# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA


# MECANISMOS DE SEGURIDAD EN EL COMERCIO ELECTRONICO

**INFORME DE SUFICIENCIA**

PARA OPTAR EL TÍTULO PROFESIONAL DE:

**INGENIERO ELECTRÓNICO**

**PRESETADO POR:**

FRITZ ROY MALDONADO NUÑEZ

**PROMOCIÓN**

**2002 - I**

**LIMA - PERÚ**

**2007**

# MECANISMO DE SEGURIDAD EN EL COMERCIO ELECTRONICO

*Dedicó este trabajo a mis padres*
*Otilio y Estela, fuente de inspiración y*
*a mis hermanos por su continuo apoyo.*

# SUMARIO

Las redes mundiales de información están transformando al mundo y acercando más a la gente a través de la innovación de las comunicaciones mundiales, lo cual posibilita cambios en todos los ámbitos de la actividad humana, por ejemplo la competitividad, el empleo y la calidad de vida de las naciones. Con las nuevas tecnologías, el tiempo y la distancia dejan de ser obstáculos, los contenidos pueden dirigirse a una audiencia masiva o a un pequeño grupo de expertos y buscar un alcance mundial o meramente local. Las redes mundiales de información, como Internet no conoce fronteras.

La rápida difusión y el gran interés en el mundo de la informática, ha permitido la creación de tecnología Internet/Web, una herramienta fundamental para redes de computadoras y sus usuarios. Internet ofrece un nuevo mercado que define la "economía digital". Los productores, proveedores de bienes/servicios y usuarios logran tener acceso y transmisión mundial de la información y esparcimiento en forma sencilla y económica, sean con fines comerciales o sociales. La apertura de mercados es fundamental para el rápido crecimiento del uso de nuevos servicios y la asimilación de tecnologías nuevas. En la práctica, las empresas están comenzando a usar Internet como un nuevo canal de ventas, sustituyendo las visitas personales, correo y teléfono por pedidos electrónicos, ya que gestionar un pedido por Internet cuesta 5% menos que hacerlo por vías tradicionales. Nace entonces el comercio electrónico, como una alternativa de reducción de costos y una herramienta fundamental en el desempeño empresarial.

# INDICE

# PROLOGO

La Internet rápidamente ha ganado aceptación como medio de mercadeo y distribución para una amplia variedad de negocios, ya que provee una plataforma barata para la negociación y el intercambio de servicios, información y bienes a consumidores. Existe un incremento de organizaciones que han tomado la Internet como medio de reducir costos y extenderse. El comercio electrónico es un servicio de la tecnología que permite la realización de operaciones de negocios y la compraventa de bienes y servicios mediante la utilización de sistemas electrónicos.

Sin embargo, la seguridad representa una barrera para el comercio electrónico en la Internet. La habilidad de enviar y recibir datos seguros es un requerimiento fundamental. En un medio tan inseguro es necesario un mecanismo que prevenga los accesos no autorizados a los datos intercambiados por los usuarios, tales como información de tarjetas de crédito y cuentas. Aunado a esto, en este ambiente anónimo, los negocios y las organizaciones necesitan un medio para establecer su identidad y credibilidad para protegerse a sí mismas y a sus clientes de impostores.

En el panorama actual de Internet existen dos tipos de negocios: los que se sirven de la Red, como de un mero escaparate virtual en el que anunciar sus productos y servicios, y los que utilizan mecanismos web para además vender esos productos. Por supuesto, la ventaja competitiva de estas empresas es muy superior a la de las primeras: su comercio, no sólo su catálogo, está disponible las 24 horas del día, siete días a la semana, accesible a un mercado potencialmente mundial. En contrapartida, también la complejidad de gestión de pagos a la que se enfrentan es mucho mayor. Como cualquier otro canal de distribución, la Red plantea un conjunto único de retos de seguridad que deben afrontarse racionalmente para minimizar el riesgo y ofrecer una confianza sólida a los actores de las relaciones telemáticas que no se conocen entre ellos, tanto en el business-to-business entre empresas, como en el comercio al por menor entre vendedores y compradores particulares.

# CAPITULO I

# CONSIDERACIONES A TENER SOBRE SEGURIDAD

## 1.1 Riesgos y Ataques en Internet

Para entender los distintos riesgos que podemos tener en Internet, es necesario revisar los diferentes elementos de infraestructura que están involucrados.

- ***Navegador o browser***. Es un programa básico para que los usuarios interactúen en Internet a través de una interfaz gráfica (GUI) hacia los distintos tipos de servidores de Web. Actualmente, los dos principales browsers en el mercado son el Netscape Navigator y el Microsoft Explorer.
- ***Web Server***. Es el servidor que ejecuta el servicio **WWW (World Wide Web)** y que puede establecer sesiones con los browsers de diversos usuarios. Éstos pueden estar en Internet o en una Intranet y establecen conexiones con el Web Server, conversando a través de HTML que a su vez viaja en el protocolo HTTP (utilizando conexiones TCP regularmente a través del puerto 80). De acuerdo al sistema operativo, existen varias marcas de servidores Web.
- ***ISP*** **(Internet Service Provider; Proveedor de servicios de Internet)**. Cada una de las empresas que se encarga de establecer la conexión entre los usuarios –empresas, universidades y usuarios individuales– y el resto de Internet.
- ***NAP*** **(Network Access Point; Punto de acceso a la red).** Puntos de concentración de tráfico, típicamente puntos de unión entre las redes de varios ISPs.
- ***Router*** **o** ***enrutador***. Dispositivo físico que se encarga de determinar la ruta que tomarán los paquetes. Trabaja a nivel de capa 3.
- ***Enlace a Internet***. Es el enlace que se establece entre los usuarios de Internet y el ISP. Este enlace puede ser de distintos tipos: enlace de marcado o dial-up

usando módems tradicionales, enlaces vía cable módem, RDSI (Red digital de servicios integrados), xDSL (Digital Subscriber Line; Línea digital del usuario), líneas T1, E1 o fracciones de ésta (dependiendo del país en donde nos encontremos), e incluso líneas de mayor velocidad (T3 o similares).

- ***HTML* (HyperText Markup Language; Lenguaje de marcado de hipertexto)**. Es el lenguaje con el que se describen las páginas Web.
- ***HTML Form***. La manera más común de generar páginas dinámicas para dar entrada o desplegar datos variables.
- ***HTTP* (HyperText Transfer Protocol; Protocolo de transferencia de hipertexto).** Protocolo que usa el servicio WWW.
- **CGIs (Common Gateway Interface; Interfaz común de puerta de enlace**). Una de las maneras de "invocar" programas externos desde HTML.
- ***Código móvil***. Programas, componentes o rutinas de programación que se ejecutan en alguno de los elementos (en el navegador del lado del cliente, en el servidor Web o en algún otro servidor). Este código puede estar escrito en lenguaje Java (denominándose scripts, applets o servlets, dependiendo de sus características y en dónde corren) o en algún lenguaje de Microsoft (denominados controles ActiveX y páginas ASP).
- ***HTTP-S***. Forma segura del protocolo HTTP. Se monta sobre los servicios de SSL (Secure Sockets Layer; Capa de zócalos seguros).
- ***SSL***. Protocolo que brinda seguridad a los servicios que usan TCP (Transmission Control Protocol; Protocolo de control de transmisión). Al servicio que usa SSL, se le deberá agregar una S al final: HTTP-S, Telnet-S, FTP-S, etcétera.

### 1.1.1 Principales Riesgos de Internet

**a) Espionaje o alteración de mensajes que viajan en Internet**. Usando analizadores de protocolos o accediendo de forma no autorizada a servidores de correo (tanto los finales, como los que tienen los ISPs), un atacante podría espiar e incluso alterar dichos mensajes.

**b) Entrada no autorizada a algún equipo o aplicación para modificar páginas Web.** Este es uno de los ataques más comunes y vistosos. Aprovechando huecos en la programación o en la configuración del Web Server (incluyendo el sistema operativo), el atacante logra modificar el contenido de las páginas HTML. Aquí el impacto se refiere más a la imagen de la organización que a un posible robo de información.

**c) Espiar, robar o alterar información en bases de datos.** Es común que las aplicaciones transaccionales de Internet utilicen uno o más servidores de bases de datos, de ahí que exista el riesgo de que alguna persona no autorizada tenga acceso y/o modifique esos datos.

**d) Realizar transacciones fraudulentas o alterar transacciones válidas.** Son ya muy comunes distintos sitios Web en donde es posible ejecutar transacciones, desde una simple compra (con o sin pago electrónico) o una compra/venta de acciones, hasta cuantiosas transferencias de dinero de las cuentas de una empresa a la de sus proveedores.

**e) Recepción de virus y caballos de Troya vía anexos del e-mail.** Este riesgo se refiere a que un usuario reciba un e-mail que contiene anexos aparentemente interesantes. Al abrir dichos anexos, se instala algún tipo de programa malicioso.

En los ejemplos más conocidos (los virus Melissa y I Love You), el atacante explota vulnerabilidades específicas asociadas con Outlook de Microsoft (ejecución de macros y de Visual Basic Script). Es importante mencionar que en algunos casos (como I Love You) el virus no sólo causa que el mismo e-mail se reenvíe a otros usuarios de nuestra lista de correos, sino que trata de instalar un caballo de Troya que roba passwords y los envía a una dirección externa. En otros casos el único propósito del anexo malicioso es instalar un caballo de Troya en la PC para abrir una conexión externa (usando un puerto de TCP) con el equipo del hacker, logrando que desde esta máquina se tome el control remoto de la PC. Los ejemplos más comunes de caballos de Troya son Back-Orifice (versiones para Windows 95/98 y Windows NT) y NetBus.

**f) Ejecución de código malicioso en la PC.** Además de las formas anteriores (virus y caballos de Troya), cuando un usuario está visitando páginas Web es posible que su navegador descargue código móvil desde el servidor Web hacia su navegador. En este caso, el usuario no sólo estaría "navegando" por la página, sino que estaría ejecutando en su PC rutinas de programación hechas en Java o algún otro lenguaje. Es posible que dichos programas hayan sido escritos con mala intención y que realicen operaciones maliciosas (como borrar o formatear el disco duro).

**g) Caída del servicio**. Por alguna razón, el acceso a un servicio de nuestro sitio de Internet queda temporalmente bloqueado o con tiempos de respuesta tan largos que es inoperable.

**h) Realización de ataques a otros sitios "vecinos" desde nuestro sistema (personal nuestro o ataques "implantados).** Es un riesgo real, sobre todo en grandes empresas, que alguna persona realice ataques a otros sitios de Internet desde nuestra propia red.

**i) Malos Usuarios** que envían información crítica a competidores y fuentes no autorizadas. Un riesgo que aumenta con el uso de Internet es tener usuarios enviando información crítica o sensible a otras partes de la Red. Usando servicios como ftp e incluso enviando anexos en un e-mail, es muy sencillo transmitir esta información hacia el exterior.

**j) Desperdicio y mal uso de recursos tales como e-mail y navegadores Web.** Ante la falta de políticas y lineamientos claros, los usuarios de correo electrónico y quienes tienen acceso a Internet, frecuentemente hacen un uso inadecuado de los mismos enviando a cientos de usuarios e-mails con contenidos sexuales, religiosos, violentos, políticos o de otros temas muy ajenos a los del negocio.

### 1.1.2 Principales Formas de Ataque

Aunque existen diversas definiciones de hacker y varias palabras para referirse a los distintos tipos de ciberpiratas (hackers si no tienen motivos criminales, crackers si los tienen, phreaks si son especialistas en "jugar" con la infraestructura telefónica, etcétera), lo cierto es que si el objetivo es protegernos, poco ayudan las distintas categorías.

Es importante entender las distintas formas de ataque para prevenirnos de ellas adecuadamente. Y aunque no podemos ilustrar en unos cuantos párrafos las diferentes técnicas y métodos (o sus variantes) que usan los hackers para atacar, citaremos algunos puntos que son muy frecuentes en sus ataques:

**a) Averiguar información vía telefónica.** Esta técnica, conocida como "ingeniería social", es la utilización de preguntas inteligentes hechas en forma amable a las personas adecuadas, haciéndose pasar por otra persona para obtener algún tipo de información.

