptación así como de protocolos de seguridad que se utilizan o que se podrían utilizar en un ambiente de comercio electrónico.

Firewalls

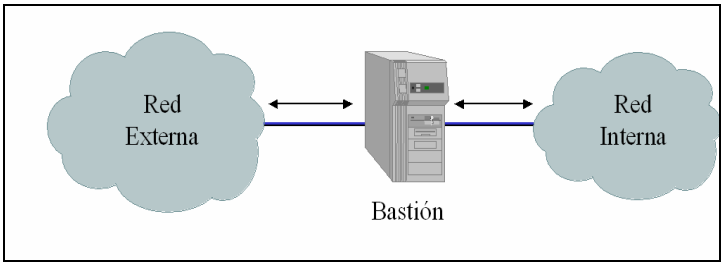
El firewall es considerado como el guardián de seguridad de Internet en la puerta de la empresa, sin una apropiada configuración y ubicación estratégica, resulta imposible proteger la red corporativa adecuadamente. Con el crecimiento comercial en Internet, el firewall es la parte más vital para la defensa del perímetro contra accesos no autorizados. Sin embargo, no es la única respuesta a la seguridad en el ambiente Web.

El concepto de *cortafuego* o *firewall*, consiste en un dispositivo formado por uno o varios equipos que se sitúan entre la red de la empresa y la red exterior (normalmente la Internet), el cortafuego analiza todos los paquetes que transitan entre ambas redes y filtra los que no deben ser reenviados, de acuerdo con un criterio establecido de antemano.



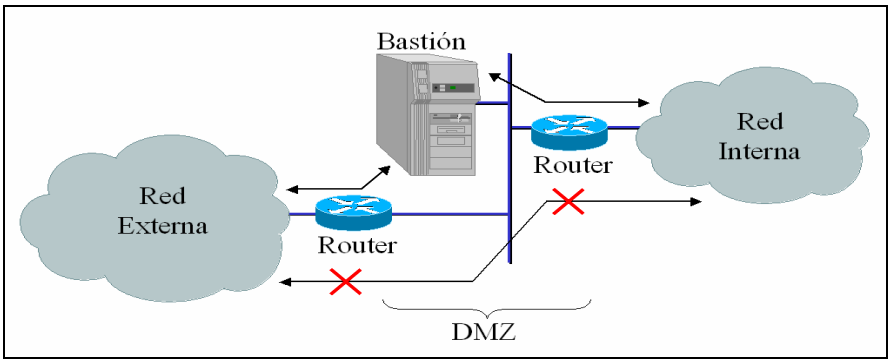
1.4.1 Cortafuegos basado en router

La versión más simple de un firewall consiste únicamente en un router en el que se han configurado diversos filtros, por ejemplo impidiendo o limitando el acceso a determinadas direcciones de red, o el tráfico de ciertas aplicaciones o una combinación de ambos criterios, como vemos en la *Figura 1.4.1*. Dado que los usuarios siguen teniendo conexión directa a nivel de red con el exterior esta solución no es muy fiable; además las posibilidades de definir filtros en los routers son limitadas y el rendimiento baja considerablemente si al router se le carga con una tarea de filtrado compleja.



1.4.2 Cortafuegos basado en host bastión (*dual homed gateway*)

El siguiente nivel de firewall está formado por un host (*dual homed gateway*) que conecta por una parte a la Internet y por otra a la red corporativa, actuando él como router, como vemos en la *Figura 1.4.2*. El host implementa un servidor Web Proxy que actúa como pasarela de aplicación para los servicios que se quieren permitir, limitado por los filtros o reglas especificados. La computadora que actúa como barrera entre las dos redes se denomina "bastion host". Esta solución ofrece una seguridad mayor que la anterior ya que el servidor Proxy, al ser un host, puede procesar filtros mas complejos que un router; pero si un usuario malintencionado consiguiera instalar un programa espía (sniffer) en el host bastión podría capturar tráfico de la red interna de la empresa, ya que está directamente conectado a la LAN.



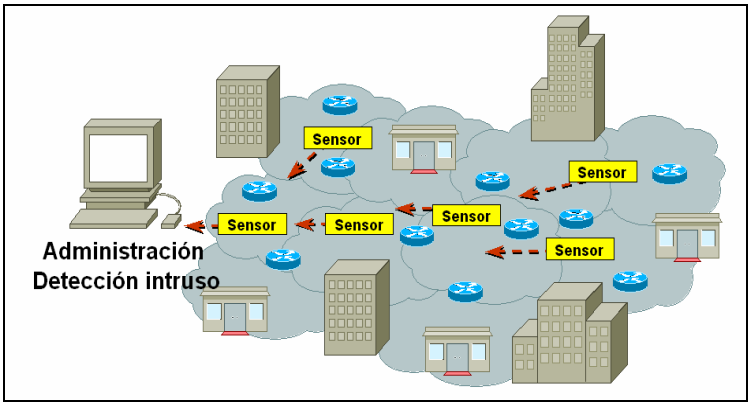
1.4.3 Cortafuegos con zona desmilitarizada, subred apantallada (*screened subnet*)

Un nivel mayor de seguridad se consigue configurando el firewall mediante un host y dos routers conectados entre sí por una pequeña red local; uno de los routers se conecta con la red local de la empresa y el otro con la Internet; el host implementa una pasarela multiaplicación (servidor Proxy), pero al no estar él directamente conectado a la red local de la empresa incluso en el caso de que un hacker consiguiera instalar en él un sniffer no podría capturar tráfico confidencial, pues solo podrá ver los paquetes dirigidos a él como vemos en la *Figura 1.4.3*. Esta configuración se llama subred apantallada o *screened subnet*. En este modelo la red

que une los routers con el host se denomina *zona desmilitarizada* o zona DMZ (Demilitarized Zone, algo así como una zona neutra de seguridad).

Detección de intrusos o IDS (Intrusion Detection System)

El Software de detección de intrusos es otro ingrediente esencial en el ambiente de seguridad de la Web, mientras el firewall actúa como un cerco protector alrededor de la red corporativa, el IDS actúa como un sistema de monitoreo por video y alarma contra ladrones. Estos sistemas se diseñan para complementar las capacidades del firewall. Las características deseables para un IDS son que esté continuamente en ejecución y debe poderse analizar él mismo y detectar si ha sido modificado por un atacante, utilizar los mínimos recursos posibles y adaptarse fácilmente a los cambios de sistemas y usuarios, por lo que en ocasiones poseen inteligencia para adaptarse (aprender por su experiencia) y configurarse.



1.4.4 Ejemplo de detección de intrusos en red

Las intrusiones pueden clasificarse de la siguiente manera basándonos en el efecto de las mismas y la forma de llevarlas a cabo:

- Intento de entrada: una persona ajena al sistema intenta acceder de forma no autorizada al mismo. Se detectan normalmente por modelos de comportamiento extraños, o violaciones de las restricciones dadas por la política de seguridad.
- Ataque enmascarado: a partir de un usuario del sistema se intenta un ataque del mismo. Este es detectado a partir de modelos de comportamiento extraño o violaciones de inconvenientes de seguridad.

- Penetraciones en el sistema de control: que son normalmente detectadas a partir de la observación de modelos especiales de actividad.
- Fuga: cuando se utilizan de manera excesiva los recursos de un sistema. Se detectan normalmente por usos anormales de los recursos de E/S.
- Rechazo de Servicio: detectados por uso extraño de los recursos del sistema.
- Uso malicioso: detectado normalmente por modelos de comportamiento extraño, violaciones de las restricciones de seguridad, o uso de privilegios especiales.

Una clasificación según su localización es:

- NIDS (Network Intrusion Detection System): detecta los paquetes armados maliciosamente y diseñados para no ser detectados por los cortafuegos. Consta de un sensor situado en un segmento de la red y una consola. La ventaja que tiene este tipo de cortafuegos es que no se requiere instalar software adicional en ningún servidor y su inconveniente es que es local al segmento, si la información cifrada no puede procesarla.
- HIDS (Host Intrusion Detection System): analiza el tráfico sobre un servidor. Las ventajas que tiene es que registra comandos utilizados, es más fiable, mayor probabilidad de acierto que NIDS.

Clasificación según modelos de detección:

- Detección de mal uso: verifica sobre tipos ilegales de tráfico, secuencias que previamente se sabe se utilizan para realizar ataques (conocidas como exploits)
- Detección de uso anómalo: verifica diferencias estadísticas del comportamiento normal de una red, según franjas horarias, según la utilización de puertos.

Clasificación según naturaleza

- Pasivos: registran violación y generan una alerta
- Reactivos: responden ante la situación, anulando sesión, rechazando conexión por el firewall, etc.

5. Normas de seguridad

Es esencial establecer prácticas estándar de cómo dirigir las revisiones de los códigos de las aplicaciones de la Web; el uso de software para la búsqueda de vulnerabilidades en los servidores así como requerir de razones justificadas y validadas antes de adecuar y permitir el acceso de otras organizaciones por medio del firewall, sin esto se corre el riesgo de generar nuevas vulnerabilidades que pueden causar exposiciones serias a la seguridad de información sensible. Estas normas no tienen que ser rigurosamente restrictivas, pero deben ser eficaces y capaces de minimizar los riesgos.

Valoración de la seguridad: asegurar el ambiente del comercio también involucra mirar al futuro. Esto significa que continuamente deben analizarse las nuevas técnicas y productos que proporcionarán una fuerte autentificación de usuarios, necesario para afianzar el desenvolvimiento del comercio electrónico. Parte de esta tarea puede ser llevada a cabo por una comprensión del concepto de la Infraestructura de Clave Pública (PKI) y el uso de Certificados Digitales, como un método para proporcionar identificación positiva del usuario y privacidad a través de encriptación de los datos.

Respuesta de Incidentes: otro factor importante a considerar es la creación de un Equipo de Respuesta a Incidentes para proporcionar una reacción rápida y firme a una intrusión seria en la red, como un ataque de Hacker o un virus no fácilmente manejable. Un equipo de esta naturaleza apropiadamente organizado involucrara la representación de las áreas técnicas y del negocio. A veces puede ser deseable establecer un acuerdo contractual con una tercera parte calificada para el apoyo inmediato en una base de 24x7.

Políticas: empleados, contratistas y otros que pueden ser autorizados para acceder a la red necesitan entender y seguir las reglas establecidas por la organización para comunicarse vía Internet o cualquier otra red externa. La comunicación y el buen entendimiento de las políticas son esenciales para proteger los recursos de la información.

6. Conclusiones

Con todo lo anteriormente expuesto, puedo concluir que se necesita mucho tiempo, esfuerzo y especialización para manejar con éxito la seguridad en un ambiente Web, más aun cuando nos enfrentamos a redes corporativas literalmente abiertas al mundo, con un número no imaginario de usuarios potenciales que se conectan a nuestra red, algunos de ellos averiguando día a día maneras de acceder a los datos que protegemos, obligándonos a encontrar la manera de no cometer errores de seguridad y evitar más amenazas de exposición. Definitivamente la protección de la información debe entenderse como una preocupación de primera importancia en la organización, pues esta es tanto un riesgo de negocio como una preocupación crítica de la infraestructura tecnológica.

CAPITULO 2: PROTOCOLOS DE SEGURIDAD

1. Introducción

Es un hecho conocido que Internet constituye un canal de comunicaciones inseguro, debido a que la información que circula a través de ésta red es fácilmente accesible en cualquier punto intermedio por un posible atacante. Los datos transmitidos entre dos nodos de Internet por ejemplo su máquina y el servidor Web desde el que quiere descargar una página, se segmentan en pequeños paquetes que son encaminados a través de un número variable de nodos intermedios hasta que alcanzan su destino.