Por ejemplo, un hacker averigua que José Luis es el nombre de un especialista de soporte técnico de su empresa. El viernes por la tarde le llama por teléfono a varios usuarios y se hace pasar por José Luis, comentándoles que el fin de semana hará ajustes a la red. Ante la queja –casi universal– de los usuarios, él les propone que para evitar cualquier contratiempo, el departamento de soporte técnico está dispuesto a probar cada una de las cuentas de los usuarios para asegurarse que todo estará bien el

domingo por la noche. "José Luis" realiza todos los cambios con el compromiso de los usuarios de modificar sus passwords inmediatamente después. Si el hacker ha hecho todo esto de forma amable y segura, ¿no caerían en el truco muchos usuarios y estarían más que dispuestos a darle su password a un supuesto "amigo"?

**b) Realizar una radiografía de la red.** Existen muchas herramientas de dominio público que permiten –con una conexión de Internet– analizar nuestra red y dar información valiosa (direcciones de servidores, servicios que prestan, configuración de los mismos, etcétera). Entre estas herramientas se encuentran el famoso ping (que hace pings por rangos) y traceroute (para saber por dónde pasan los paquetes y así "descubrir" los routers de la red). También existen otros comandos más poderosos como NMAP, o un sinfín de utilerías gratuitas y otras más costosas. Tal es el caso de Satán (gratuita, bajada desde Internet) o Internet Scanner (una de las herramientas más poderosas que no es gratuita).

**c) Averiguar passwords.** Existen también muchas herramientas de dominio público para averiguar passwords. Una vez que se conoce el tipo de equipo que tenemos, es más factible realizar este tipo de ataque y entrar a nuestros equipos incluso con claves "privilegiadas". Normalmente estas herramientas se basan en la copia del password file, aunque existen variantes que incluso pueden interceptar dichos passwords cuando viajan en la red (sobre todo en la red local o LAN).

En la mayoría de los sistemas operativos los passwords se guardan encriptados; sin embargo, las herramientas tratan de descubrirlos utilizando una lista de palabras, encriptando cada una de ellas y viendo si existe match entre la palabra encriptada y alguno de los passwords que se tienen. La lista de palabras puede ser un diccionario de términos comunes que la gente usa para sus passwords (distinta de acuerdo al país y al lenguaje), o bien puede deducirse de diversas combinaciones hechas con los nombres de usuarios (login names). También puede ser generada por fuerza bruta (se prueban todas las combinaciones posibles).

Las herramientas más comunes para realizar las tareas anteriores son: l0pht-crack en el caso de servidores Windows-NT, y John the Ripper para equipos Unix. No hay que olvidar que los routers también manejan passwords y desafortunadamente a veces sucede que las empresas no modifican los nombres de usuario y passwords por omisión, lo que hace más fácil que un usuario entre al router sin autorización, e incluso pueda reconfigurarlo.

**d) Averiguar "huecos" de seguridad (vulnerabilidades) en sistemas operativos y servicios que se están ejecutando en nuestras máquinas.** En Internet están "bibliotecas" completas que relacionan todos los huecos de seguridad para un ambiente en particular e incluyen los programas (exploits) que explotan dichos huecos. Si no hemos instalado todas las actualizaciones y "parches" de seguridad sobre nuestros equipos, los hackers pueden tomar ventaja de esos huecos y entrar fácilmente a ellos.

**e) Aprovecharse de páginas Web (código HTML) con diferentes huecos de seguridad.** Una de las maneras comunes de penetrar un sistema –o por lo menos inhabilitarlo– es realizando algunos trucos en las formas HTML. Por ejemplo, es común que el programador que definió una forma HTML no se asegure que la información que el usuario ha escrito para llenar en un campo, no incluya caracteres especiales o esté fuera de especificaciones. ¿La consecuencia? Un atacante puede introducir información inválida y ocasionar que se caiga el servidor (debido a un buffer overflow). En algunos casos la explotación de este tipo de huecos puede incluso darle acceso privilegiado (root o administrador) al atacante.

**f) Ejecución de ataques específicos** (además de los exploits mencionados anteriormente). Existe varios ataques conocidos que explotan alguna característica especial de ciertos protocolos o se aprovechan de alguna debilidad en algún software. A continuación se mencionan algunos de los más conocidos:

- **IP Spoofing.** Se basa en modificar el campo de dirección origen de los paquetes IP, por otra que queramos suplantar. Dado que los routers trabajan con base en tablas de direcciones IP, es necesario que el paquete utilice un campo opcional del encabezado denominado Source Routing. Dicho campo le especificará a los routers que no utilicen sus tablas de enrutamiento, sino que obedezcan la ruta especificada en dicho campo.
- **Ping flood ( tormenta de pings)**. Este ataque –también llamado "pitufo" o smurf– se basa en enviar un comando ping (petición de eco) a un grupo de equipos usando una dirección grupal o broadcast pero sustituyendo nuestra dirección IP con la dirección IP de la máquina víctima. Lo que sucede entonces es que todas las máquinas que están en ese grupo le responden el ping (echo reply) a la máquina víctima, saturándola de tráfico y provocando posiblemente que se caiga o por lo menos que se degrade su tiempo de respuesta.
- **Ping de la muerte.** Dado que el máximo tamaño especificado para el mensaje en el que viaja un ping es de 65 mil 535 bytes, muchos equipos y dispositivos tienen

problemas para ensamblar un mensaje de mayor tamaño, causando en algunos casos una caída del sistema.

- **Syn flood (inundación de SYNs).** El equipo del atacante trata de iniciar una conexión con el equipo víctima, pero no termina el proceso sino que repite la misma petición muchísimas veces. Como para cada petición la máquina víctima asigna un área de memoria (buffers para la conexión), es frecuente que después de diversos inicios de conexión se tenga una conexión de buffer o memory overflow, lo que puede ocasionar la caída del equipo (negación del servicio). El nombre del ataque proviene de que la bandera de sincronización (SYN) se ocupa para indicar un inicio de conexión. Existen diversas variantes de este ataque.
- **Land.** Este ataque se basa en poner la misma dirección (vía IP spoofing) de origen y destino. Muchos equipos al ver un paquete de esas características, entran en un ciclo infinito (loop) hasta que se cae el sistema.
- **Teardrop.** Se basa en el envío de un mensaje TCP en diversos paquetes que se traslapan. Algunos sistemas operativos tiene problemas para reensamblar paquetes traslapados, ocasionando caídas.
- **TCP hijacking (rapto de conexiones TCP).** Consiste en romper una conexión TCP entre dos computadoras que ya han realizado su proceso de autentificación, y tratar de reestablecer la comunicación con una de ellas, simulando ser la otra. El ataque es complicado puesto que se tiene que "poner a dormir" a un equipo, hacer IP spoofing de su dirección, y tratar de adivinar el número de secuencia de los mensajes TCP para que el equipo al que queremos entrar no se percate del ataque.
- **Sniffers de passwords (husmeadores).** Este no es un ataque activo como los demás. Aquí se trata de "sembrar" en algún equipo, un programa que cuando se ejecute, actúe como la primera interfaz entre el usuario y el sistema operativo. De esta forma, cuando el usuario se autentifique e introduzca su nombre y password, realmente el programa ante quien se autentifica no es el sistema operativo, sino el husmeador de passwords. Éste, para no ser detectado, envía dicha información al sistema operativo para que el usuario pueda entrar, al mismo tiempo que graba en un archivo, el nombre y password del usuario.
- **Ataques distribuidos de negación de servicio (DDoS attacks).** Los ataques de Denial Of Service Distribuidos (DDoS) son variantes de algunos de los ataques de negación de servicio –como el smurf– pero que surgen de diversas máquinas atacantes. Para que se pueda ejecutar, el atacante ha "sembrado" previamente programas maliciosos en decenas o cientos de equipos. Todos estos equipos en

una fecha determinada o ante instrucciones específicas del atacante, realizarán algún ataque de negación de servicio.

## 1.2 Seguridad y el World Wide Web

El web es construido desde un programa especialmente escrito llamado Web Server que disponibiliza información en la red. Otros programas llamados Web Browser, pueden ser usados para acceder a la información que es almacenada en los servidores y desplegada en las pantallas de los usuarios.

Otro excitante uso de la Web hoy día involucra poner programas detrás de las páginas Web. Los programas son creados con un protocolo llamado el Common Getway Interfase (CGI). Los script de CGI pueden ser simples por ejemplo, un contador que se incremente cada vez que una persona mira la página, o compra un libro que permita a las personas señalarlas en el sitio.

Muchas otras compañías están explotando el uso de WWW para el comercio electrónico. Los clientes despliegan catálogos de mercancías y servicios, seleccionan artículos y luego pagan por ellos sin ninguna otra cosa más que un formulario desplegado en la pantalla.

El WWW es uno de lo más excitantes usos de la Internet. Pero así mismo posee profundos retos de seguridad, estos retos son:

- Errores (bugs) o mal configuración del servidor Web: tanto el software del servidor Web y el sistema operativo que sirve de plataforma para el mismo puede contener errores que representen agujeros vulnerables a ataques, tal es el caso del sistema Unix, lo que facilita a usuarios remotos no autorizados se aprovechen de estos agujeros para robar documentos confidenciales, ejecutar comandos en la maquina servidor para ganar acceso al sistema o simplemente lanzar un ataque de negación de servicio. Sin embargo, se debe considerar el factor de la experiencia de los administradores de los sistemas y los anfitriones.
- Perspectiva del cliente: no sólo el servidor Web puede presentar riesgos en la seguridad, así también los usuarios que utilizan los navegadores (browser) para visitar los Web Sites son vulnerables a ataques. Contenidos activos, tales como los applets de java o códigos de JavaScript, pueden dañar el sistema del usuario, violar la privacidad del mismo o simplemente molestarlo.

- Interceptación de la información enviada desde el usuario al servidor Web y viceversa a través de la red. El protocolo que utiliza la Internet (TCP/IP) hace que viaje la información a través de la red en forma legible, siendo vulnerable a ser capturada por los llamados espías de la red en cualquier punto del camino entre el usuario y el servidor, atentando de esta manera a la confidencialidad de la misma.
- Impersonificación del servidor web o del usuario: en un medio anónimo como Internet, existe el riesgo de que un tercero pueda personificar a un determinado usuario o a un servidor web, ya que el protocolo TCP/IP es vulnerable a ataques spoofing.

## 1.3 Seguridad para un Web Site Público

La WWW es una de las vías más importantes de las organizaciones para la publicación de la información. Desafortunadamente, si no tienes cuidado al configurar y operar el sitio Web, dejarás a la organización vulnerable a una variedad de problemas de seguridad. Se encontrará en una situación embarazosa porque los intrusos pueden cambiar el contenido de la página Web. El Web site público tiene también el punto de entrada para violaciones en la red interna de la organización para propósitos de acceso a la información. Las prácticas recomendadas son diseñadas para ayudar a prevenir estos y otros daños con respecto a la seguridad.

Estas prácticas son aplicables a su organización si, operar el Web site para hacer publica la información de la organización.

- Mantener la integridad de la información que piensas publicar
- Prevenir el uso del Web Host, como área de instrucciones en la red de trabajo de la organización, que daría como resultado la violación de la confidencialidad, integridad, o disponibilidad de los recursos de información.
- Prevenir el uso del Web Host como área de instrucciones de sitios externos, que resultaría perjudicial para la organización.

Hay dos razones principales en la seguridad relacionada a la operación de un sitio Web público:

a) La configuración u operación impropia del servidor Web puede dar como resultado la revelación inadvertida de información confidencial. Estas pueden incluir:

- Cualidades de la información de la organización
- Información sobre la configuración del servidor o red que debe ser explotada por ataques subsecuentes.
- Información sobre quien solicita los documentos desde el servidor.

b) El host usado por su servidor Web puede estar expuesto permitiendo:

- Cambiar la información almacenada en el servidor Web, particularmente la información que intenta publicar.
- Lograr accesos no autorizados a recursos en la red de la organización.
- Atacar sitios externos desde el servidor, de este modo, encubre la identidad del intruso y puede que haga que la organización corra riesgo de daños.