En cualquiera de ellos es posible leer el contenido de los paquetes, destruirlo e incluso modificarlo, posibilitando todo tipo de ataques contra la confidencialidad y la integridad de sus datos. El ejemplo más conocido y gráfico para ilustrar esta situación es el de la tarjeta postal, que puede ser revisada por los empleados de correos, por los vecinos o por la familia, por lo que no suele confiársele información sensible, para prevenir esto se utilizaría un sobre cerrado y lacrado. En el caso de Internet, la solución más comúnmente adoptada para construir el análogo digital de este sobre se basa en la utilización de los protocolo SSL y SET, que los estudiaremos a continuación.

1.1 Protocolo SSL (Secure Sockets Layer)

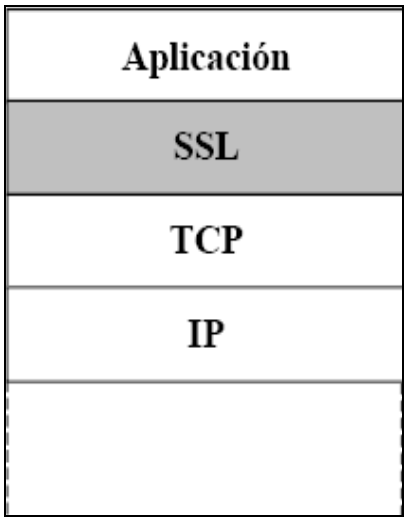
SSL fue diseñado y propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator. Sin embargo, no fue hasta su tercera versión, conocida como SSL v3.0 que alcanzó su madurez, superando los problemas de seguridad y limitaciones de sus predecesores. En su estado actual, proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

SSL v3.0 goza de gran popularidad, por lo que se encuentra ampliamente extendido en Internet. Viene soportado por los principales navegadores del mercado, así es que

no se necesita realizar ninguna acción especial para invocar este protocolo, basta con seguir un enlace o abrir una página cuya dirección empieza por https://. El navegador se encarga del resto. Eso sí, debemos asegurarnos de tener SSL habilitado en el navegador.

1.2 Funcionamiento del Protocolo SSL

Usado principalmente en comunicaciones de hipertexto pero con posibilidad de uso en otros protocolos, ya que SSL es una capa por debajo de HTTP y tal como lo indica su nombre está a nivel de socket por lo que permite ser usado no tan solo para proteger documentos de hipertexto sino también servicios como FTP, SMTP, TELNET entre otros. *Figura 2.1.1*.



2.1.1 Situación de SSL en la pila

El protocolo SSL se comporta como una máquina de estados, durante el intercambio de información siempre hay un estado de escritura activo y otro pendiente y un estado de lectura activo y otro pendiente. Para cambiar del estado activo al pendiente se utiliza un subprotocolo del Handshake llamado **Change Cipher Spec**, entre dos entidades cliente y servidor se pueden abrir varias sesiones SSL, aunque no es habitual, y dentro de cada sesión se pueden mantener varias conexiones SSL. Las conexiones se abren o cierran a través del protocolo de Handshake.

Un **estado de sesión** incluye los siguientes elementos:

- Identificador de sesión: Un número arbitrario elegido por el servidor para identificar la sesión.
- Certificado: El certificado X.509v3 del otro.
- Método de compresión: Algoritmo de compresión.
- Algoritmo de encriptación: Especifica el algoritmo simétrico de encriptación para confidencialidad y la función Hash de resumen para integridad. También se definen atributos de Hash o encriptación.
- Clave maestra: Un número de 48 bytes secreto entre el servidor y el cliente.
- Flag de nuevas conexiones: Indica si desde esta sesión se pueden iniciar nuevas conexiones.

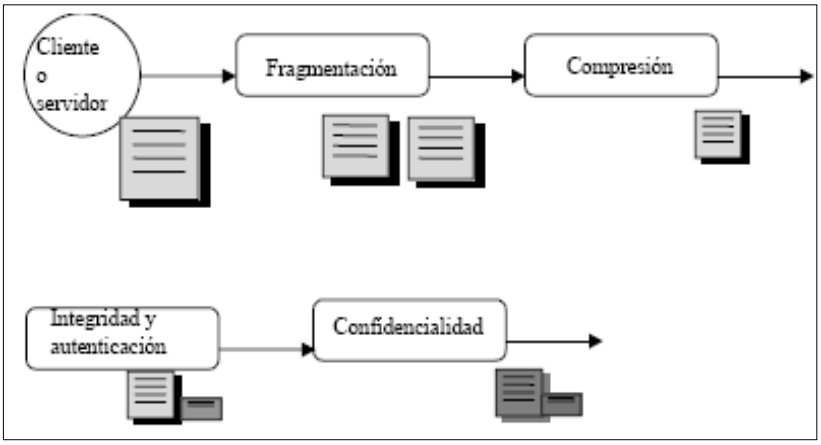
Un **estado de conexión** incluye los siguientes elementos:

- Números aleatorios del servidor y el cliente: Números de inicio de la secuencia elegidos por el cliente y el servidor.
- Número secreto del cliente para MAC: Número secreto utilizado por el cliente para calcular los MAC de sus mensajes.
- Número secreto del servidor para MAC: Número secreto utilizado por el servidor para calcular los MAC de sus mensajes.
- Clave secreta del cliente: Clave secreta utilizada por el cliente para encriptar sus mensajes.
- Clave secreta del servidor: Clave secreta utilizada por el servidor para encriptar sus mensajes.
- Vectores iniciales (IV): Si se utiliza encriptación con modo CBC (Cipher Block Chainning) se necesita un vector inicial para cada clave.
- Números de secuencia: Cada parte actualiza números de secuencia en cada mensaje, estos son puestos a cero cuando se recibe un mensaje change chiper spec.

Protocolo de registro en SSL

El protocolo de registro realiza las funciones de seguridad sobre los mensajes que llegan de la capa de Handshake o de las aplicaciones (HTTP, FTP,...). Para ello

utiliza los parámetros de conexión que se han negociado antes mediante la capa de Handshake. En la *Figura 2.1.2* se pueden ver las funciones realizadas por orden de actuación en el emisor.

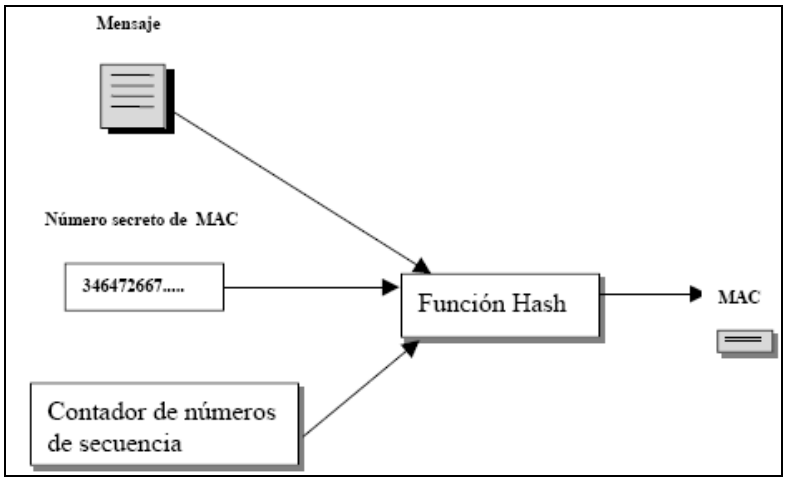


2.1.2 Protocolo de registro de SSL

La **fragmentación** divide los mensajes mayores de 214 bytes en bloques más pequeños.

La **compresión** se realiza utilizando el algoritmo que se ha negociado en la fase inicial, puede ser algoritmo nulo (Null) si no se comprimen los mensajes.

La **autenticación e integridad** se realiza calculando un resumen del mensaje concatenado con un número secreto y el número de secuencia (*Figura 2.1.3*). El resultado de este resumen es el MAC y se añade al mensaje. La autenticación se puede comprobar con el número secreto, que sólo comparten el cliente y el servidor, y mediante el número de secuencia que viaja siempre cifrado. La integridad se realiza mediante la función Hash.



2.1.3: Integridad en el protocolo de registro de SSL

La **confidencialidad** se realiza encriptando con un algoritmo simétrico mediante la clave secreta negociada en el Handshake. Las encriptaciones pueden ser de:

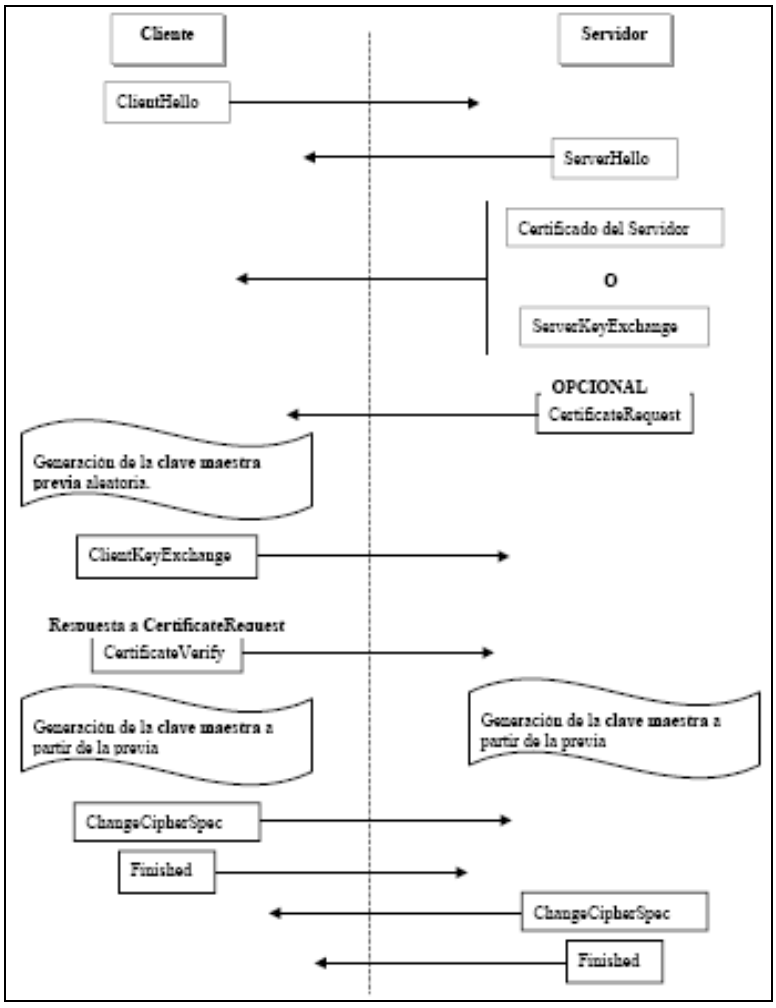
- **Bloque**. Se encripta en bloques de 64 bits. Si el mensaje no es múltiplo de 64 se añaden bits de relleno y se indica en el formato del mensaje. Los algoritmos utilizados son RC2 y DES en forma CBC, para la forma CBC se utiliza un vector inicial (IV) previamente pactado.
- **Stream**. Se encripta realizando la OR-Exclusiva entre los bytes y un generador pseudoaleatorio, este generador es el algoritmo RC4.

Protocolo Handshake en SSL

Se encarga de establecer, finalizar y mantener las conexiones SSL. Durante el Handshake se negocian los parámetros generales de la sesión y los particulares de cada conexión. Hay dos subprotocolos anexos:

- **Change Cipher Spec**. Es un único mensaje que sirve para pasar de los estados activos a los pendientes.
- **Alerta**. Son mensajes que avisan de problemas ocurridos durante la conexión, pueden obligar a una terminación brusca de la sesión.