### 1.3.1 Aislar el Servidor Web de la Red Interna de la Organización

Usualmente tenemos varias opciones de donde colocar un servidor de Web público en nuestra organización. Recomendamos que sea colocado en una subred separada, de manera que el tráfico entre la Internet y el servidor no atraviese partes de su red interna y la red interna no sea visible en el servidor.

Un servidor Web público es una computadora que da a entender que el acceso es público. Esto quiere decir que muchas personas accesarán el host desde ubicaciones en todo el mundo. El descuido del host y la mala configuración del software de aplicación, dan oportunidad que alguien descubra una nueva vulnerabilidad, explotándola, e intentando el acceso al Servidor Web. Si eso pasa, necesita prevenir estos eventos.

- El intruso es capaz de observar o capturar el trafico de la red que está fluyendo entre los host internos. Este tráfico puede incluir autenticación de información, información comercial del propietario, datos personales, y muchos otros datos sensibles.
- El intruso es capaz de conseguir host internos, u obtendrá información detallada de ellos.

Para vigilar estas dos amenazas, el servidor debe aislar la red interna del tráfico del Server.

Podemos lograrlo de la siguiente manera:

- Colocar el host en una subred aislada de la red principal interna.
- Use filtros o un cortafuego para restringir el tráfico desde el servidor Web a la red interna.
- Desviar las rutas al servidor Web de manera que no pueda usar la red interna.

### 1.3.2 Ofrecer Solamente los Servicios de Red Esenciales y los Servicios de Sistema Operativo en el Servidor

Idealmente, el servidor Web debería ser dedicado, host de propósito individual. Muchas computadoras modernas son configuradas "out of the box" para proveer un amplio juego de servicios y aplicaciones que estrictamente son requeridos por los servicios Web. Por esto, la configuración explícita debe ser requerida para eliminar o deshabilitar servicios y aplicaciones innecesarias.

Ofreciendo sólo los servicios esenciales de red en un host particular se puede aumentar la seguridad en varias vías:

- Otros servicios no pueden ser usados para atacar el host.
- Los diferentes servicios pueden ser administrados por diferentes individuos. Deberá minimizar la posibilidad de conflictos entre los administradores
- El host puede ser configurado para mejorar la demanda de los requerimientos del servicio particular provisto. Los diferentes servicios pueden requerir diferentes configuraciones de hardware y software, reduciendo vulnerabilidades o restricciones de servicios.
- Con los servicios reducidos, se reduce el número de logs y entrada de logs, para así detectar anomalías.

### 1.3.3 Configurar el Servidor Web para Aumentar la Seguridad

Cuando instala el software del servidor, estas presentan normalmente un número de alternativas para configurar las opciones o preferencias. Estas alternativas deberán ser hechas cuidadosamente para balancear los requerimientos de seguridad y operación.

También, el sistema operativo del host puede proveer controles de acceso para almacenar información en el host. Esto es particularmente común en sistemas que soportan múltiples usuarios simultáneamente. Deberás tomas ventaja de estos controles para ayudar a la prevención de accesos y salida de información que no debe ser publica.

Los requerimientos para sitios públicos varían de una organización a otra, así que los vendedores de software proveen la configuración del mismo para cada uno de ellos. La configuración puede ser optimizada por un sitio "típico", como es imaginado por el vendedor, y puede ser basado más en requerimientos de ejecución o fácil instalación. Usualmente, los requerimientos de seguridad necesitarán una configuración diferente. El cambiar la configuración por defecto puede reducir la seguridad del sitio.

Un servidor típico almacena no sólo la información para publicar, sino también una gran variedad de diferentes temas que no deben ser publicados. Estos normalmente incluyen los archivos log del servidor así como sistemas y aplicaciones tales como archivos de password. Si eres cuidadoso al usar los controles de accesos provistos por el sistema operativo en el servidor, puedes reducir la probabilidad de dejar salir información o la corrupción de esta información.

Podemos hacerlo así:

- Configurar la capacidad de logins del servidor
- Configurar servicios auxiliares del servidor
- Configurar programas ejecutables por el servidor
- Configurar el servidor para la administración local y/o remota
- Determinar que controles de acceso son provistos por el sistema operativo de host.
- Use el archivo de controles de Acceso para llevar a cabo lo siguiente
- Los archivos del Web público son de lectura, pero no pueden ser escritos por los procesos que implementan los servicios Web.
- El directorio donde está el contenido Web almacenado no puede ser escrito por los procesos de servidor

- Los archivo que contienen el Web público puede ser escrito solamente por los procesos que permita la administración del Web.
- Los archivo log del servidor pueden ser escritos por los procesos del servidor, pero no pueden ser leídos como contenido del Web.
- Los archivos log del servidor Web son leídos solamente por los procesos de administración
- Cualquier archivo temporal creado por un proceso server es limitado a un subdirectorio particular.
- Disponer de listado de directorios de archivos
- Configurar el servidor de manera que los archivos server no sean externos al directorio especificado
- Hacer seguro el servidor y cualquier archivo log o configuración de archivos
- Después que todas las opciones han sido escogidas, se crean y se registran criptográficamente o por otro medio de registro.

### 1.3.4 Administrar el Servidor Web de una Manera Segura

La administración de un Servidor Web incluye tareas tales como transferencia de nuevo contenido al server, examinar los logs del server, instalación de nuevos programas externos, y otros cambios a la configuración del servidor. Estas tareas usualmente pueden ser ejecutadas ya sea de la consola del servidor o desde un host separado por medio de conexión de red. En cualquier caso, debe ser segura la ejecución de las tareas de manera que no ofrezca oportunidades a los intrusos infringir la seguridad del servidor.

Aunque el estado de operación normal de su servidor puede ser segura, durante la ejecución de tareas administrativas, el servidor puede estar en un estado de transición vulnerable. Esto es verdadero especialmente si el administrador del servidor está en un host remoto, porque este requiere que este abierta la conexión de red a través del firewall. Tal conexión puede ser vulnerable a algunas formas ataques, y puede abrir la puerta a Internet y a la administración de su servidor. El resultado sería la perdida de integridad del contenido de su Web.

Podemos hacer lo siguiente:

- Si escoge administrar el servidor desde un host remoto, necesita tomar precauciones para hacerlo de una manera segura.
- Si es fiable para su Web, use un medio de almacenamiento móvil para transferir el contenido desde la copia autorizada al servidor público.
- Si decide inspeccionar los archivos log del servidor desde otro host, use un método seguro para transferir los logs.
- Después que todas las opciones han sido escogidas, se crean y se registran criptográficamente o por otro medio de registro.

### 1.3.5 Observar los Cambios Inesperados de Directorios y Archivos

Los sistemas de archivos de su ambiente de redes contienen una variedad de software y archivos de datos. Los cambios inesperados en directorios y archivos, especialmente aquellos que el acceso es normalmente restringido, puede ser un indicativo que una violación a ocurrido. Los cambios incluyen modificación, creación, o eliminación de directorios y archivos.

Los intrusos frecuentemente sustituyen, modifican, y dañan archivos en los sistemas en que han violado el acceso. Ocultan su presencia en sus sistemas, es común para los intrusos reemplazar programas de sistemas con sustitutos que ejecutan las mismas funciones pero excluyen información que revelaría sus actividades ilícitas. Encubriendo su presencia en los sistemas, los intrusos prolongan el tiempo para usar el sistema para sus propósitos. Es notable la seriedad del caso, la presencia de intrusos en sistemas no es descubierto hasta muchos meses después de haber entrado ilícitamente.

Los archivo de datos privados y los archivos de información critica son el blanco común de modificaciones o corrupciones por los intrusos. La información de la organización que es accesible al público o para suscribirse vía pública y la Internet también son blancos comunes. Existen varios casos documentados de organizaciones en donde su Web Site ha sido modificado para incluir contenido ofensivo y otras informaciones erróneas.

Podemos hacer lo siguiente:

- Establecer prioridades y plan de trabajos
- Mantener referencia de datos de archivos críticos y directorios.

- Verificar la integridad de directorios y archivos de acuerdo a su plan de trabajo establecido.
- Identificar cualquier archivo o directorio perdido.
- Identificar cualquier archivo o directorio nuevo.
- Investigue cualquier cambio inesperado

### 1.3.6 Inspeccionar sus Sistemas y Logs Red

Frecuentemente, los intrusos dejan indicios de sus acciones en los archivo log del sistema. Por esto, se verifica el sistema y los archivos log periódicamente ya que es una vía para detectar las violaciones.

Los logs contienen evidencias de actividades inusuales e inesperadas que han ocurrido en el sistema o en la red. Talles entradas pueden indicar que alguien ha cambiado o intentado cambiar el sistema.

A continuación en la tabla 2.1 se describe el contenido de los archivos log:

Tabla 2.1 Contenido de los Logs

| **Tipo de Log** | **Información contenida en el Log** |
|---|---|
| Actividad de Usuario | • Actividad de login<br>• Cambios en la identidad del usuario<br>• Accesos a archivos por el usuario<br>• Información de autorización<br>• Información de autenticación |
| Actividades de proceso | • Comandos ejecutados por el usuario<br>• Información de procesos ejecutados incluyendo el nombre del programa, usuario, inicio y fin, y parámetros de ejecución. |
| Actividades del sistema | • Levantar y bajar el sistema |

| | |
|---|---|
| | • Logins administrativos |
| Conexiones de Red | • Detalles de intentos de conexiones o conexiones establecidas con el sistema |
| Monitoreo del Tráfico de Network | • Registro de todas las transacciones |

Para llevarlo a la práctica hay hacer lo siguiente:

- Periódicamente inspeccionar cada tipo de archivo log
- Documentar cualquier entrada inusual que se descubra
- Investigue cada documento anormal
- Reporte todas las evidencias confirmadas de violaciones al contacto de la seguridad interna de la organización.
- Leer los boletines de seguridad de fuentes confiables y otras publicaciones regulares de seguridad.

# CAPITULO II

# SEGURIDAD EN LA TRANSACCION

## 2.1 Criptografía

Cuando las personas piensan acerca de la seguridad del Web la criptografía es una de las primeras cosas que toma en cuenta. Gracias a los desarrolladores de los navegadores ha aumentado la conciencia en el consumidor acerca de los riesgos de transmitir números de tarjetas de crédito a través de la Web.

La criptografía juega un papel crucial en la Web. Permite que la información confidencial sea transmitida de un lugar a otro a través de redes inseguras sin el riesgo de intersección o modificación y permite a los dos lados de la comunicación verificar su identidad sin verse en persona.

La palabra criptografía viene del griego de "escritura secreta". La criptografía ha sido usada por los militares desde los días de las guerras Helénicas y ha crecido firmemente en la sofisticación en paralelo con las Matemáticas y Tecnologías de Información.

Todos los sistemas criptográficos, sin importar cuan complejos sean tienen las siguientes cuatro partes básicas.

**a) *Plaintex*** (texto claro)

Este es el mensaje antes de que se haga cualquier cosa. Este es leíble por los humanos o en un formato que cualquier software adecuado pueda usar.

**b) *Texto Cifrado***

Este es el mensaje en plaintext después de que ha sido modificado para hacerlo ilegible. El proceso de convertir texto claro a texto cifrado se dice encriptar y la operación inversa es desencriptar.

**c) *Algoritmo de encripción***

Esta es la operación usada para convertir texto claro a texto cifrado y viceversa.

**d) *Llave***

Esta es una llave secreta usada para encriptar o desencriptar el mensaje. Cada llave transforma el mismo texto claro en diferente texto cifrado. Si el sistema criptográfico funciona bien, solamente las personas que conocen la llave correcta pueden descifrar el texto cifrado.

La belleza de la criptografía es tal que el texto cifrado pueda ser transmitido a través de canales públicos de comunicación inseguros aun si el texto cifrado es interceptado no tiene utilidad para nadie que no posee la llave de desencriptamiento. Antes de la llegada de las computadoras digitales el texto cifrado y la llave estaban usualmente en la forma de texto leído para humanos ahora las tres son típicamente cadenas arbitrarias de información binaria. Vídeo, sonido y software pueden ser encriptados tan fácilmente como el texto en claro.

Una característica importante de un buen sistema depende completamente en la secreto de la llave de desencriptamiento. No es necesario guardar en secreto el algoritmo de encriptamiento. Esto permite al mismo algoritmo ser rehusado por muchos personas y evita la necesidad de proteger el software de encriptamiento.

El texto cifrado puede ser roto y leído por usuarios no autorizados en varias formas, una forma es a través del criptoanálisis. Criptógrafos entrenados analizan el texto cifrado en busca de patrones (secuencias) residuales dejados desde el texto claro. Cualquiera de estos patrones pueden ser usados para reconstruir el mensaje original ó la llave usada para encriptarlo. Un buen algoritmo de encriptamiento es uno que genera estos patrones: el texto cifrado es indistinto del ruido randón. Todos los algoritmos comúnmente usados en el Web tienen esta propiedad y por tanto son resistentes a los criptoanalistas por esta razón.

Otra forma de romper el texto cifrado es adivinar la llave de desencriptamiento, pruebas cada llave posible en turno hasta que se encuentre una que regrese un mensaje leíble, este es conocido como “ataque de fuerza bruta”. Esto puede sonar impracticó pero recuerde que las computadoras pueden realizar millones de pruebas por segundo, aun

cuando las computadoras individuales no son muy rápidas pueden ser conectadas en red para trabajar en paralelo, adivinando password a una velocidad asombrosa. Esta es la razón por la longitud de la llave es tan importante. Una llave de 16 bits de largo tiene 2 a la 16 ó 65536 diferentes posibilidades y van a caer en un ataque de fuerza bruta inmediatamente. Una llave con 40 bits de largo tiene mas de 10 a la 12 posibilidades. Aunque esto se vea como mucho, llaves de 40 bits son consideradas. Demasiado débiles para confiarles información valiosa.

Las llaves usadas para encriptar información sensible son típicamente de 128 bits o mayores (10 a la 38 posibilidades) más que el numero de moléculas de agua en todos los océanos del planeta. La forma más fácil para romper un mensaje encriptado es encontrar una forma de darle la vuelta al sistema. Uno podría entrar en la maquina en donde el texto en claro esta guardado y robar el archivo, sobornar a alguien para que revele la llave de encriptamiento, etc.

## 2.2 Algoritmos Criptográfico

Es un método matemático que se emplea para cifrar y descifrar un mensaje. Generalmente funciona empleando una o más *claves* (números o cadenas de caracteres) como parámetros del algoritmo, de modo que sean necesarias para recuperar el mensaje a partir de la versión cifrada.

El mensaje antes de cifrar se denomina *texto claro* y una vez cifrado se denomina *texto cifrado*.

### Algoritmos de resumen de mensajes

Transforman mensajes de tamaño variable a textos cifrados de tamaño fijo sin emplear claves. Se emplean para convertir mensajes grandes en representaciones más manejables.

### Algoritmos de claves secretas o simétricas

Convierten un mensaje en un texto cifrado del mismo tamaño que el original. Emplean una sola clave para cifrar y descifrar. Son los algoritmos empleados para transferir grandes cantidades de información de modo seguro.

**Algoritmos de claves públicas o asimétricas**

Encriptan un mensaje generando un texto cifrado del mismo tamaño que el original. Usan una clave para cifrar el mensaje (clave privada) y otra para descifrar (clave pública). Tienen un coste computacional alto y se suelen emplear para distribuir las claves de los algoritmos simétricos

Tabla 2.1 Principales Algoritmos

| NOMBRE | TIPO | REFERENCIA |
|---|---|---|
| MD5 | MD | RFC 1321 ftp://ds.internic.net/rfc/rfc1321.txt |
| SHA-1 | MD | NIST FIPS 180-1 http://www.nist.gov/itl/div897/pubs/fip180-1.htm |
| HmacMD5 | MAC | RFC 2104 ftp://ds.internic.net/rfc/rfc2014.txt |
| HmacSHA1 | MAC | RFC 2104 ftp://ds.internic.net/rfc/rfc2014.txt |
| DSA | Firma | NIST FIPS 186 http://www.nist.gov/itl/div897/pubs/fip186.htm |
| ElGamal | Firma | |
| DES | Cifrador Simétrico | NIST FIPS 46-2 http://www.nist.gov/itl/div897/pubs/fip46-2.htm |
| DESede | Cifrador Simétrico | ANSI X9.17 o ISO 8732 http://www.ansi.org/ |
| PBEWithMD5 andDES | Cifrador Simétrico | PKCS#5 http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-5.html |
| ElGamal | Cifrador Asimétrico | |
| DH | Intercambio de Llaves | PKCS#3 http://www.rsa.com/rsalabs/pubs/PKCS/ps/pkcs-3.ps |

En la práctica los principios criptográficos deben ser incorporados a software y protocolos de comunicación que estén trabajando. Hay una variedad de protocolos criptográficos en el Internet, y cada uno especializado en diferentes tareas como se muestra en la tabla siguiente:

**Protocolos de uso general y particulares**

Tabla 2.2 Protocolos mas usados

| PROTOCOLO | PROPOSITO |
|---|---|
| CyberCash | Transacciones electrónica de Fondos |
| DNSSEC | Sistemas de Dominio de Nombres |
| IPSec | Encripción a nivel de paquete |
| PCT | Encriptamiento a nivel de TCP/IP |
| PGP | E-Mail |
| S/MIME | El desplegado de WEB |
| Secure RPC | Llamadas a procedimientos remotos |
| SET | Transacciones electrónica de Fondos |
| SSL | Login Remoto |
| TLS | Encriptamiento a nivel de TCP/IP |

Algunos fueron diseñados para seguridad en módulos específicos de comunicación, tales como el e-mail y el loggin remoto. Otros son generales, proveen servicios de criptografía para múltiples nodos de comunicación.

En la Web, SSL (Secure Sockets Layer) es el protocolo dominante para encriptar la comunicación en general entre los navegadores y servidores, mientras que SET (Secure Electronic Transaction) es un protocolo especializado para salvaguardar transacciones basadas en tarjetas de crédito.

## 2.3 Códigos de Autentificación de Mensajes y Firmas Digitales

Un *código de autentificación de mensaje* (*message authentication code* o ***MAC***) es un bloque de datos de tamaño fijo que se envía con un mensaje para averiguar su origen e integridad. Son muy útiles para proporcionar autentificación e integridad sin confidencialidad. para generar MACs se pueden usar algoritmos de clave secreta, de clave pública y algoritmos de resumen de mensajes.

Un tipo de MAC muy empleado en la actualidad es el *código de autentificación de mensaje resumido* (*hashed message authentication code* o *HMAC*). Lo que hacemos es generar el MAC aplicando una función de dispersión criptográfica a un conjunto formado por un mensaje y un código secreto. Así, el que recibe el mensaje puede calcular su

propio MAC con el mensaje y el código secreto (que comparte con el que ha generado el MAC). Si no coinciden sabemos que el mensaje ha sido manipulado. Este tipo de técnicas se emplean para proteger comunicaciones a nivel de la capa de red.

La ***firma digital*** es un item que responde del origen e integridad de un mensaje. El que escribe un mensaje lo firma usando una *clave de firmado* y manda el mensaje y la firma digital. El destinatario usa una *clave de verificación* para comprobar el origen del mensaje y que no ha sido modificado durante el tránsito.

Para firmar los mensajes se emplean algoritmos de clave pública y funciones de dispersión. El proceso es como sigue:

a) El emisor genera un resumen del mensaje, lo encripta con su clave privada (*clave de firmado*) y envía el mensaje y el texto cifrado que corresponde al resumen del mensaje.
b) El destinatario genera un resumen del mensaje que recibe y desencripta el resumen cifrado que lo acompañaba usando la clave pública del emisor (*clave de verificación*).>Si al comparar los resúmenes ambos son iguales el mensaje es válido y ha sido firmado por el emisor real, ya que de otro modo no se hubiera podido descifrar correctamente con su clave pública.

Hay que indicar que los MAC y las firmas digitales se diferencian en un punto importante: aunque los MAC se pueden usar para verificar la autenticidad de los mensajes, no se pueden usar para firmar los mensajes, ya que sólo se usa una clave secreta que comparten el emisor y el receptor, lo que hace que ambos puedan generar la misma firma.

Para que un sistema criptográfico sea considerado como fuerte debe tener las siguientes características:

- Debe disponer de un número muy elevado de claves posibles, de modo que sea poco razonable intentar descifrar un mensaje por el método de la fuerza bruta (probando todas las claves).
- Debe producir texto cifrado que parezca aleatorio a un test estadístico estándar.
- Debe resistir todos los métodos conocidos de romper los códigos, es decir, debe ser resistente al criptoanálisis

## 2.4 Certificados Digitales

Para solucionar el problema de la Autentificación en las transacciones por Internet se buscó algún sistema identificativo único de una entidad o persona. Ya existían los sistemas criptográficos de clave asimétrica, mediante los cuales una persona disponía de dos claves, una pública, al alcance de todos, y otra privada, sólo conocida por el propietario. Cuando deseamos enviar un mensaje confidencial a otra persona, basta pués con cifrarlo con su clave pública, y así estaremos seguros de que sólo el destinatario correcto podrá leer el mensaje en claro.

El problema era estar seguro de que efectivamente la clave pública que nos envían sea de la persona correcta, y no de un suplantador. Entonces se pensó en implementar una especie de documento de identidad electrónica que identificara sin dudas a su emisor.

La solución a este problema la trajo la aparición de los **Certificados Digitales** o **Certificados Electrónicos**, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales. La misión principal de un Certificado Digital es garantizar con toda confianza el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.

Un Certificado Digital es un documento electrónico que contiene datos identificativos de una persona o entidad (empresa, servidor web, etc.) y la llave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada **Autoridad Certificadora**. Las principales Autoridades Certificadoras actuales son ***Verisign*** (filial de RSA Data Security Inc.) y Thawte.

El formato de los Certificados Digitales es estándar, siendo X.509 v3 el recomendado por la Unión Internacional de Comunicaciones (ITU) y el que está en vigor en la actualidad. El aspecto de los certificados X.509 v3 se muestra en la figura 2.1.

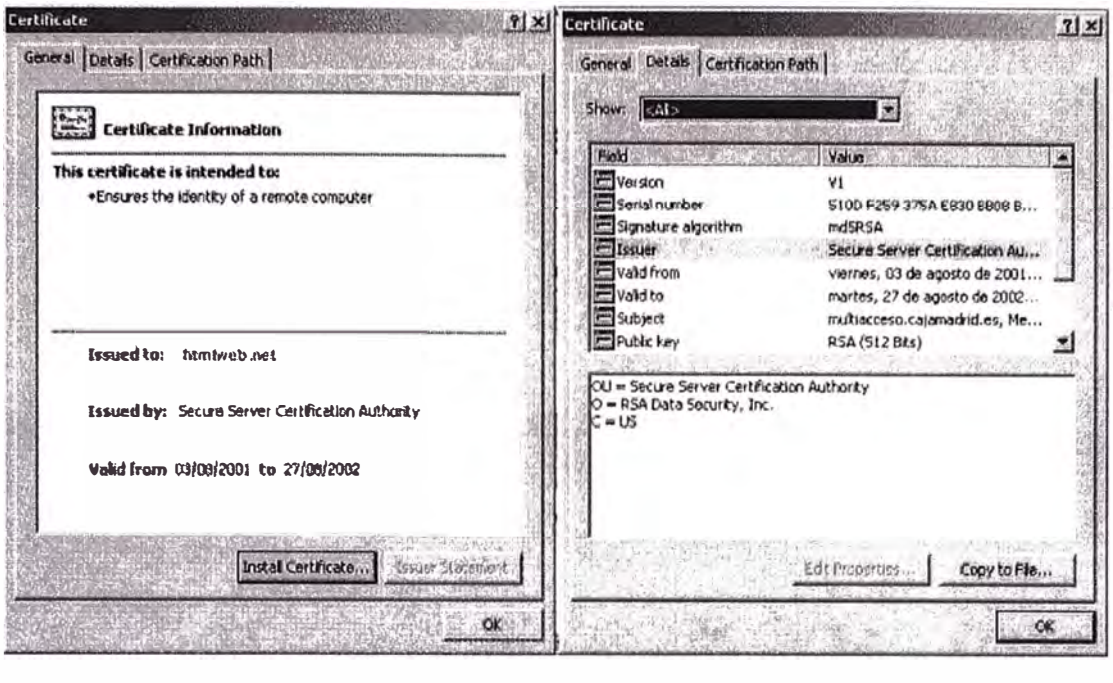


Figura 2.1 Certificado Digital con Formato X.509

El formato de certificados X.509 es un estándar del ITU-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y el ISO/IEC (*International Standards Organization /International Electrotechnical Commission*) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios. Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996.