En la *Figura 2.1.4* se puede ver el esquema del protocolo.



2.1.4 Protocolo Handshake de SSL

Los mensajes llevan la siguiente información:

- **ClientHello**. Es el mensaje que envía el cliente cuando establece contacto con un servidor seguro. Describe los parámetros que quiere utilizar durante la sesión:
  - **Hora y fecha.**
  - **Identificador de sesión.**
  - **Algoritmos de encriptación.** Consecutivamente envía los algoritmos por orden de preferencia de intercambio de claves, encriptación de mensajes y MAC.
  - **Algoritmos de compresión.** Se envían los algoritmos que acepta por orden de preferencia.

- **ServerHello**. Se envían los algoritmos elegidos para la conexión, siempre deben ser alguno de los propuestos en el mensaje de ClientHello. Si no hay acuerdo con los algoritmos se envía un mensaje de error.
- **Certificado o ServerKeyExchange**. Si el servidor tiene certificado X.509v3 se envía, si no tiene se puede utilizar el mensaje ServerKeyExchange para enviar la clave pública sin certificado. El cliente puede elegir si acepta una clave sin certificado.
- **CertificateRequest**. Los servidores pueden pedir certificados a los clientes utilizando este mensaje.
- **CertificateVerify**. Si el cliente recibe una petición de certificado debe enviar su certificado mediante este mensaje.
- **ClientKeyExchange**. Se envía un número aleatorio que sirve para calcular la clave maestra, esta clave sirve para generar todas las claves y números secretos utilizados en SSL. Se envía encriptada con la clave pública del servidor.
- **ChangeCipherSpec**. Inicia la sesión segura.
- **Finished**. Termina la fase de Handshake. Sirve para comprobar que la negociación de parámetros y claves ha funcionado correctamente.

1.3 Implementación del Protocolo SSL

Para crear un sistema de pago electrónico basado en SSL es necesario conseguir un certificado electrónico para el vendedor, generalmente se obtiene de la empresa Verisign, la misma que esta considerada por Microsoft y Netscape como Autoridad Certificadora de confianza y por defecto viene activada en sus respectivos navegadores, una vez realizado el pago, el vendedor obtiene el PIN de la tarjeta de crédito del cliente por lo que debe estar provisto de algún método que permita enviar estos datos a una entidad financiera capaz de realizar la transferencia bancaria. Otra opción que han ofrecido varios bancos es la de utilizar un Terminal Punto de Venta (TPV) para realizar la retransferencia, el TPV se conecta al servidor del vendedor y mediante un software CGI se realiza la comunicación.

1.4 Funcionamiento del Protocolo SSL en el Comercio electrónico

SSL es considerado como la solución de seguridad implantada en la mayoría de los servidores Web que ofrecen servicios de comercio electrónico. Su mayor mérito radica en ofrecer respuesta al principal problema que afronta el comercio en línea: la resistencia de los usuarios a enviar su número de tarjeta de crédito a través de un formulario Web por el temor de que caiga en manos de un hacker y por la desconfianza generalizada hacia Internet.

La forma más fácil y extendida para construir un sistema de comercio en Internet consiste en utilizar un servidor Web con un catálogo con información sobre los productos o servicios ofrecidos y un formulario para procesar los pedidos. El catálogo estará compuesto por una serie de páginas Web describiendo la mercancía en venta o los servicios ofrecidos, junto a cada artículo o servicio se sitúa un botón que el usuario puede pulsar para acceder al mismo. Cuando el cliente ha terminado sus compras o llenado los datos de su consulta, pasa por una "caja virtual", que iniciará el proceso de pago, o mostrará el resultado de su consulta.

Hoy por hoy, el medio de pago más común en Internet es la tarjeta de crédito. No obstante, no hay que despreciar otros métodos más conservadores como el envío contra reembolso o la transferencia bancaria, que representan un porcentaje importante de las ventas en línea. El usuario debe rellenar un formulario con sus datos personales, y los datos correspondientes a su tarjeta de crédito (número, fecha de caducidad, titular). Esta arquitectura no exige que el servidor disponga de capacidades especiales para el comercio. Basta con que se utilice como mínimo un canal seguro para transmitir la información de pago y el comerciante ya se ocupará manualmente de gestionar con su banco las compras.

Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura. A medida que el comercio crece, esta arquitectura podría llegar a resultar difícil de expandir o de incorporar nuevas tecnologías y componentes a medida que vayan apareciendo. Existen una serie de desventajas al utilizar exclusivamente SSL para llevar adelante ventas por Internet:

- Por un lado, SSL ofrece un canal seguro para el envío de números de tarjeta de crédito, pero carece de capacidad para completar el resto del proceso comercial: verificar la validez del número de tarjeta recibido, autorizar la transacción con el banco del cliente, y procesar el resto de la operación con el banco adquiriente y emisor.
- Por otro lado, es importante recalcar que SSL sólo garantiza la confidencialidad e integridad de los datos en tránsito, ni antes ni después. Por lo tanto, si se envían datos personales al servidor, entre ellos el ya citado número de tarjeta de crédito, el número de la seguridad social, etc., SSL solamente asegura que mientras viajan desde el navegador hasta el servidor no serán modificados ni espiados. Lo que el servidor haga con ellos, está ya más allá de la competencia de este protocolo. Los datos podrían ser manipulados irresponsablemente o caer en manos de un atacante que asaltara el servidor con éxito.
- Además, SSL permite realizar ataques sobre servidores de comercio creados para averiguar números de tarjeta reales. Un programa escrito por un hacker va probando números de tarjeta válidos, pero que no se sabe si corresponden o no a cuentas reales, realizando compras ficticias en numerosos servidores. Si el número de tarjeta no sirve, el servidor devuelve un error, mientras que si es auténtico, el servidor lo acepta. El programa entonces cancela la compra y registra el número averiguado, para seguir adelante con el proceso. De esta forma, el hacker puede hacerse en breve con cientos de números auténticos.

Todos estos inconvenientes convierten a SSL en una solución deficiente desde el punto de vista del pago electrónico, lo cual no significa que no se deba utilizar ni que no sea útil en otras muchas facetas igualmente necesarias de la actividad empresarial. Al proporcionar un canal seguro de comunicaciones, el comerciante puede ofrecer al cliente de manera confidencial una serie de servicios para estrechar las relaciones de confianza: autenticación del cliente frente al comercio, trato personalizado, evitar que terceras partes espíen las compras de los clientes, intercambio de información privada, etc. Dado que SSL es un protocolo seguro de propósito general, que no fue diseñado para el comercio en particular, se hace necesaria la existencia de un protocolo específico para el pago. Este protocolo existe y se conoce como SET.

2. Protocolo SET (Transacciones electrónicas seguras)

SET es un protocolo estandarizado y respaldado por la industria, diseñado para salvaguardar las compras pagadas con tarjeta a través de redes abiertas, incluyendo Internet. El estándar SET fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de otras compañías líderes en el mercado de las tecnologías de la información, como Microsoft, IBM, Netscape, RSA, VeriSign y otras. En cuanto el protocolo SET 1.0 fue finalizado, comenzó a emerger una infraestructura basada en el mismo para soportar su uso a gran escala. Ya existen numerosos fabricantes de software que han empezado a crear productos para consumidores y comerciantes que deseen realizar sus compras de manera segura disfrutando de las ventajas ofrecidas por este protocolo.

2.1 Servicios del Protocolo SET

- **Autenticación:** todas las partes implicadas en la transacción económica (el cliente, el comerciante y los bancos, emisor y adquiriente) pueden autenticarse mutuamente mediante certificados digitales. De esta forma, el comerciante puede asegurarse de la identidad del titular de la tarjeta y el cliente, de la identidad del comerciante. Se evitan así fraudes debidos a usos ilícitos de tarjetas y a falsificaciones de comercios en Internet imitando grandes Web comerciales. Por su parte, los bancos pueden verificar así las identidades del titular y del comerciante.
- **Confidencialidad:** la información de pago se cifra para que no pueda ser espiada. Es decir, solamente el número de tarjeta de crédito es cifrado por SET, de manera que ni siquiera el comerciante llegará a verlo, para prevenir fraudes. Si se quiere cifrar el resto de datos de la compra, como por ejemplo qué artículos se han comprado, debe recurrirse a un protocolo de nivel inferior como SSL.
- **Integridad:** garantiza que la información intercambiada no podrá ser alterada de manera accidental o maliciosa mientras viaja a través de la red, utilizando algoritmos de firma digital.
- **Gestión del pago:** SET gestiona tareas asociadas a la actividad comercial de gran importancia como registro del titular y del comerciante, autorizaciones y liquidaciones de pagos, anulaciones, etc.

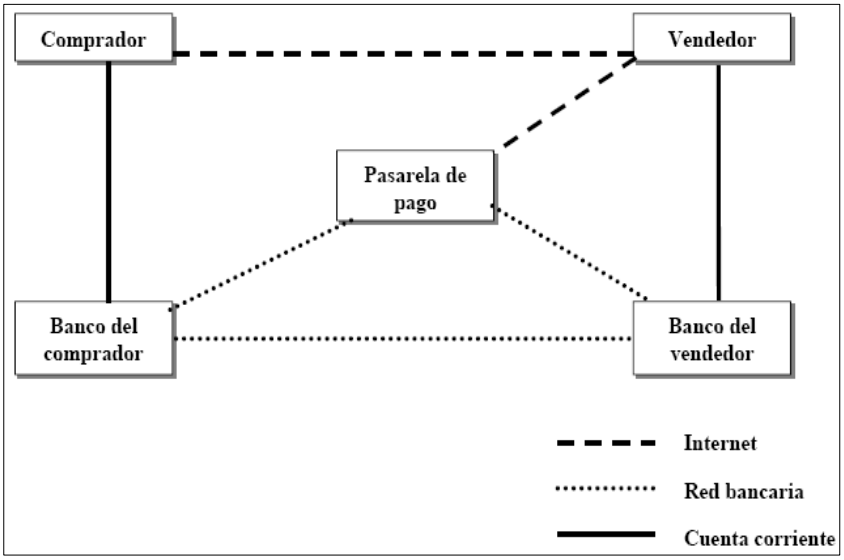
- **Intimidad:** haciendo que el banco emisor de la tarjeta de crédito no pueda acceder a información sobre los pedidos del titular, dejándolo incapacitado para elaborar perfiles de hábitos de compra de sus clientes.
- **Verificación inmediata:** asegura al comerciante una verificación inmediata, antes de completarse la compra, de la disponibilidad de crédito y de la identidad del cliente. De esta forma el comerciante puede completar los pedidos sin riesgo de que posteriormente se invalide la transacción.
- **No repudio para resolución de disputas:** la mayor ventaja de SET frente a otros sistemas seguros es la adición al estándar de certificados digitales (X.509v3) que asocian la identidad del titular y del comerciante con entidades financieras y los sistemas de pago de Visa, MasterCard, etc.

2.2 Entidades Participantes en el Protocolo SET

El pago mediante tarjeta es un proceso complejo en el cual se ven implicadas varias entidades:

- **El banco emisor:** emite la tarjeta del cliente, extiende su crédito y es responsable de la facturación, recolección y servicio al consumidor.
- **El banco adquiriente:** establece una relación con el comerciante, procesando las transacciones con tarjeta y las autorizaciones de pago.
- **El titular de la tarjeta:** posee la tarjeta emitida por el banco emisor y realiza y paga las compras.
- **El comerciante:** vende productos, servicios o información y acepta el pago electrónico, que es gestionado por su entidad financiera (adquiriente).
- **La pasarela de pagos:** mecanismo mediante el cual se procesan y autorizan las transacciones del comerciante. La pasarela puede pertenecer a una entidad financiera (adquiriente) o a un operador de medio de pago, el cual procesa todas las transacciones de un conjunto de entidades.
- **El procesador (redes de medios de pago):** proporciona servicios adicionales operando la infraestructura de telecomunicaciones sobre la que se realizan las transacciones.
- **Autoridad de certificación:** certifica las claves públicas del titular de la tarjeta, del comerciante y de los bancos.