Los elementos del formato de un certificado X.509 v3 son:

• **Versión**. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.

• **Número de serie del certificado**. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.

• **Identificador del algoritmo de firmado**. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).

• **Nombre del emisor**. Este campo identifica la CA que ha firmado y emitido el certificado.

• **Periodo de validez**. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del

mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.

• **Nombre del sujeto**. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.

• **Información de clave pública del sujeto**. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.

• **Identificador único del emisor**. Este es un campo opcional que permite reutilizar nombres de emisor.

• **Identificador único del sujeto**. Este es un campo opcional que permite reutilizar nombres de sujeto.

• **Extensiones**. Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

**a) Tipo de extensión**. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.

**b) Valor de la extensión**. Este subcampo contiene el valor actual del campo.

**c) Indicador de importancia**. Es un *flag* que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3:

• **Limitaciones básicas**. Este campo indica si el sujeto del certificado es una CA y el máximo nivel de profundidad de un camino de certificación a través de esa CA.

• **Política de certificación**. Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.

• **Uso de la clave**. Este campo restringe el propósito de la clave pública certificada, indicando, por ejemplo, que la clave sólo se debe usar para firmar, para la encriptación de claves, para la encriptación de datos, etc. Este campo suele marcarse como importante, ya que la clave sólo está certificada para un propósito y usarla para otro no estaría validado en el certificado.

El formato de certificados X.509 se especifica en un sistema de notación denominado *sintaxis abstracta uno* (*Abstract Sintax One* o ASN-1). Para la transmisión de los datos se aplica el DER (*Distinguished Encoding Rules* o *reglas de codificación distinguible*), que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales.

Un ejemplo se muestra en la figura 2.2.

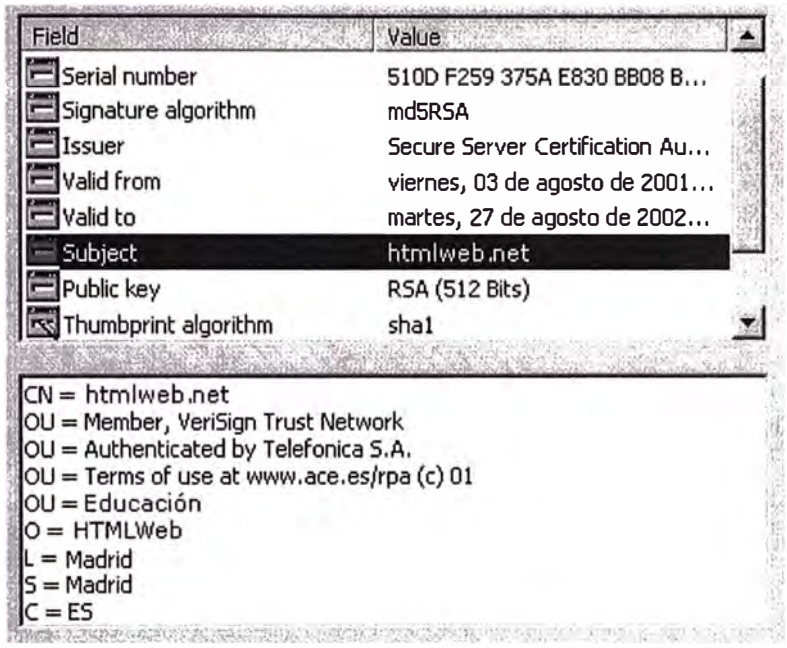


Figura 2.2 Notación del Formato X.509

| | |
|---|---|
| CN | nombre común del usuario |
| OU | información varia |
| O | organización |
| L | ciudad |
| S | estado (provincia) |
| C | país |
| E | correo electrónico |
| UID | ID de usuario |

El problema que se plantea ahora es: si la Autoridad Certificadora avala los datos del certificado ¿Quién avala a la autoridad Certificadora?. Para solventar esto se han creado una serie de entidades autorizadas a emitir certificados, de tal forma que éstas a

su vez son avaladas por otras entidades de mayor confianza, hasta llegar a la cabeza de la jerarquía, en la que figuran unas pocas entidades de reconocido prestigio y confianza, como ***Verisign***, que se autofirman su certificado.

Cada certificado emitido por una AC debe estar firmado por una AC de mayor grado en el esquema jerárquico de autoridades certificadoras, formándose así una cadena de certificados, en los que unas AC se avalan a otras hasta llegar a la AC superior, que se avala a sí misma. La jerarquía de firmas y la cadena con ella formada están contempladas en el estándar X.509 v3, que indica la forma correcta de realizar estas cadenas de certificaciones.

El certificado Digital vincula pues indisolublemente a una persona o entidad con una llave pública, y mediante el sistema de firma digital se asegura que el certificado que recibimos es realmente de la persona que consta en el mismo. El sistema de firma digital liga un documento digital con una clave de cifrado.

El procedimiento de **firma digital** lo que hace es obtener un resumen de un documento o de un texto aleatorio y cifrarlo con llave privada del propietario del certificado. Cuando nos llega un certificado, y su firma digital asociada, tan sólo debemos obtener nosotros el resumen el mismo, descifrar la firma con la llave pública del remitente y comprobar que ambos resúmenes coinciden, lo que nos hace estar totalmente seguros de la autenticidad del certificado.

Se firma un resumen del documento y no el documento mismo para evitar ataques contra el sistema de cifrado RSA (por ejemplo, encriptar un documento especialmente concebido por un pirata, con lo que éste podría llegar a obtener la llave privada) y para no hacer el proceso demasiado lento.

Para obtener el resumen del documento se utilizan las **funciones hash** o de resumen, algoritmos criptográficos muy rápidos, de uso público e irreversibles (de un sólo sentido). Son funciones de dispersión que no usan ninguna clave, y que transforman el mensaje original en una cadena de dígitos de longitud fija (generalmente de entre 16 y 128 bits). Ver figura 2.3.

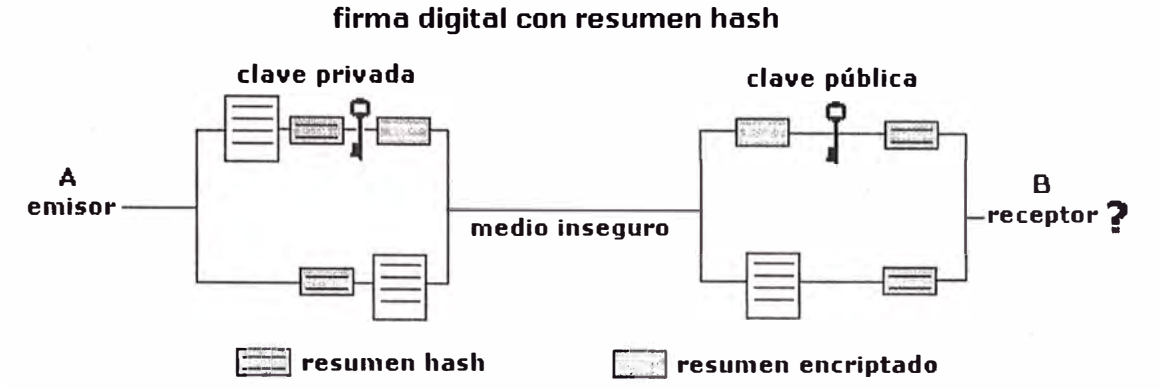


Figura 2.3 Firma Digital con Resumen Hash

Los procesos de validación de certificados, obtención de resúmenes, descifrados y comprobación de coincidencia se realizan por el software adecuado del navegador web o programa de seguridad particular de forma transparente al usuario, por lo que éste será informado sólo en el caso de que el certificado no sea válido.

## 2.5 Validez de los Certificados Digitales

Los certificados, debido a su propia naturaleza y al papel que desempeñan, no son documentos imperecederos, al igual que sucede con 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 periodos de tiempo largos, ya que uno de los principales problemas del manejo de claves es que cuanto más vida tienen más facil es que alguien extraño se apodere de ellas. Además, con el paso del tiempo los equipos informáticos van teniendo cada vez más poder de cálculo, facilitando con ello la labor de lso criptoanalistas, por lo que es conveniente que cada cierto tiempo se vaya aumentando el tamaño de las claves criptográficas. Por este motivo los Certificados Digitales tienen estipulado un periodo de validez, que suele ser de un año.

En segundo lugar, es posible que un certificado convenga anularlo en un momento dado, bien porque se crea que las claves estén comprometidas, bien porque la persona o entidad propietaria haya caído en quiebra o delito. Es por esto 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.

Cuando nuestro software de seguridad recibe un Certificado Digital de otra persona o entidad comprueba antes de darlo por bueno si dicho certificado se encuentra en la lista más actualizada de certificados revocados. Si está en la lista, el certificado será rechazado.

Ahora bien, imaginemos que recibimos un certificado como medio de autentificación en una transacción, nuestro software comprueba que no está revocado en la última CRL y lo da por válido, pero resulta que al día siguiente aparece como revocado en la CRL nueva. En estos casos deberemos poder demostrar de algún modo que hemos recibido el certificado antes de que se produjera la actualización.

Para solucionar este tipo de situaciones 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.

Resumiendo, mediante la consulta a una Lista de Certificados Revocados y un recibo de una Autoridad de Oficialía de partes 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 un proceso de Autentificación presenta varios problemas adicionales. En primer lugar sólo podemos considerarlo válido cuando la fecha del mismo es igual o posterior a la que queremos usar como referencia en la validez del documento, y en segundo lugar, también puede resultar inadecuado en aquellas operaciones que

exijan una velocidad alta en la transacción, sobre todo si el CRL a 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, por el 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 UTC 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 Autencitidad de la respuesta recibida.

## 2.6 Emisión de Certificados Digitales

Los Certificados Digitales, como ya hemos dicho, son emitidos por las Autoridades de Certificación, entidades consideradas de confianza probada, como Verisign, Cybertrust o Nortel. Al hacerse responsables estas entidades de los certificados que emiten, dando fe de la relación existente entre los datos que figuran en un certificado y la persona o entidad que lo solicita, una de las tareas más importantes de las mismas en ejercer un control estricto sobre la exactitud y veracidad de los datos incorporados en el certificado.

Para solicitar un certificado a una AC la persona o entidad interesada debe cumplir unos procedimientos previos, confecccionando un documento, denominado **Requerimiento de Certificación**, en el que deben figurar los datos representativos del solicitante (nombre personal o de empresa, domicilio personal o social, dominio asociado a la empresa y al servidor seguro, etc.) y su llave pública. También debe manifestar su voluntad de aceptar dicha llave pública y demostrar que es el propietario real de la llave privada asociada, mediante el firmado digital de un mensaje.

La presentación de todos estos datos ante la Autoridad Certificadora puede acarrear problemas, al estar éstas normalmente muy distantes de los solicitantes. Para solventar esto se han creado unas entidades intermedias, conocidas como **Autoridades Registradoras**, autorizadas por las AC, y cuya misión es comprobar la validez de los datos presentados en el Requerimiento de Certificación. Una vez comprobados, las AR envía el OK a las AC, que emiten el correspondiente Certificado Digital.

Para que se pueda obtener con facilidad el Certificado Digital de cualquier persona o entidad las Autoridades de Certificación disponen de servidores de acceso público que realizan la función de depósito de certificados, en los que se puede buscar el deseado y descargarlo a nuestro ordenador. Es ésta una forma más segura que la de usar directamente un certificado recibido por correo o descargado de una página web, ya que la Autoridad de Certificación responsable del servidor es la encargada de verificar constantemente la validez y autenticidad de los certificados que distribuye.

Además de las Autoridades de Certificación reconocidas existen otras entidades que también pueden expedir certificados. Este es el caso de entidades gubernamentales (como el Servicio Postal de EEUU) y ciertas corporaciones empresariales que compran un servicio de certificación a un vendedor que haya sido a su vez certificado por una AC. Estos certificados se suelen usar para empleados de la propia compañía que deben hacer negocios para ella. Se espera que en el futuro este tipo de certificados adquiera cada vez mayor importancia.

## 2.7 Tipos de Certificados

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

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

* **Certificados de Clase 1**: corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.

* **Certificados de Clase 2**: en los que la Autoridad Certificadora comprueba además el permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento.

* **Certificados de Clase 3**: en la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante un servicio como Equifax.

* **Certificados de Clase 4**: que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

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

a) **Certificados SSL para cliente**: usados para identificar y autenticar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.

b) **Certificados SSL para servidor**: usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

c) **Certificados S/MIME** : usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autenticación, Integridad y No Rechazo. También se puede cifrar el mensaje con la llave pública del destinatario, lo que proporciona Confidencialidad al envío.

d) **Certificados de firma de objetos**: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc). Cuando un código de éste tipo puede resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.

e) **Certificados para AC**: que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.

Toda persona o entidad que deseé obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso

que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor), más costará el certificado.

## 2.8 Aplicaciones de la Criptografía

La criptografía es una disciplina con multitud de aplicaciones, muchas de las cuales están en uso hoy en día. Entre las más importantes destacamos las siguientes:

- ***Seguridad de las comunicaciones***. Es la principal aplicación de la criptografía a las redes de computadores, ya que permiten establecer canales seguros sobre redes que no lo son. Además, con la potencia de cálculo actual y empleando algoritmos de cifrado simétrico (que se intercambian usando algoritmos de clave pública) se consigue la privacidad sin perder velocidad en la transferencia.
- ***Identificación y autentificación***. Gracias al uso de firmas digitales y otras técnicas criptográficas es posible identificar a un individuo o validar el acceso a un recurso en un entorno de red con más garantías que con los sistemas de usuario y clave tradicionales.
- ***Certificación***. La certificación es un esquema mediante el cual agentes fiables (como una entidad certificadora) validan la identidad de agentes desconocidos (como usuarios reales). El sistema de certificación es la extensión lógica del uso de la criptografía para identificar y autentificar cuando se emplea a gran escala.
- ***Comercio electrónico.*** Gracias al empleo de canales seguros y a los mecanismos de identificación se posibilita el comercio electrónico, ya que tanto las empresas como los usuarios tienen garantías de que las operaciones no pueden ser espiadas, reduciéndose el riesgo de fraudes y robos.

# CAPITULO III

# SEGURIDAD EN LA TRANSMISIÓN

## 3.1 Security Sockects Layer (SSL)

### 3.1.1 Características del Ssl

Secure Socket Layer es un sistema de protocolos de caracter general diseñado en 1994 por la empresa Nestcape Communcations Corporation, y está basado en la aplicación conjunta de Criptografía Simétrica, Criptografía Asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet. De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se aprovecha la rapidez de operación, mientras que los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la confidencialidad en la transmisión de datos.

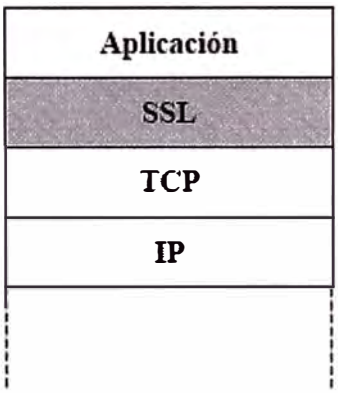


Figura 3.1 Ubicación de SSL en la Pila TCP/IP

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socked. Los sockets son el interficie entre las aplicaciones y el protocolo TCP/IP del sistema operativo (Ver Figura 3.1). Así puede servir para cualquier

aplicación que utilice TCP/IP: Mail, Webs, FTP, News, etc... Aunque las aplicaciones de los programas actuales sólo permiten HTTP (Webs).

Actualmente es el estándar de comunicación segura en los navegadores web más importantes (protocolo HTTP), como Nestcape Navigator e Internet Explorer, y se espera que pronto se saquen versiones para otras otros protocolos de la capa de Aplicación (correo, FTP, etc.).

La identidad del servidor web seguro (y a veces también del usuario cliente) se consigue mediante el **Certificado Digital** correspondiente, del que se comprueba su validez antes de iniciar el intercambio de datos sensibles (Autenticación), mientras que de la seguridad de Integridad de los datos intercambiados se encarga la **Firma Digital** mediante funciones hash y la comprobación de resúmenes de todos los datos enviados y recibidos.

Desde el punto de vista de su implementación en los modelos de referencia OSI y TCP/IP, SSL se introduce como una especie de nivel o capa adicional, situada entre la capa de Aplicación y la capa de Transporte, sustituyendo los sockets del sistema operativo, lo que hace que sea independiente de la aplicación que lo utilice, y se implementa generalmente en el **puerto 443.** (NOTA: Los puertos son las interfaces que hay entre las aplicaciones y la pila de protocolos TCP/IP del sistema operativo).

El SSL puede realizar las funciones:

• **Fragmentación**. En el emisor se fragmentan los bloques mayores que 214 octetos y en el receptor se vuelven a reensamblar.

• **Compresión**. Se puede aplicar un algoritmo de compresión a los mensajes.

• **Autenticación**. Permite autenticar el cliente y el servidor mediante certificados. Este proceso se realiza durante la fase de Handshake. Durante la transmisión los mensajes autentican al emisor mediante un resumen con clave, llamado **MAC**, en cada mensaje.

• **Integridad**. En todos los mensajes se protege la integridad mediante el MAC.

• **Confidencialidad**. Todos los mensajes se envían encriptados.

SSL proporciona servicios de seguridad a la pila de protocolos, encriptando los datos salientes de la capa de Aplicación antes de que estos sean segmentados en la capa de Transporte y encapsulados y enviados por las capas inferiores. Es más, también puede aplicar algoritmos de compresión a los datos a enviar y fragmentar los bloques de tamaño mayor a $2^{14}$ bytes, volviéndolos a reensamblarlos en el receptor.

La versión más actual de SSL es la 3.0. que usa los algoritmos simétricos de encriptación DES, TRIPLE DES, RC2, RC4 e IDEA, el asimétrico RSA, la función hash MD5 y el algoritmo de firma SHA-1.

Los algoritmos, longitudes de clave y funciones hash de resumen usado en SSL dependen del nivel de seguridad que se busque o se permita, siendo los más habituales los siguientes:

* **RSA + Triple DES de 168 bits + SHA-1**: soportado por las versiones 2.0 y 3.0 de SSL, es uno de los conjuntos más fuertes en cuanto a seguridad, ya que son posibles 3.7 * $10^{50}$ claves simétricas diferentes, por lo que es muy dificil de romper. Por ahora sólo está permitido su uso en Estados Unidos, aplicándose sobre todo en transacciones bancarias.

* **RSA + RC4 de 128 bits + MD5**: soportado por las versiones 2.0 y 3.0 de SSL, permite 3.4 * $10^{38}$ claves simétricas diferentes que, aunque es un número inferior que el del caso anterior, da la misma fortaleza al sistema. Análogamente, en teoría sólo se permite su uso comercial en Estados Unidos, aunque actualmente ya es posible su implementación en los navegadores más comunes, siendo usado por organismos gubernamentales, grandes empresas y entidades bancarias.

* **RSA + RC2 de 128 bits + MD5**: soportado sólo por SSL 2.0, permite 3.4 * $10^{38}$ claves simétricas diferentes, y es de fortaleza similar a los anteriores, aunque es más lento a la hora de operar. Sólo se permite su uso comercial en Estados Unidos, aunque actualmente ya es posible su implementación en los navegadores más comunes.

* **RSA + DES de 56 bits + SHA-1**: soportado por las versiones 2.0 y 3.0 de SSL, aunque es el caso de la versión 2.0 se suele usar MD5 en vez de SHA-1. Es un sistema menos seguro que los anteriores, permitiendo 7.2 * $10^{16}$ claves simétricas diferentes, y es el que suelen traer por defecto los navegadores web en la actualidad (en realidad son 48 bits para clave y 8 para comprobación de errores).

* **RSA + RC4 de 40 bits + MD5**: soportado por las versiones 2.0 y 3.0 de SSL, ha sido el sistema más común permitido para exportaciones fuera de Estados Unidos. Permite aproximadamente 1.1 * $10^{12}$ claves simétricas diferentes, y una velocidad de proceso muy elevada, aunque su seguridad es ya cuestionable con las técnicas de Criptoanálisis actuales.

* **RSA + RC2 de 40 bits + MD5**: en todo análogo al sistema anterior, aunque de velocidad de proceso bastante inferior.

* **Sólo MD5**: usado solamente para autentificar mensajes y descubrir ataques a la integridad de los mismos. Se usa cuando el navegador cliente y el servidor no tienen ningún sistema SSL común, lo que hace imposible el establecimiento de una comunicación cifrada. No es soportado por SSL 2.0, pero si por la versión 3.0.

La clave de encriptación simétrica es única y diferente para cada sesión, por lo que si la comunicación falla y se debe establecer una nueva sesión SSL, la contraseña simétrica se generará de nuevo.

SSL proporciona cifrado de alto nivel de los datos intecambiados (se cifran incluso las cabeceras HTTP), autenticación del servidor (y si es necesario también del cliente) e integridad de los datos recibidos.

Durante el proceso de comunicación segura SSL existen dos estados fundamentales, el **estado de sesión** y el **estado de conexión**. A cada sesión se le asigna un número identificador arbitrario, elegido por el servidor, un método de compresión de datos, una serie de algoritmos de encriptación y funciones hash, una clave secreta maestra de 48 bytes y un flag de nuevas conexiones, que indica si desde la sesión actual se pueden establecer nuevas conexiones. Cada conexión incluye un número secreto para el cliente y otro para el servidor, usados para calcular los MAC de sus mensajes, una clave secreta de encriptación particular para el cliente y otra para el servidor, unos vectores iniciales en el caso de cifrado de datos en bloque y unos números de secuencia asociados a cada mensaje.

¿Cómo podemos saber si una conexión se está realizando mediante SSL?. Generalmente los navegadores disponen de un icono que lo indica, generalmente un candado en la parte inferior de la ventana. Si el candado está abierto se trata de una conexión normal, y si está cerrado de una conexión segura. Si hacemos doble click sobre el candado cerrado nos aparecerá el Certificado Digital del servidor web seguro.

### 3.1.2 Protocolo SSL

El protocolo SSL se divide en dos capas complementarias (ver Figura 4.2):

- **Protocolo Handshake**. Realiza las siguientes funciones:

  Autenticación de usuario y servidor.

Selección de los parámetros de la sesión y de la conexión.

Establece la conexión segura.

• **Protocolo de registro** (Record protocol). Se utiliza para la encriptación de los protocolos de las capas más altas: Handshake y aplicaciones.

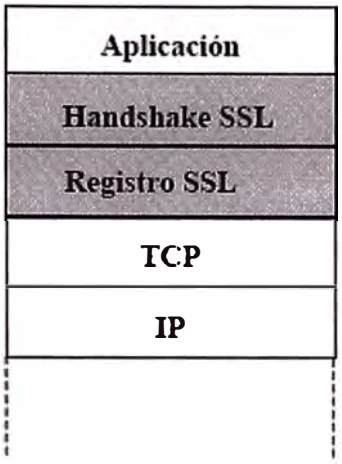


Figura 3.2 Protocolo SSL

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.