Se relacionan entre ellos como marca la *Figura 2.2.5*.



2.2.5 Agentes del SET

2.3 Transacción Electrónica del Protocolo SET

Una transacción SET típica funciona de forma muy parecida a una transacción convencional con tarjeta de crédito y consta de los siguientes pasos:

1. **Decisión de compra del cliente.** El cliente navega por el sitio Web del comerciante y decide comprar un artículo, para ello llena algún formulario y posiblemente hace uso de alguna aplicación tipo carrito de compra, para ir almacenando diversos artículos y pagarlos todos al final. El protocolo SET se inicia cuando el comprador pulsa el botón de Pagar.
2. **Arranque del monedero.** El servidor del comerciante envía una descripción del pedido que despierta a la aplicación monedero del cliente.
3. **El cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante.** La aplicación monedero del cliente crea dos mensajes que envía al comerciante. El primero con la información del pedido y el segundo que contiene las instrucciones de pago del cliente (número de tarjeta de crédito, banco emisor, etc.) para el banco adquiriente. En este momento, el software monedero del cliente genera una firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el comerciante pueda acceder a la información del pedido, pero no a las instrucciones de pago y el banco pueda acceder a las instrucciones de pago pero

no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso.

4. **El comerciante envía la petición de pago a su banco.** El software SET en el servidor del comerciante crea una petición de autorización que envía a la pasarela de pagos, incluyendo el importe a ser autorizado, el identificador de la transacción y otra información relevante acerca de la misma, todo ello convenientemente cifrado y firmado. Entonces se envían al banco adquiriente la petición de autorización junto con las instrucciones de pago.
5. **El banco adquiriente valida al cliente y al comerciante y obtiene una autorización del banco emisor del cliente.** El banco del comerciante descifra y verifica la petición de autorización. Si el proceso tiene éxito, obtiene a continuación las instrucciones de pago del cliente, que verifica a su vez, para asegurarse de la identidad del titular de la tarjeta y de la integridad de los datos. Se comprueban los identificadores de la transacción en curso (el enviado por el comerciante y el codificado en las instrucciones de pago) y, si todo es correcto, se formatea y envía una petición de autorización al banco emisor del cliente a través de la red de medios de pago convencional.
6. **El emisor autoriza el pago.** El banco emisor verifica todos los datos de la petición y si todo está en orden y el titular de la tarjeta posee crédito, autoriza la transacción.
7. **El adquiriente envía al comerciante un testigo de transferencia de fondos.** En cuanto el banco del comerciante recibe una respuesta de autorización del banco emisor, genera y firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, la cual se la hace llegar al comerciante.
8. **El comerciante envía un recibo al monedero del cliente.** Cuando el comerciante recibe la respuesta de autorización de su banco, verifica las firmas digitales y la información para asegurarse de que todo está en orden. El software del servidor almacena la autorización y el testigo de transferencia de fondos. A continuación, se completa el procesamiento del pedido del titular de la tarjeta, enviando la mercancía o suministrando los servicios pagados.
9. **El comerciante usa el testigo de transferencia de fondos para cobrar el importe de la transacción.** Después de haber completado el procesamiento del pedido del titular de la tarjeta, el software del comerciante genera una petición de

transferencia a su banco, confirmando la realización con éxito de la venta, como consecuencia, se produce el abono en la cuenta del comerciante.

10. **A su debido tiempo, el dinero se descuenta de la cuenta del cliente (cargo).**

El protocolo definido por SET especifica el formato de los mensajes, las codificaciones y las operaciones criptográficas que deben usarse. No requiere un método particular de transporte, de manera que los mensajes SET pueden transportarse sobre HTTP en aplicaciones Web, sobre correo electrónico o cualquier otro método. Como los mensajes no necesitan transmitirse en tiempo presente, son posibles implantaciones de SET eficientes basadas en correo electrónico u otros sistemas asíncronos.

En su estado actual SET solamente soporta transacciones con tarjeta de crédito/débito, y no con tarjetas monedero. Se está trabajando en esta línea para extender el estándar de manera que acepte nuevas formas de pago. Al mismo tiempo se están desarrollando proyectos para incluir los certificados SET en las tarjetas inteligentes, de tal forma que el futuro cambio de tarjetas de crédito a tarjetas inteligentes pueda incorporar el estándar SET.

3. Conclusiones

Como podemos ver el uso de los protocolos SSL y SET nos dan una gran confianza para las transacciones ya que nos proporcionan un transporte de datos cifrados por la red, cada uno diferente, pues se fabrican llaves para cada mensaje nuevo, llevando parte de él incluido, siempre se necesita tener confianza, tanto en el mundo real como en el electrónico, del lugar en el que se esta comprando y con quien se cierra la transacción, pero con el uso de certificados digitales, podemos saber a ciencia cierta con quien estamos tratando y confiar que lo que estamos realizando no va a parar a manos de hackers o crackers.

CAPITULO 3: FIRMAS Y CERTIFICADOS DIGITALES

1. Introducción

Las firmas y certificados digitales se basan en la criptografía, la misma que proviene del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Los sistemas de encriptación por software pueden ser públicos o privados.

Los privados requieren para su funcionamiento que el emisor y el receptor posean exactamente los mismos dispositivos, llamados llaves, a fin de codificar y decodificar el mensaje enviado. Si bien el uso de llaves privadas permite alcanzar niveles superiores de seguridad, el problema radica en que utilizarlas en operaciones de Internet, un medio esencialmente inseguro, resultaría extremadamente poco practico, pues, el intercambio de las propias llaves no puede realizarse a través de la red.

En lo que respecta a sistemas que utilizan una combinación de llaves publicas y privadas, estos requieren que emisor y receptor utilicen algún servicio ofrecido por un tercero, el que será el guardián de las llaves públicas. Estos sistemas ofrecen mayor facilidad para uso práctico y, en materia de seguridad, son lo suficientemente aceptables como para conducir operaciones de comercio electrónico, a continuación revisaremos con más detalle estas formas de cifrado y su uso en las firmas y certificados digitales.

1.1 Claves Simétricas

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave, es importante que dicha clave sea muy difícil de adivinar, hoy se están utilizando ya claves de 128 bits que aumentan el

"espectro" de claves posibles (2 elevado a 128) de forma que aunque se uniesen todos los ordenadores existentes en estos momentos no conseguirían adivinarla en miles de millones de años.

1.2 Claves Asimétricas

También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública (publicada por la Autoridad Certificadora en un directorio especifico en Internet llamado Repositorio y figura también en su Certificado Digital enviado automáticamente junto con cada mensaje al receptor) y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella.

Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer, el par de claves es generado durante el proceso de aplicación (obtención de un Certificado Digital), por el propio navegador mediante un algoritmo denominado RSA.

Es fácil, con los ordenadores de hoy en día, multiplicar dos números grandes para conseguir un número compuesto, pero es muy difícil la operación inversa, dado ese numero compuesto, factorizarlo para conocer cada uno de los dos números. Mientras que 128 bits se considera suficiente en las claves de cifrado simétrico, y dado que la tecnología de hoy en día se encuentra muy avanzada, se recomienda en este caso que la clave pública tenga un mínimo de 1024 bits.

2. Infraestructura para criptografía con clave pública (PKI)

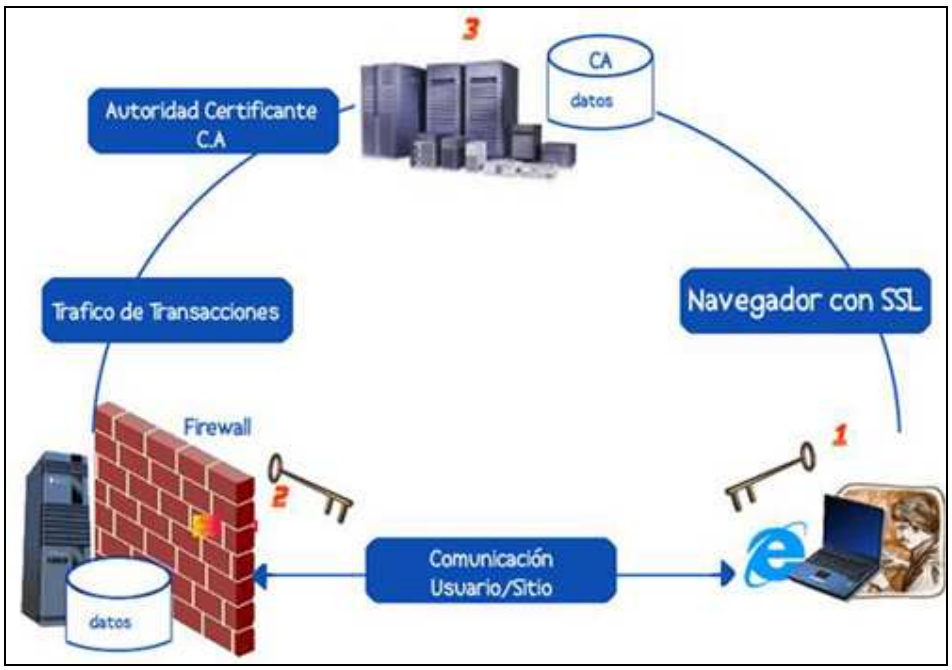
En criptografía, una **infraestructura de clave pública** (**P**ublic **K**ey **I**nfrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas. En una

operación criptográfica que use infraestructura PKI, intervienen conceptualmente las siguientes partes:

- **Política de Seguridad:** establece la manera en que una organización ejecutará procesos de gestión de claves públicas y privadas.
- **Autoridad Certificante (CA):** se encarga de generar los Certificados Digitales, usando una clave privada para firmarlos.
- **Autoridad de Registro (RA):** es la entidad encargada de gestionar altas y bajas de las peticiones de certificación y también de la revocación, entonces un usuario que desea solicitar un certificado de clave pública se debe dirigir a una RA autorizada por una CA.
- **Autoridad de Validación (VA):** proporciona información sobre el estado de los certificados. Realiza las consultas de todas las CRLs necesarias para saber el estado del certificado que se le ha pasado en una petición de validación.
- **Sistema de Distribución de Certificados:** El sistema de distribución puede ser variado, esto depende de la estructura PKI que utilicemos.

- **Aplicaciones habilitadas por PKI:**
  - Comunicación entre servidores
  - Correo Electrónico
  - EDI (Intercambio Electrónico de Datos)
  - Transacciones con tarjeta de Créditos
  - Redes Virtuales Privadas (VPN)

En la siguiente imagen se presenta la misma función en un sitio de Internet que el CA cumple de VA, y RA, dado que es una Empresa Certificadora Externa.



3.2.1 Empresa Certificadora Externa cumpliendo funciones de CA, VA, y RA

El Número 3 es nuestro CA que se encarga de:

- Emitir el Certificado
- Validar la autenticidad del Emisor y Receptor (Punto 1 y 2)
- Mantener una base de datos con los certificados válidos y los removidos.

3. Firmas digitales

La firma digital es la transformación de un mensaje en un texto incomprensible, mediante la utilización del cifrado asimétrico. Resulta tan efectiva en su función de dar seguridad al mensaje porque al ser aplicada se fusiona con este, además es distinta para cada mensaje que se aplica. Una típica transacción con firma digital comienza cuando el firmante esta de acuerdo con el contenido del documento que desea firmar.