**a) 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 negocionado antes mediante la capa de Handshake. En la Figura 3.3 se pueden ver las funciones realizadas por orden de actuación en el emisor.

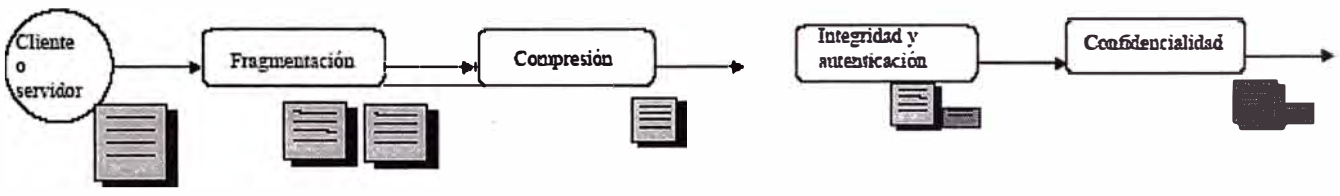


Figura 3.3 Protocolo de Registro de SSL

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 (Ver Figura 3.4). 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 nunca viaja en claro. La integridad se realiza mediante la función Hash.

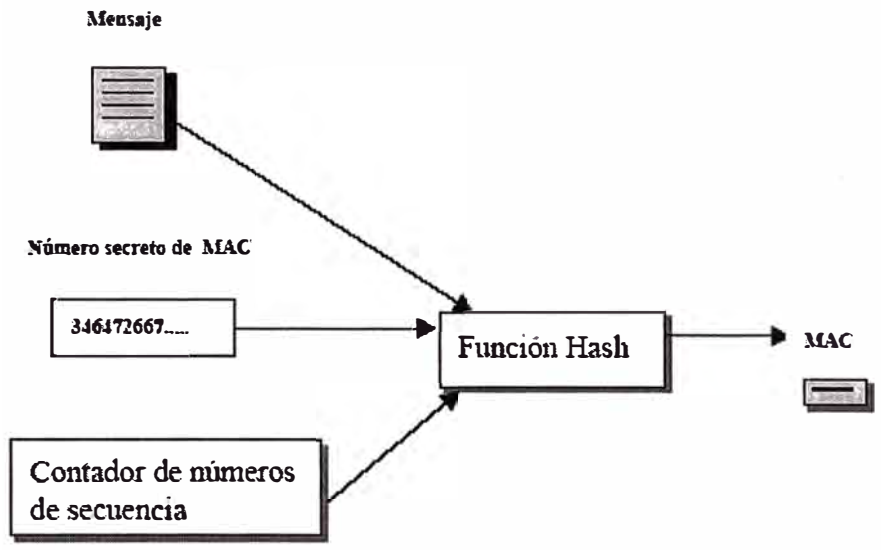


Figura 3.4 Integridad en el Protocolo de Registro de SSL

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.

**b) 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 3.5 se puede ver el esquema del protocolo.

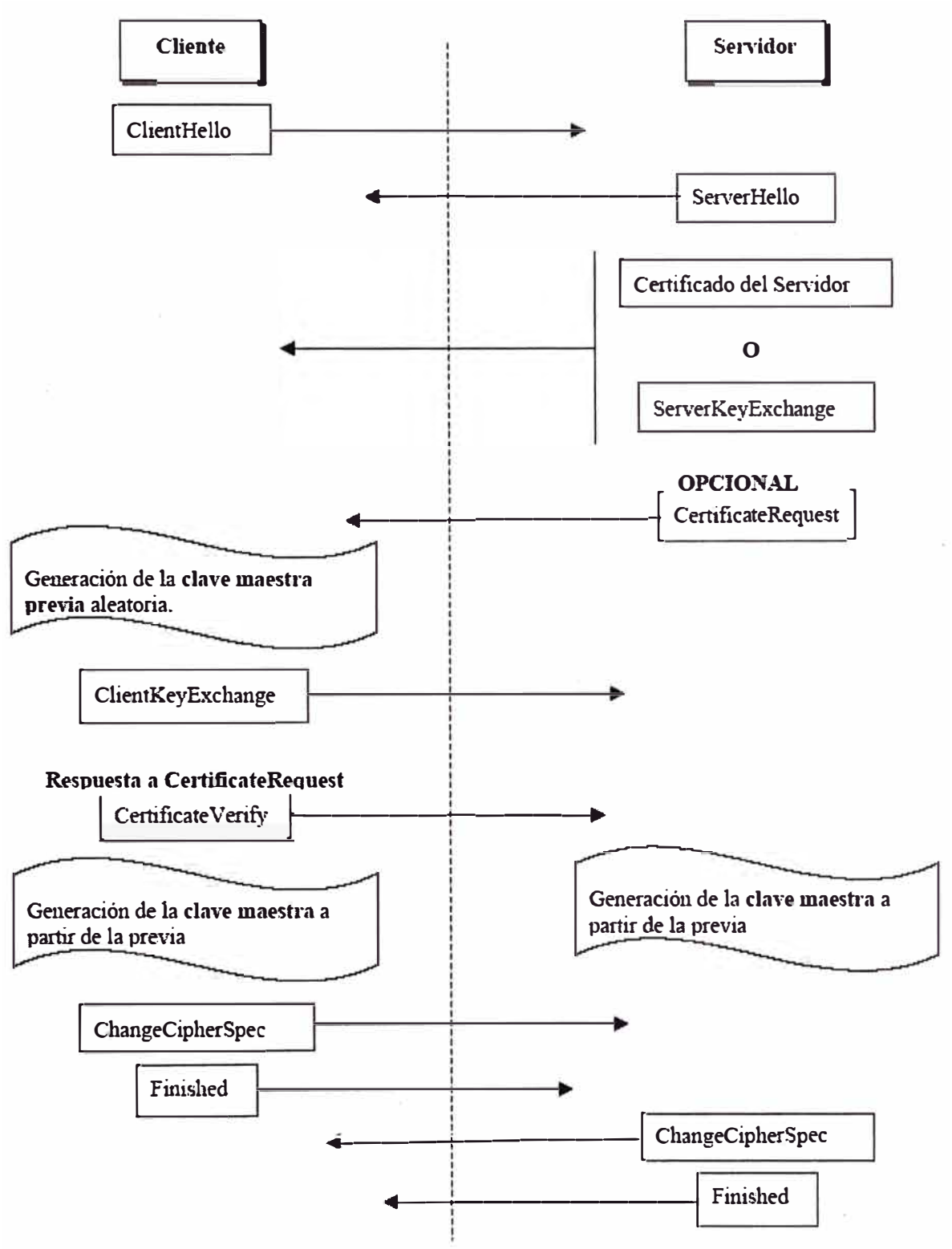


Figura 3.5 Protocolo Handshake de SSL

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, sino no tiene se puede utilizar el mensaje ServerKeyExchange para enviar la clave pública sin certificado. El cliente puede elegir si accepta 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.

### 3.1.3 Pasos de la Conexión

a) El cliente (esto es, el navegador) abre una conexión al puerto del servidor y envía un mensaje "ClientHello" como se muestra en la Fig. 4.6. "ClientHello" lista las capacidades del cliente, incluyendo la versión de SSL que tiene, los cipher suites que soporta, y los métodos que compresión que tiene.

b) El servidor responde con un mensaje "ServerHello". El servidor regresa un mensaje que contiene los cipher suite y compresión de datos que ha escogido, así como un ID de sesión que identifica a la conexión.

Nota que el servidor es el responsable de escoger el cipher suite y métodos de compresión. Si no hay coincidencias entre los cipher suites soportadas entre el cliente y el servidor, entonces el servidor envía un mensaje de "handshake failure" y termina la conexión

c) El servidor envía sus certificados. Si el servidor esta usando autenticación basada en certificados ( que usualmente así es casi siempre ), el servidor envía su certificado de sitio X.509v3 firmado. Si el certificado esta firmado por una autoridad non-root, el servidor También envía la cadena de certificados firmados que llegan hasta un CA primario.

d) El servidor en vía al cliente un solicitud de certificado (opcional) Si certificado s de los clientes están siendo usados para autenticación de clientes (actualmente raro pero posiblemente se vea mas en el futuro ), el servidor le envía al cliente un mensaje de solicitud de certificado.

e) El cliente envía su certificado ( opcional ). Si el servidor lo ha pedido, el cliente envía su certificado X.509v3 firmado. Si el cliente no tiene un certificado, envía una alerta de "no certificate". El servidor puede decidir abortar en este punto con una falla de conversación (handshake - darse la mano ), o continuar adelante.

f) El cliente envía un mensaje "ClientKeyExchange". Aqui es donde la llave de sesión simétrica es escogida. Los detalles varían dependiendo de el cipher suite escogido, pero en el caso más típico, el cliente genera un secreto "pre-master" usando un buen conjunto números generados aleatoriamente. Este número secreto será usado tanto del lado del cliente como del servidor para generar el verdadero número secreto que es usado como la llave de la sesión (puesto que diferentes cifradores simétricos usan diferentes tamaños de llave, la llave de la sesión no es generada directamente). El navegador cifra el número secreto usando la llave publica RSA del servidor (que la obtuvo del certificado del servidor) para crear un sobre digital. El sobre es enviado al servidor.

g) El cliente envía un mensaje de "CertificateVerify" ( opcional). Si se esta usando autenticación del cliente, el cliente se tiene que autenticar con el servidor mostrando que el conoce la llave privada de RSA correcta. El mensaje "CertificateVerify" consiste en el número secreto pre-master generado en el paso 6, que ha sido manipulado en varios formas para que sea mas difícil de verlo si alguien esta escuchando la conversación. El número secreto es firmado con la llave secreta RSA del cliente y enviado al servidor, que procede a validarla chocándola contra el certificado del cliente. Nótese que el servidor no tiene que probar su identidad. Puesto que el cliente envía el número secreto pre-master

al servidor usando la llave publica del servidor, solo el legitimo poseedor del certificado del servidor podrá descifrarlo y usarlo.

h) El cliente y el servidor envían el mensaje "ChangeCipherSpec". Este es un mensaje sencillo que confirma que tanto el cliente con el servidor están listos para empezar la comunicación usando la llave y cifrado acordado.

i) El cliente y el servidor envían el mensaje "finished" (terminar). Este mensaje consiste en el hash de MD5 y SHA de toda la conversación hasta este punto y permite a las partes confirmar que los mensajes fueron recibidos intactos y no fueron modificados en el camino.