Luego un software especifico crea una imagen digital o resumen del mensaje mediante la aplicación de una función denominada Hash Function. Al resultado de la aplicación de esta función se lo denomina Hash Result y consiste en un código único para el mensaje. De esta forma si el mensaje es modificado, el Hash Result será

diferente. Por ultimo el software encripta el Hash Result con la firma digital mediante la aplicación de la clave privada del firmante.

La firma obtenida es única tanto para el mensaje como para la clave privada que se utilizó para su creación. La verificación de la firma digital es realizada computando un nuevo Hash Result del mensaje original utilizando la misma Hash Function usada en la creación de la firma digital. Finalmente con la clave publica que surge del certificado del firmante, el receptor comprueba si la firma digital proviene de la clave privada del firmante y si el nuevo Hash Result es igual al que proviene de la firma digital. El receptor realiza esta operación comunicándose con el registro de claves públicas donde se encuentra registrado el certificado correspondiente. Además del emisor y el receptor, para que el sistema funcione se requiere de terceras partes confiables, estas son las Autoridades de Certificación.

Para obtener una firma digital, la persona interesada, luego de crear las claves debe presentarse ante la autoridad certificadora para registrar su clave pública, acreditando su identidad y/o cualquier otra circunstancia requerida para obtener el certificado que le permita firmar el documento tratado. La información es almacenada en Registros a los cuales se puede acceder on line para saber la validez, vigencia o cualquier otra situación relacionada con los certificados.

3.1 Requerimientos

Los mensajes de autentificación protegen a dos usuarios de intercambio de mensajes contra un tercer usuario. No obstante, no protegen a los dos usuarios cuando se trata del enfrentamiento entre ambos, por ejemplo, en transferencias bancarias y otras operaciones monetarias, donde no hay confianza entre emisor y receptor, es necesario algo mas que la autentificación, es por esto que se utiliza la firma digital, la misma que debe tener las siguientes propiedades:

- Debe ser posible verificar el autor, la fecha y el tiempo de la firma.
- Debe ser posible autentificar los contenidos durante el proceso de firma.
- La firma debe ser verificada por tres partes, para resolver conflictos o disputas.

Con estas propiedades, se pueden formular los siguientes requerimientos:

- La firma debe ser una parte extraída del mensaje que se quiere firmar.

- La firma debe utilizar alguna información exclusiva del emisor para prevenir una invención de un mensaje o denegación.
- Debe ser relativamente fácil producir una firma digital.
- Debe ser relativamente fácil reconocer y verificar la firma digital.
- Debe ser imposible forjar una firma digital, ya sea construyendo un nuevo mensaje para una firma existente o construyendo una firma engañosa dado un mensaje.
- Debe ser práctico retener una copia de la firma digital almacenada.

3.2 Formatos de la Firma Digital

Las normas TS 101 733 *y* TS 101 903 definen los formatos técnicos de la firma electrónica. La primera se basa en el formato clásico PKCS#7 y la segunda en XMLDsig firma XML especificada por el consorcio W3C. Bajo estas normas se definen tres modalidades de firma:

- **Firma básica**. Incluye el resultado de operación de hash y clave privada, identificando los algoritmos utilizados y el certificado asociado a la clave privada del firmante.
- **Firma fechada**. A la firma básica se añade un sello de tiempo calculado a partir del hash del documento firmado por una **TSA** (Time Stamping Authority)
- **Firma validada** o firma **completa**. A la firma fechada se añade información sobre la validez del certificado procedente de una consulta de CRL o de OCSP realizada a la Autoridad de Certificación.

La **firma completa** libera al receptor del problema de ubicar al Prestador de Servicios de Certificación y determinar los procedimientos de validación disponibles y además de cumplir con los principios de autenticidad, cumple el principio de integridad, pues esta queda vinculada al documento de tal forma que cualquier modificación del mismo sea detectable.

4. Certificados digitales

Uno de los problemas que surgen en Internet es el de la identificación de las personas o entidades, por Ejemplo, cómo asegurarnos de que una clave pública que hemos encontrado en Internet pertenece realmente a quién dice pertenecer, una posible solución es la utilización de un certificado digital que es un fichero digital

intransferible y no modificable, emitido por una tercera parte de confianza, Autoridad de Certificación, que asocia a una persona o entidad una clave pública.

4.1 Elementos que contiene un Certificado Digital

Un certificado digital que siga el Standard X509v3, utilizado por los navegadores, contiene la siguiente información:

- Identificación del titular del certificado: Nombre, dirección, etc.
- Clave pública del titular del certificado.
- Fecha de validez.
- Número de serie.
- Identificación del emisor del certificado.

4.2 Principios de los Certificados Digitales

Los principios que la doctrina reconoce como fundamento de las transacciones electrónicas se basan en la necesidad de establecer presunciones que las hagan seguras. Se busca asegurar que la transacción en si misma se forme de acuerdo a la voluntad de las partes:

Integridad: protege a través de la presunción de la no-alteración de los datos que han sido recogidos en el mensaje firmado digitalmente.
Autenticidad: se corresponde con la presunción de que la firma digital pertenece exclusivamente a la persona titular del certificado.
No Repudio: se encuentra recogido en la presunción de que la firma digital refleja el pleno consentimiento del titular del certificado con el contenido de la transacción.

Si coinciden todas las condiciones para acreditar la autenticidad del mensaje electrónico, se garantiza la veracidad de lo documentado y se identifica plenamente al titular y autor de la firma digital. El documento electrónico debe ser considerado valido y gozar de plenos efectos jurídicos.

4.3 Tipos de Certificados Digitales

Hay dos tipos principales de certificados digitales que son importantes para la construcción de un sitio Web seguro y éstos son:

Certificados del servidor: Los certificados del servidor permiten simplemente que los visitantes del sitio Web transfieran con seguridad su información personal como la información de las tarjetas de crédito y de la cuenta bancaria sin la preocupación de hurto. Los certificados del servidor son también responsables de validar la identidad de los dueños del sitio Web de modo que los visitantes puedan sentirse como si estuvieran ocupando una fuente legítima cuando crean o ingresan contraseñas.

Certificados personales: Los certificados personales permiten validar la identidad de los visitantes del sitio Web e incluso restringir su acceso a ciertas porciones del mismo. Los certificados personales se pueden utilizar para cosas tales como enviar y recibir e-mail para la información privada de la cuenta como contraseñas olvidadas o la información del nombre de usuario. Los certificados personales son ideales para las comunicaciones tales como abastecimiento de socios y surtidores controlados, que tienen acceso al sitio para las fechas de envío, disponibilidad del producto, e incluso la gerencia de inventario.

La mayor parte de los protocolos estándares que son adoptados extensamente para las comunicaciones electrónicas confían en los siguientes certificados digitales:

El SSL: Se acepta extensamente como el estándar básico para la autentificación del Web browser y del servidor, e intercambio de datos seguro en Internet, y son el tipo más común de seguridad. Tanto para servidor como para cliente.

S/MIME: protocolo multipropósito seguro de las extensiones del correo del Internet, se considera como el estándar básico para e-mail seguro y EDI (intercambio de los datos electrónicos).

Certificados de firma de objetos: se usan para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red.

Certificado para AC: para identificar a las propias Autoridades Certificadoras. Es usado por el software cliente para certificar la confianza o no de un certificado.

4.4 Niveles de Certificados

Clase 1: emitidos y comunicados electrónicamente a personas físicas, y relaciona el nombre de usuario o su alias y su dirección de e-mail con el registro llevado por el AC. No autentican la identidad del usuario. Son usados fundamentalmente para e-mail y Web Browsing, afianzando la seguridad de sus entornos. En general no se usa en ambientes comerciales.

Clase 2: son emitidos a personas físicas, y confirman la veracidad de la información aportada en el acto de presentar la aplicación que no difiere de la que surge de alguna base de datos de usuarios reconocido. Es usado para comunicaciones intra-inter organizaciones vía e-mail; transacciones comerciales de bajo riesgo; validación de software y suscripciones on line.

Clase 3: emitidos a personas físicas, para asegurar la identidad del suscriptor, y a organizaciones públicas y privadas, para asegurar la existencia y nombre mediante el cotejo de los registros denunciados con los contenidos en bases de datos independientes.

4.5 Funcionamiento de los Certificados Digitales

En el esquema de funcionamiento intervienen tres actores:

- **La Autoridad de Registro (AR):** es la entidad, empresa, banco, organismo público, que conoce al individuo y que autoriza que se le otorgue un Certificado Digital para realizar operaciones con el mismo.
- **El Usuario:** es el cliente, personal directo o personal de organizaciones vinculadas a la Autoridad de Registro.
- **La Autoridad Certificadora (AC):** es la entidad encargada de emitir y administrar los Certificados Digitales, publicando las claves públicas en un Repositorio (directorio en Internet).

Los Certificados Digitales utilizan técnicas de encriptación de clave pública. En un Certificado Digital, el par de claves corresponde al nombre del usuario y otra información de identificación. Instalado en un navegador Web, el Certificado Digital funciona como una credencial electrónica que el sitio Web puede verificar, permitiendo, tras el uso de una contraseña, el acceso a información o servicios restringidos a usuarios autorizados. La Autoridad de Certificación firma un

Certificado Digital emitido por dicha Autoridad. Los Certificados Digitales Múltiples pueden adjuntarse a un mensaje o transacción, formando una cadena de certificación, donde cada Certificado Digital testifica sobre la autenticidad del Certificado Digital anterior. El receptor debe conocer y confiar en la autoridad de certificación máxima.

4.6 Revocación

Del mismo modo que un documento de identidad personal o pasaporte puede ser robado, falsificado, perdido o, simplemente, expirar, un certificado digital puede dejar de ser válido por motivos idénticos o de otra índole. Los motivos de revocación pueden ser los siguientes:

- **Compromiso de la clave privada del usuario:** esto hace referencia a dos casos, que la clave privada caiga en manos de un atacante y este la use para suplantar al usuario o que el usuario olvide la contraseña que protege su clave privada, privándose así de su uso.
- **Compromiso de la clave privada de la AC:** este suceso es aún más grave pues el atacante podría suplantar a la propia autoridad de certificación, con consecuencias desastrosas. En cuanto la AC lo advirtiera, debería cambiar su clave invalidando todos los certificados reconocidos emitidos hasta ese momento. Las medidas de seguridad de la empresa de certificación son lo suficientemente estrictas como para que la probabilidad de este suceso sea prácticamente nula.
- **Cambio en los datos del certificado:** Los usuarios cambian de trabajo, lugar de residencia, dirección de correo, etc., motivos que pueden justificar la emisión de un nuevo certificado que refleje verazmente la nueva información personal del titular y la invalidación del certificado antiguo.
- **Violación de la política de la AC:** Si un usuario viola las normas de certificación de la AC, ésta puede decidir revocar su certificado.
- **Expiración del certificado:** los certificados tienen un tiempo de vida limitado y claramente especificado en sus datos, al final del cual dejan de ser válidos.

Revocación de un Certificado de Identidad Personal

La Autoridad de Certificación deberá revocar un Certificado Digital de Identidad Personal, a petición del suscriptor del mismo una vez que haya comprobado que la persona que realiza la solicitud de revocación es el suscriptor, sin ser preciso justificar la petición en modo alguno y siguiendo el protocolo que se describe a continuación:

- El solicitante de la credencial se apersonará ante el Agente de Registro asociado y presentará su documento de identidad personal, Pasaporte o Tarjeta de Residencia para que el agente verifique su autenticidad y vigencia.
- Confirmado esto, el Agente de Registro verificará la razonable coincidencia entre la fotografía contenida en aquellas y la apariencia física del solicitante.
- El Agente de Registro comprobará que el solicitante posee un certificado firmado por la CA a la que representa.
- A continuación, el Agente de Registro pedirá al solicitante que entregue y firme, en su presencia, un documento de solicitud de Revocación. Una vez firmado, el Agente de Registro comprobará la firma manuscrita de la solicitud con la que aparece en las credenciales oficiales presentadas, después procederá también a la firma y al sellado de la solicitud.
- El Agente de Registro enviará la solicitud de revocación a la Autoridad de Certificación para que la ejecute.

Revocación de un Certificado Digital de Servidor

La Autoridad de Certificación podrá revocar un Certificado Digital de Servidor siguiendo los siguientes pasos:

- El solicitante de la revocación será su responsable técnico y deberá disponer de una credencial de Identidad Personal emitida por la Autoridad de Certificación, inscrita bajo la Autoridad de Certificación principal de la institución u organismo donde se encuentra ubicado el servidor.
- El solicitante enviará a la Agencia de Registro de la CA, junto con una copia de su Credencial de Identidad Personal, una solicitud de revocación firmada

con su clave personal. Este envío se puede realizar a través de un mensaje de correo o un archivo firmado.

- El Agente de Registro procederá a verificar tanto la validez del Certificado de Identidad del solicitante como la firma que acompaña a la solicitud digital.
- Una vez verificado esto, el Agente de Registro enviará la solicitud de revocación a la Autoridad de Certificación para que la ejecute.

Revocación de un Certificado Digital de CA

La revocación de un Certificado Digital de CA firmado por la Autoridad de Certificación principal, se realizará siguiendo el protocolo siguiente:

- Será el responsable técnico directo de la Autoridad de Certificación inscrita bajo la Autoridad de Certificación principal el que solicitará a la Agencia de Registro de la AC la revocación del certificado.
- Para que dicha revocación se lleve a cabo, el responsable deberá hacer llegar a la Agencia de Registro, con la mayor brevedad posible, además del documento de solicitud, el código secreto emitido por la Agencia de Registro que aprobó la emisión de un Certificado Digital en favor de dicha CA.
- La Agencia de Registro comprobará que el código secreto corresponde con el emitido en su momento y si es así, procederá a enviar la solicitud de revocación a la Autoridad de Certificación para que ésta la ejecute.
- A partir de este momento, se consideran inválidos todos los certificados firmados por dicha CA, procediendo a la generación de un nuevo certificado y clave privada emitidos por la Autoridad de Certificación principal para todos los miembros de su comunidad.

4.7 Validez de los Certificados Digitales

Los certificados, debido a su naturaleza y al papel que desempeñan, no son documentos imperecederos al igual que el resto de documentos de autentificación de otros tipos, en primer lugar, al estar basados en el uso de claves no conviene que sean válidos por períodos de tiempo largos, ya que uno de los principales problemas del manejo de claves es cuanta más vida tienen más fácil es que alguien

se apodere de ellas, además, con el paso del tiempo los equipos informáticos van teniendo cada vez más poder de cálculo, por lo que conviene que cada cierto tiempo se vaya aumentando el tamaño de las claves criptográficas. Por este motivo los Certificados Digitales tienen estipulado un período de validez de un año.

En segundo lugar, es posible que convenga anularlo en un momento dado, bien porque se crea que las claves estén comprometidas, o porque la persona o entidad propietaria haya caído en quiebra o delito. Por lo que existe la posibilidad de revocar o anular un certificado y esta revocación puede llevarla a cabo el propietario del mismo, la Autoridad Certificadora o las autoridades judiciales.

Para llevar un control de los certificados revocados (no válidos) las Autoridades de Certificación han implementado unos servidores especiales que contienen bases de datos en las que figuran los certificados anulados, que se conocen con el nombre de Lista de Certificados Revocados, CRL. Un CRL es un archivo firmado por la Autoridad Certificadora, que contiene la fecha de emisión del mismo y una lista de certificados revocados, figurando para cada uno de ellos su número de identificación y la fecha en que ha sido revocado.

Ahora bien, en caso que se reciba un certificado como medio de autentificación en una transacción, el software de seguridad comprueba que no esta revocado en la última CRL y lo da por válido, pero resulta que al día siguiente aparece como revocado en la CRL nueva, para demostrar que se ha recibido el certificado antes de que se produjera la actualización, existen los documentos digitales denominados recibos.

Un recibo es un documento firmado digitalmente por una persona o entidad de confianza llamada Autoridad de Oficialía de Partes, que añade la fecha actual a los documentos que recibe para su certificación, firmando luego el resultado con su llave privada. De esta forma los usuarios disponen de un documento que atestigua la hora y fecha exacta en la que envía o recibe un Certificado Digital u otro documento electrónico cualquiera, así, disponemos de pruebas suficientes para considerar cualquier transacción realizada en base a

Certificados Digitales como segura, por lo menos en el sentido de Autenticación.

El uso de un CRL en el proceso de Autentificación presenta varios problemas adicionales. En primer lugar sólo se puede considerarlo válido cuando la fecha del mismo es igual o posterior a la que se quiere usar como referencia en la validez del documento, y en segundo lugar, también puede resultar inadecuado en aquellas operaciones que exijan velocidad alta en la transacción, sobre todo si el CRL por consultar tiene un tamaño muy grande.

La solución a estos problemas la dan los Servicios de Directorios o de Consulta de Certificados, servicios ofrecidos por personas o entidades de confianza aceptada, que al recibir una petición de validez de un certificado responde al instante si en esa fecha y hora concreta el mismo es válido o si por el contrario está revocado, en cuyo caso proporcionará también la fecha de revocación. Para dar validez a la respuesta, el Servicio de Directorios firma con su llave privada la misma, con lo que el usuario estará seguro de la Autenticidad de la respuesta recibida.

4.8 Responsabilidad en los Certificados Digitales

El poseedor del certificado es responsable de notificar variaciones en los datos certificados, pérdida del mismo, o cualquier otra posible incidencia que sólo conozca él mismo.

La Autoridad de Registro es responsable de realizar una identificación consistente y completa, seguir los trámites con fidelidad, y realizar las labores de revocación, modificación y renovación de manera correcta y fiel, siendo responsable directa de los datos que certifica.

La Autoridad de Certificación es responsable de emitir, con calidad técnica y de manera segura e irrepetible por otros medios o en otras circunstancias, el doble par de claves, pública y privada, que constituyen el eje del certificado. Además de poner a salvo su clave privada, garantizar la calidad técnica del

sistema informático y el libre y fácil acceso a las listas y directorios de claves públicas para la verificación de firmas emitidas por la misma.

4.9 Principales usos de los Certificados Digitales

- Los Bancos pueden entregar Certificados Digitales a sus clientes, tanto individuales como corporativos, para operar a través de Home Banking o Cash Management, reemplazando el esquema de user id y password basado en claves simétricas.
- Las Grandes Empresas pueden proveer a su personal Certificados Digitales como esquema de seguridad interna para ingresar a la intranet.
- Los Supermercados pueden brindar Certificados Digitales a sus cientos de proveedores para realizar pedidos y licitaciones en línea de forma segura a través de una extranet.
- Los Organismos Públicos pueden recibir declaraciones juradas o iniciar trámites vía Internet en base a solicitudes firmadas digitalmente por sus usuarios con Certificados Digitales.

4.10 Certificados SET

Certificados en SET

SET proporciona los mecanismos necesarios para que tanto consumidores como comerciantes se autentifiquen mutuamente antes de que la transacción tenga lugar, simulando que el cliente se encuentra físicamente delante del mostrador del vendedor a la hora de pagar la compra, utilizando certificados digitales, los mismos que sirven como documentos de identidad digitales que permiten verificar la identidad de una persona a través de una red de telecomunicaciones, similar a la firma en las tarjetas de crédito que atestigua que el signatario es el legítimo titular. Por su parte, los certificados emitidos a comerciantes equivalen a las etiquetas mostradas en los locales, en las que se informa de que Banco se acepta las tarjetas, además de dar fe de su identidad.

Los certificados son emitidos y gestionados por la misma entidad financiera o emisor de tarjetas de la que se recibió la tarjeta de pago. Se necesita un certificado distinto para cada marca diferente de tarjeta de crédito. Los certificados SET son emitidos por autoridades de certificación (AC) dentro de la jerarquía de certificación SET. Esta jerarquía asegura la autentificación válida de los participantes. Garantiza además la seguridad de los datos intercambiados entre titulares, comerciantes, bancos y pasarelas de pagos.

La autoridad raíz autentifica y emite certificados a las casas de medios de pago, cada una de las cuales se establece a su vez como autoridad de certificación para su marca y establece su pasarela de pagos como una AC, pudiendo así emitir certificados digitales para bancos adquirientes o procesadores de pago de terceras partes que actúan en representación de entidades adquirientes, de manera que estas puedan aceptar transacciones por Internet y convertirlas en mensajes que las redes privadas de pago pueden entender para procesar el pago.

Las AC de marcas de tarjetas autentifican y emiten certificados a sus bancos y entidades de crédito miembros, a las que establecen como autoridades de certificación. Las entidades adquirientes se transforman en AC de comerciantes, mientras que las entidades emisoras lo hacen en AC de titulares. Una vez transformada en AC de titular y/o comerciante, la entidad financiera puede autenticar y emitir certificados a sus clientes, sean estos particulares y/o comerciantes. De un modo general podría resumirse de la siguiente forma:

- Se consigue que la autentificación se extienda a todas las figuras implicadas en la transacción, pudiendo así verificar su identidad mutuamente.
- El grado de confidencialidad es mucho mayor pues la información está fuertemente cifrada para evitar fraudes.
- La integridad verifica que la información intercambiada no puede ser alterada intencionalmente, detecta incluso el cambio de un solo bit de información.

- Intimidad, con lo que las partes implicadas en la transacción sólo tendrán acceso a aquellas partes que les implique, manteniendo el resto oculto.
- La verificación inmediata de la disponibilidad del crédito e identidad del cliente al comerciante, antes de completarse la compra.
- Resolución de disputas con facilidad al ir asociadas las identidades de las partes.

Pero este sistema necesita de una serie de elementos:

- Un software de cartera del titular, programa que permite a los compradores almacenar y distribuir digitalmente sus órdenes de compra y medios de pago.
- Un software de punto de venta, programa TPV compatible con SET que acepte pedidos además de distribuir órdenes de pago en el circuito.
- Un software de pasarela de pagos que procese automáticamente los pagos, reciba peticiones de autorización/liquidación y los encamine a los sistemas tradicionales.
- Certificados. Todas las partes necesitan contar con los certificados electrónicos que garanticen la identidad de los participantes.

Certificados SET de Titular (Cardholder)

Los certificados de titular actúan como una representación electrónica de una tarjeta de crédito. Estos sólo pueden ser emitidos a propuesta de una entidad financiera de modo que no pueden ser alterados por una tercera parte. En el certificado los datos relativos al número de tarjeta y fecha de caducidad están codificados utilizando un algoritmo y no pueden ser derivados visualizando el certificado. El titular proporciona dicha información a la Pasarela de Pagos donde se verifica el certificado.

Mediante la solicitud de un certificado, un titular está indicando su intención de llevar a cabo operaciones de comercio electrónico. El certificado es transmitido a los comercios con la orden de compra y las instrucciones de pago encriptadas. Con la recepción del certificado de titular, el comercio puede estar seguro como mínimo, de que el número de tarjeta ha sido validado por una entidad financiera emisora. Un titular puede solicitar tantos certificados como tarjetas de crédito/débito disponga, quedando asociado cada uno a la tarjeta correspondiente.

El software utilizado por el titular para almacenar sus certificados y comunicarse con el comercio se denomina Electronic Wallet o cartera electrónica. Este software, integrado en el navegador de Internet que utilice el titular, le permitirá además almacenar la información sobre transacciones efectuadas a lo largo del tiempo. Dicho software es proporcionado por la entidad financiera.

Certificados SET de Comercio (Merchant)

Estos certificados son un sustituto de logotipos de las marcas de tarjetas de crédito que se muestran en cristaleras de los comercios. Estos logotipos indican que el comercio posee una relación con una entidad financiera que le permite aceptar pagos a través de tarjetas de crédito. Dichos certificados son aprobados por la entidad financiera adquirente y aseguran que existe un acuerdo válido entre ambas partes. Un comercio debe disponer de un certificado para cada marca de tarjeta que acepte.

El comercio necesita instalar en su servidor un software gestor o software de Merchant de transacciones comerciales a través de redes abiertas y compatible con cualquier red de proceso de pagos que soporte la especificación SET independientemente del proveedor. Dicho software gestionará los certificados del comercio y todos los procesos de encriptación, direccionamiento, desencriptación, manejo de claves públicas y privadas y comunicaciones con la pasarela de pagos de forma automática. El software necesario es proporcionado por la propia entidad financiera.

Certificados SET de Pasarela de Pagos (Payment Gateway)

Los certificados de pasarela de pagos son emitidos a los adquirientes y sus procesadores de transacciones (operador de medio de pago) y se aplican a los sistemas que procesan autorizaciones y capturan mensajes. Dichos certificados residen en la infraestructura de pasarela de pago y realizan las validaciones de los certificados de titular y comercio que reciben. Una vez que la pasarela autoriza la operación, ésta devuelve la autorización al comercio. La validez y garantías de los certificados SET residen en la jerarquía de confianza que los soporta.

Cada certificado está relacionado con la entidad que los firmó digitalmente. Mediante el seguimiento del árbol de confianza hasta una tercera parte confiable (TTP) conocida, se puede estar seguro de que el certificado es válido. Por ejemplo, un certificado de titular está relacionado con el certificado del emisor el cual a su vez está relacionado con la Marca a la que pertenece la tarjeta del titular. La clave pública raíz o clave pública de Marca es conocida por todos los software SET y podrá ser utilizado para verificar todos los certificados que se encuentran por debajo de él. La clave raíz es distribuida a través de un certificado autofirmado. Esta clave va incluida en el software distribuido por los proveedores de software SET, confirmando que posee una clave raíz válida mediante una consulta a la Autoridad de Certificación.

4.11 Servicios de Autenticación

Tanto las personas como las instituciones necesitan conocerse antes de realizar negocios, por esto, las nociones de identidad y autenticación, son conceptos fundamentales en cualquier negocio. En el comercio electrónico se requiere la utilización de métodos para el establecimiento de identidades, de sistemas de pago y de mecanismos de resolución de disputas legales similares a los tradicionales. Los servicios de, Autenticación, Pago, y Validación, proporcionan una infraestructura digital de confianza para el negocio electrónico. Los Servicios de Autentificación proporcionan los fundamentos necesarios para establecer identidades y crear relaciones de confianza en el mundo digital.

Independientemente de si el comercio se realiza en línea o en el mundo físico, las partes involucradas deben de contestar a estas preguntas: ¿Quién eres?, ¿A qué comunidad perteneces? ¿Eres miembro de confianza? ¿Cómo puedes probar tu identidad?, es decir, cualquier persona que desee realizar comercio electrónico debe establecer su identidad y presentar credenciales que la prueben. Asimismo, debe ser administrado el ciclo de vida y la presentación de credenciales. Finalmente, las credenciales deben ser accesibles a las partes involucradas en cualquier tipo de directorio. Los servicios de autentificación utilizan estos aspectos para establecer un negocio electrónico de confianza.

Si sus aplicaciones son seguras para la captura de órdenes de tarjetas de crédito, seguridad B2B, redes VPN, firma de códigos de software, seguridad internacional, e-mail seguro, redes de radiofrecuencia u otro aspecto sobre la seguridad en la red, los servicios de autentificación proporcionan la infraestructura digital global necesaria para comerciar en el mundo digital.

Autenticación

Para entender con detenimiento los servicios de autentificación es necesario comprender cada una de las siguientes áreas:

- Establecer la identidad: Antes de realizar transacciones debe establecerse la identidad de las partes. En toda transacción, las empresas deben evaluar los niveles de esfuerzo y la asunción de riesgos asociados con el establecimiento de una identidad. En el nivel más básico, debe existir un proceso que verifique que la empresa o individuo existen, tienen nombre, y son auténticamente legales. Las Terceras partes confiables o autoridades delegadas tienen el papel de respaldar la identidad de las personas que participan en el momento en el que la identificación se realiza.
- Administración de credenciales: Una vez que la identificación se establece y verifica, se puede emitir una credencial, la credencial más completa es el certificado digital. Una vez que los certificados se encuentran en su sitio, se pueden identificar socios de negocios, proveedores y clientes, consultando los certificados o buscándolos en sitios Web. Los certificados digitales crean el armazón técnico para que no se puedan repudiar las transacciones a la vez que generan registros de transacciones firmadas digitalmente.
- Validación de la identidad: Una vez que el usuario ha sido identificado y posee una credencial, está preparado para realizar negocios. En este momento le será requerida su identidad, esto es su autenticación. Este proceso requiere que la aplicación pregunte al usuario por la credencial, la verifique y una vez validada proporcione el acceso.
- Catálogo de Servicios: A diferencia del nombre de usuario y del password, los certificados digitales pueden ser tratados como credenciales públicas, es

decir, pueden ser compartidos en un directorio utilizado para realizar intercambios comerciales. Este directorio debe soportar tanto atributos públicos como privados, y permitir a los usuarios manipular de forma segura su información.

Entornos de Autentificación Típicos

Mientras que identificar y autenticar es fundamental para todo tipo de comercio electrónico, cada cliente asociado puede tener necesidades diferentes dependiendo de su entorno.

- Empresas con Intranet: Normalmente, las empresas usan intranets privadas para facilitar las comunicaciones internas entre sus empleados, para administrar reportes de gastos o peticiones del personal. Todos los usuarios son conocidos por la empresa y estos deben seguir sus reglas. Debido a que los usuarios son pocos y bien conocidos, la autentificación puede realizarse en conexión con procesos establecidos y con fuentes de datos internas de la empresa.
- Empresas con B2B Extranet: Las empresas añaden extranets B2B para generar valor añadido a sus relaciones con clientes, socios o proveedores. Por ejemplo, un fabricante puede usar una extranet para comunicarse con sus plantas de producción. Aquí, la clave está en la eficiencia y la reducción de costos. La mayoría de usuarios son conocidos por la empresa y mientras no se requiera seguir las reglas al pie de la letra están altamente motivados para hacerlo.
- Empresas con B2C Extranet: Las empresas que emplean extranets B2C ofrecen servicios a los consumidores en Internet. Por ejemplo, bancos on line, o corredurías de servicios en línea. Aquí, la clave consiste en la satisfacción de los clientes. Específicamente, las empresas desean establecer la identidad de nuevos clientes, clientes desconocidos, con la menor fricción posible. Esto significa que mientras los actuales usuarios son conocidos para la empresa, por definición, la mayoría de sus potenciales usuarios son desconocidos. En este escenario, la autentificación de los clientes existentes se hace usando passwords después de haber sido examinado por un proceso del propio banco. Por lo tanto, el desafío radica en identificar a los nuevos clientes.

- Comercio electrónico B2B en mercados electrónicos: El comercio electrónico entre empresas en mercados electrónicos une negocios entre clientes y proveedores. Aquí la clave consiste en incrementar el volumen de transacciones añadiendo cuantos más compradores y proveedores cualificados, y reducir el riesgo, compartiendo con terceras partes las responsabilidades cuando sea posible. La alta convicción en la verificación de identidades, la identificación de atributos y una tercera parte imparcial evalúa a los usuarios clave.
- Comercio electrónico B2C en mercados electrónicos: El comercio electrónico entre empresas y consumidores en mercados electrónicos junta al consumidor, al comprador y al proveedor. El mejor ejemplo son sitios de subastas para consumidores como eBay. La clave consiste en reducir el fraude identificando individualmente a los usuarios e impidiendo el acceso a los que se encubren en una falsa identidad.

5. Conclusiones

Los certificados digitales son la carta de presentación de la empresa en la cual estamos yendo a realizar la transacción, estos pueden ser SSL o SET dependiendo de la misma, para prestación de servicios se puede usar los certificados SSL y para compras en línea se usan los certificados SET pues dan mayor seguridad para la pasarela de pagos, los certificados SET emitidos por un AC son el soporte electrónico mediante el cual se genera la firma digital y el cifrado de la información de acuerdo con el protocolo SET. Cada participante en la transacción comercial electrónica debe disponer de su certificado SET.

CAPITULO 4: DESARROLLO DE LA PRÁCTICA

1. Introducción

Esta práctica consiste en simular un Web Banking, y se ha desarrollado para demostrar la seguridad en el comercio electrónico mediante el uso de certificados digitales, para esto se utilizaron varias herramientas, como son el servidor Web Apache, la Base de Datos MySQL, el gestor de certificados digitales Openssl y Macromedia Dreamweaver, los mismo que detallaré más adelante. Además para la demostración del cifrado utilizaré un programa sniffer, el mismo que es el Ethereal.

1.1 Instalación

Para el desarrollo de esta práctica se instalaron 4 programas básicos:

- Apache2triad1.5.4: es una distribución de software del tipo WAMP (acrónimo usado para describir un sistema de infraestructura de Internet que usa **W**indows, **A**pache, **M**ySQL y **P**erl, **P**HP, o **P**ython) que integra algunos de los servidores y de los intérpretes de código libre más populares para desarrollar en un entorno Web y proporcionar un webhosting, el contenido de esta versión es el siguiente: como servidores (Apache 2, MySQL, PostgreSQL, XMail, SlimFTPd), como intérpretes **(**PHP 5, Perl, Python) y las interfaces gráficas de usuario (el Panel de Control A2tmanager, las GUI para MySQL, PostgreSQL, SQLite, XMail y SlimFTPd, el webserver monitor AWStats y el cliente de correo electrónico UebiMiau.

  Apache2triad se puede llamar un sistema de infraestructura de Internet, porque contiene todos los servidores, intérpretes, e interfaces de usuarios ya configurados y listos para ser utilizados, además el modulo ssl incorporados.

4.1.1 Panel de Control de A2tManager

- Openssl: es un proyecto de software desarrollado por los miembros de la comunidad Open Source para libre descarga y está basado en SSLeay desarrollado por Eric Young y Tim Hudson. Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a navegadores Web (para acceso seguro a sitios HTTPS). Estas herramientas ayudan al sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad , como el Transport Layer Security (TLS), fue necesaria la instalación de este software porque nos permite crear certificados digitales para aplicarlos a nuestro servidor.

4.1.2 Icono de Openssl

- Macromedia Dreamweaver 8: es un editor WYSIWYG (**W**hat **Y**ou **S**ee **I**s **W**hat **Y**ou **G**et) de páginas web, creado por Macromedia (actualmente Adobe Systems). Es el programa de este tipo más utilizado en el sector del diseño y la programación Web, por sus funcionalidades, su integración con otras

herramientas como Macromedia Flash y, recientemente, por su soporte de los estándares del World Wide Web Consortium.

4.1.3 Icono de Macromedia Dreamweaver

- Ethereal: es un potente analizador libre de protocolos de redes, permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco, se destaca por su impresionante soporte de más de 300 protocolos, gracias sin duda a la licencia GPL y sus más de 200 colaboradores de todo el mundo.

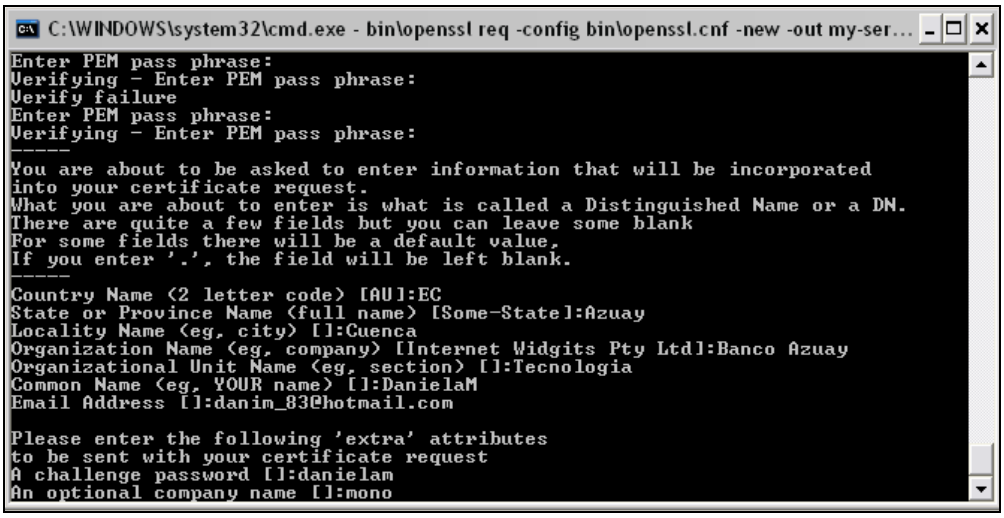
4.1.4 Icono de Ethereal

1.2 Creación de un Certificado Digital

Una vez instaladas todas las herramientas anteriormente descritas, procedí a probar que los servidores Apache2 y Apache2SSL estén corriendo sin problemas escribiendo en la barra de direcciones de mi navegador las direcciones http://localhost y https://localhost respectivamente, comprobando así que todo funcionaba correctamente, en el caso de Apache2SSL, el navegador me mostró una ventana de aceptación o denegación de un certificado digital instalado con el Apache2triad.

Para ir probando mi servidor seguro, creé un certificado digital con los datos de mi Banco, el mismo que se llama Banco Azuay, para esto utilicé el Openssl, con los siguientes comandos:

- bin\openssl req -config bin\openssl.cnf -new -out my-server.csr
  Para la creación de este archivo se pide una contraseña, cuanto más larga sea la frase, mejor, además se pide información de la empresa para la cual se creará el certificado, el país, etc., como se muestra en el siguiente cuadro:



4.1.5 Comandos de creación de un Certificado Digital con Openssl

- bin\openssl genrsa -out privkey.pem 2048

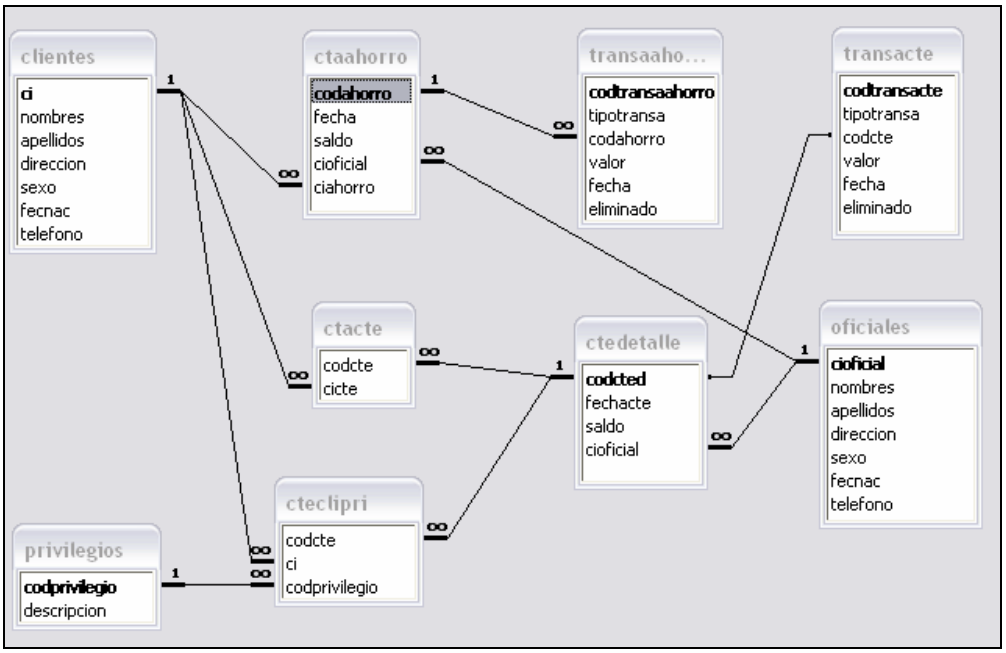
  Este comando se utiliza para crear privkey.pem
- bin\openssl rsa -in privkey.pem -out my-server.key
- bin\openssl x509 -in my-server.csr -out my-server.cert -req -signkey my-server.key -days 4000

  Esto creará un certificado que expirará en 4000 días.
- bin\openssl x509 -in my-server.cert -out my-server.der.crt -outform DER

Estos comandos crearán algunos archivos en la carpeta actual (my-server.der.crt, my-server.csr, my-server.key, .rnd, privkey.pem, my-server.cert), luego se copian los archivos server.der.crt y privkey.pem en la carpeta C:\apache2triad\opssl\cert cambiando el nombre de server.der.crt por certificate.crt, para no cambiar la configuración por defecto en el ssl.conf, así logramos que mi servidor seguro me muestre mi certificado digital.

1.3 Desarrollo del Web Banking

El Web Banking de esta práctica contiene consultas de saldos y transferencias entre cuentas del mismo Banco, para su desarrollo, se creó una base de datos utilizando la herramienta MySQLAdministrator, con las siguientes relaciones:



4.1.6 Relaciones de la DB utilizada en el Web Banking

Para el desarrollo del sitio Web, se utilizó la herramienta de Macromedia Dreamweaver 8, utilizando el lenguaje php y aplicaciones flash para su funcionamiento y apariencia.

1.4 Prueba de Certificado Trial de Verisign

Para poder obtener el certificado Trial de Verisign necesitamos un Certificate Signing Request (CSR), el mismo que ya generamos con el Openssl, en este caso es el archivo my-server.cert, lo abrimos con el Block de Notas y lo copiamos al momento que Verisign nos lo pida, debemos asegurarnos de poner los mismos datos para no tener problemas con la clave que creamos anteriormente, privkey.pem.

Verisign nos envía un correo electrónico al e-mail que le proporcionamos, en el cual nos manda el certificado digital firmado por ellos, el mismo que debemos guardarlo con la extensión .cer, como en esta configuración, el certificado utilizado es .crt, el contenido del nuevo certificado lo guardamos en el mismo formato que el archivo my-server.cert, y con la extensión .cert, luego repetimos el comando del Openssl: bin\openssl x509 -in nuevo.cert -out certificate.der.crt -outform DER y así obtenemos nuestro certificado firmado por Verisign, para probarlo lo copiamos con

el nombre certificate.crt a C:\apache2triad\opssl\cert y podremos ver la jerarquía del mismo.

1.5 Demostración con el Ethereal

Se desarrollaron dos páginas Web para el ingreso de claves de usuarios al Web Banking, la primer accederá por el protocolo general http:// y la segunda por el protocolo https://. Se realizaron capturas de los dos tipos de ingreso demostrando así el cifrado de datos con el protocolo SSL.

2. Conclusiones

Al desarrollar esta práctica, se puede llegar a la conclusión, de que sin importar la plataforma en la cual se esta trabajando, sea esta Windows o Linux, el montar un servidor seguro no es una tarea demasiado complicada, sólo es cuestión de investigar un poco y ponerlo en práctica, los costos del mismo, son completamente justificables pues la información es el activo más importante de toda empresa comercial, al hablar de costos en esta práctica me refiero a la compra del certificado digital.

Creo que debe quedar claro además que un certificado de clave pública es una información disponible públicamente, y no se necesita emplear medidas de seguridad específicas con respecto a su transporte al directorio del servidor. Como éste es producido por una autoridad de certificación fuera de línea a nombre de un usuario que recibirá una copia del mismo, el usuario necesita solamente almacenar esta información siguiendo la configuración de su servidor.

CONCLUSIONES

Con todo lo investigado y practicado podemos concluir que si es posible tener un canal de comunicaciones seguro y que es lo primordial para ganar la confianza del cliente y brindarle calidad, seguridad y comodidad al momento de hacer compras, consultas o transferencias que necesiten datos personales y números de tarjetas de crédito o dinero digital, pues la protección de la información debe entenderse como una preocupación de primera importancia en la organización, ya que de esta dependemos, por eso es necesario tener todas las medidas pertinentes para evitar fallas, ataques y fraudes.

La seguridad debe ser parte primordial de la infraestructura tecnológica de un sitio de comercio electrónico pues en esta se basa el éxito o fracaso del mismo, para esto debemos contar con un buen firewall, y mantener un servidor manejado con el protocolo SSL y SET para la pasarela de pagos, si es requerida, además de contar con un certificado digital firmado correctamente por una CA de confianza y antes de ser aceptado, verificarlo en el CRL, para estar seguros de su vigencia y de que como clientes estamos intercambiando información con el servidor correcto y no con un intruso disfrazado

Gracias a la UIT (International Telecommunications Union), varios países en desarrollo han sido acreditados para proporcionar servicios de seguridad y confianza usando certificación digital y firmas digitales, algunos de ellos son: Ecuador (CORPECE), Perú, Turquía, etc., además se puede afirmar que la competitividad no se consigue con la sola apertura de las economías al mercado internacional, a la inversión y a la tecnología o con la reducción de los salarios, sino mediante la creación de capacidades para el uso de las nuevas tecnologías para lo cual los países tienen que adquirir conocimientos, aptitudes y prácticas específicas para las empresas.

BIBLIOGRAFÍA

- **Asegurando el servidor con SSL**
  http://tortoisesvn.net/docs/release/TortoiseSVN_es/tsvn-serversetup.html
  14-03-07 - 16:20
- **Certificados de prueba de e-sign**
  https://digitalid.e-sign.cl/trial/trialserver/index.html
  27-03-07 - 15:00
- **Certificados digitales**
  http://www.microsoft.com/technet/prodtechnol/exchange/ES/Guides/E2k3MsgSecGuide/b26b91d9-d569-4d1f-914f-2d7027e2cb16.mspx?mfr=true
  04-03-07 - 11:27
- **CORPECE**
  http://www.corpece.org.ec/
  17-02-07 - 15:00
- **Criptografía**
  http://es.wikipedia.org/wiki/Criptograf%C3%ADa
  27-02-07 - 21:25
- **Del comercio electrónico a la administración electrónica: tecnologías y metodologías para la gestión de información**
  http://www.uoc.edu/dt/20204/index.html
  11-01-07 - 14:30
- **e-Seguridad seguridad en la red**
  http://www.wikilearning.com/el_certificado_digital-wkccp-3270-1.htm
  23-01-07 - 14:20
- **Guía Corporativa VeriSign**
  http://www.verisign.com/latinamerica/esp/static/034837.pdf
  11-01-07 - 13:00
- **Instalar un servidor seguro**
  http://raibledesigns.com/wiki/Wiki.jsp?page=ApacheSSL
  12-03-07 - 17:30
- **Seguridad en la Web**
  http://www.iec.csic.es/criptonomicon/seguridad/servicio.html
  24-01-07 - 13:00
- **Seguridades en redes**
  http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml
  11-01-07 - 14:00