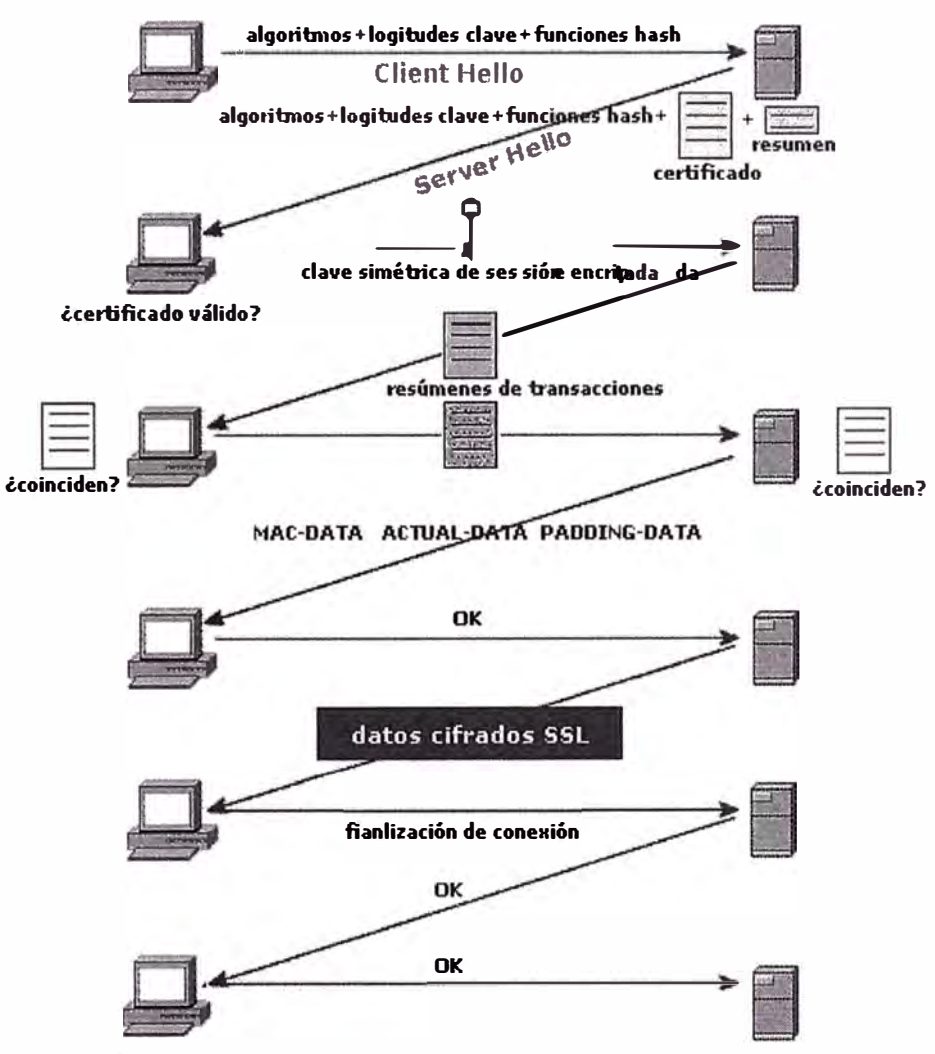


Figura 3.6 Pasos de la Conexión

En este punto tanto el cliente como el servidor cambian a modo cifrado, usando la llave de la sesión (generada de el secreto pre-master) para cifrar simétricamente transmisiones subsecuentes en ambos sentidos.

### 3.1.4 Ventajas e Inconvenientes de SSL

La tecnología basada en los protocolos Secure Socket Layer proporcionó grandes avances en la implantación de sistemas de comunicación seguros, que han hecho posible un crecimiento importante en las transacciones por Internet. Si estudiamos SSL desde el punto de vista de las bases necesarias para considerar una comunicación segura podemos sacar las siguientes conclusiones:

**Autenticidad**: SSL requiere para su funcionamiento la identificación del servidor web ante el cliente y la realiza adecuadamente, pero normalmente no se produce una identificación en sentido contrario. Es decir, no es obligada en la mayoría de los casos la presencia del certificado del usuario que se está conectando al servidor.

Por ejemplo, una de las aplicaciones más comunes de SSL es el de las aplicaciones bancarias. Cuando nos conectamos a la página web de nuestro banco para consultar las cuentas o realizar alguna operación, el servidor web tan sólo nos pide las contraseñas de acceso, lo que conlleva los típicos problemas a la hora de manejar claves: cambiarlas cada cierto tiempo, mantenerlas bien protegidas, elegirlas adecuadamente, etc. Y el tema e complica cuando tenemos que seguir las mismas precauciones con cada una de las diferentes claves que los diferentes bancos y servidores seguros nos requieren.

Otro de los usos comunes de SSL es la protección de números de tarjetas de crédito o débito en compras por Internet. Pero como no se exige el uso del Certificado de Cliente, cualquier persona que obtenga el número de nuestra tarjeta y unos pocos datos personales nuestros puede realizar compras en nuestro nombre. Esto conlleva el tener que prestar mucha atención a los resguardos de nuestras operaciones en cajeros automáticos, a desconfiar cuando un empleado de una tienda o cafetería desaparece con nuestra tarjeta para cobrar el importe de nuestra compra, etc.

Este es precisamente uno de los tipos de fraude más comunes y que causa mayores pérdidas a las compañías de crédito, lo que origina que éstas añadan una comisión en las compras bastante elevada (sobre un 5%), lo que incrementa el precio final del producto a la venta.

**Confidencialidad**: SSL proporciona una buena seguridad de que los datos no van a ser capturados por extraños en el proceso de transferencia de los mismos, pero no proporciona ninguna seguridad después de finalizar la conexión.

Supongamos que realizamos una compra por Internet, para la cual enviamos los datos de nuestra tarjeta de crédito mediante SSL. Dichos datos quedan en poder del responsable de la tienda, que normalmente los almacena en una base de datos. Con ello, el número de nuestra tarjeta y demás datos quedan en un medio que no controlamos y que no tiene porqué ser seguro, pudiendo tener acceso a los mismos cualquier empleado de la tienda, un hacker que entre en el ordenador en el que reside la base de datos, etc.

**Integridad**: ocurre algo parecido a lo anterior. En el corto proceso que dura el envío de datos sí podemos estar seguros de que éstos no van a ser modificados, puesto que SSL lo impide. Pero una vez que finaliza la conexión segura no podemos estar tranquilos.

Por ejemplo imaginemos ahora que después de realizar nuestra compra el responsable de la tienda decide cambiar los datos del pedido, y en vez de enviarnos una grabador de CD a $ 27 nos envía 5 de $ 33. ¿Qué podemos hacer cuando nos lleguen a casa los grabadores de CD y la factura del banco?. No podemos hacer nada, ya que no hay ningún recibo válido del pedido que hicimos.

**No Repudio**: en este aspecto SSL falla al máximo, ya que no hay por defecto establecido nigún método para dejar constancia de cuándo se ha realizado una operación, cuál ha sido y quiénes han intervenido en ella. SSL no proporciona formas de emitir recibos válidos que identifiquen una transacción.

Vamos ahora a suponer que realizamos un pedido a una tienda on-line, un ordenador por ejemplo, y que cuando nos llega a casa decimos que nosotros no hemos hecho ninguna compra, devolvemos el ordenador y requerimos la devolución del dinero. ¿Cómo puede demostrar el comerciante que en verdad le hicimos el pedido?. Mediante SSL, de ninguna forma.

A todo esto hay que añadir que SSL sólo proporciona seguridad en la transacción cliente-servidor seguro, pero queda otra fase de la transacción, la que va desde el servidor seguro a la empresa emisora de la tarjeta de crédito, y sobre ésta no tenemos ningún tipo de control.

Con SSL toda la seguridad de la transacción recae en la confianza que el cliente tenga en el vendedor, pues en las manos del mismo está el ser honrado y no realizar ningún fraude con los datos obtenidos y en la posterior entrega del producto comprado. Por este motivo, sólo las empresas con una honradez demostrada podrán a priori ganarse la confianza de los potenciales clientes.

Vemos pues que SSL carece de muchos de los elementos necesarios para construir un sistema de transacciones seguras usando Internet. Para intentar paliar estos fallos se han intentado sacar al mercado y estandarizar otros sistemas diferentes, como SET, que veremos a continuación, pero el caso es que hasta ahora ninguno de ellos ha conseguido desplazar a SSL.

A pesar de sus fallos, SSSL es una tecnología rápida, fácil de implementar, barata y cómoda para el usuario, que no tiene que conocer cómo funciona, tan sólo usarla. Y desde el punto de vista del comerciante o de la empresa que le facilita el hosting, SSL es igualmente sencillo de implementar, no precisando de servidores de características especiales.

### 3.2 Protocolo TLS – Transport Layer Security

El TLS es un protocolo estandarizado por el IETF, por lo tanto, es un estándar de facto de Internet. Su origen es el SSL versión 3 pero se aparta de éste para mejorar algunas cosas y, sobre todo, porque SSL es propiedad de una empresa privada: Netscape.

Así el **TLS** puede ser el **estándar mundial** para todo el software de cliente y servidor. El TLS permite **compatibilidad con SSLv3**, el cliente y el servidor definen el protocolo utilizado durante el Handshake.

Las diferencias más importantes son sobre los siguientes aspectos:

- **Alerta de certificado**. En respuesta al mensaje CertificateRequest los clientes que no tienen certificado sólo contestan con un mensaje de alerta si son SSL.
- **Claves de sesión**. Se calculan de forma diferente.
- **Algoritmos de intercambio de claves**. El TLS no soporta el algoritmo Fortezza Kea del SSL, un algoritmo secreto y de propiedad privada muy similar al Diffie Hellman.
- **Campos incluidos en el MAC**. En TLS se utilizan dos campos más del mensaje que en SSL para el cálculo del MAC. Es más seguro.

## 3.3 Protocolo S-HTTP

El protocolo Secure HTTP fue desarrollado por Enterprise Integration Technologies, EIT, y al igual que SSL permite tanto el cifrado de documentos como la autenticación mediante firma y certificados digitales, pero se diferencia de SSL en que se implementa a nivel de aplicación. Se puede identificar rápidamente a una página web servida con este protocolo porque la extensión de la misma pasa a ser .shtml en vez de .html como las páginas normales.

El mecanismo de conexión mediante S-HTTP, que ahora se encuentra en su versión 1.1, comprende una serie de pasos parecidos a los usados en SSL, en los que cliente y servidor se intercambian una serie de datos formateados que incluyen los algoritmos criptográficos, longitudes de clave y algoritmos de compresión a usar durante la comunicación segura.

En cuanto a estos algoritmos, lo usados normalmente son RSA para intercambio de claves simétricas, MD2, MD5 o NIST-SHS como funciones hash de resumen, DES, IDEA, RC4 o CDMF como algoritmos simétricos y PEM o PKCS-7 como algoritmos de encapsulamiento.

A diferencia de SSL, el protocolo S-HTTP está integrado con HTTP, actuando a nivel de aplicación, como ya hemos dicho, negociándose los servicios de seguridad a través de cabeceras y atributos de página, por lo que los servicios S-HTTP están sólo disponibles para el protocolo HTTP. Recordemos que SSL puede ser usado por otros protocolos diferentes de HTTP, pues se integra a nivel de socket.

## 3.4 Protocolo SET

### 3.4.1 Características de SET

El SET es un protocolo inventado **exclusivamente para realizar comercio electrónico con tarjetas de crédito**. Fue impulsado por las empresas de tarjetas de crédito Visa y MasterCard, las más extendidas e importantes del mundo. Han colaborado en su desarrollo las empresas más significativas del mundo de la telemática: GTE, IBM, Microsoft, SAIC, Terisa, Verisign, etc... La participación de estas empresas tan importantes y especialmente el impulso de las marcas de tarjetas Visa y MasterCard hacen que este protocolo tenga muchas posibilidades de convertirse en el futuro sistema de comercio electrónico seguro.

Es un **sistema abierto y multiplataforma**, donde se especifican protocolos, formatos de mensaje, certificados, etc. sin limitación de lenguaje de programación, sistema operativo o máquina. El **formato de mensajes** está basado en el estándar definido por la empresa RSA Data Security Inc. **PKCS-7**, como los protocolos S-MIME y SSL.

La especificación del SET v1.0 está contenida en 3 volúmenes publicados en mayo de 1997 y es de libre distribución en la web www.setco.org. El organismo SETco homologa los módulos de programación y los certificados desarrollados por empresas privadas, después de pasar unos tests técnicos y pagar unos derechos. El software homologado por SETco tiene derecho a llevar el logotipo de SET.

**El protocolo SET se puede transportar directamente en TCP, mediante correo electrónico con SMTP o MIME y en Webs con HTTP**.

### 3.4.2. Agentes del Comercio Electrónico de SET

En SET se definen **5 agentes** que pueden intervenir en transacciones comerciales:

- **Comprador**. Adquiere un producto utilizando la tarjeta de crédito de su propiedad.
- **Banco o entidad financiera** (Issuer). Emite la tarjeta de crédito del comprador.
- **Comerciante** (Merchant). Vende los productos.
- **Banco del comerciante** (Acquirer). Banco donde el comerciante tiene la cuenta.
- **Pasarela de pagos** (Payment gateway). Gestiona la interacción con los bancos. Puede ser una entidad independiente o el mismo banco del comerciante.

Dos agentes relacionados pero que no actúan directamente en las transacciones son:

- **Propietario de la marca de la tarjeta**. Avalan las tarjetas: Visa, MasterCard, American Expres, etc...
- **Autoridad de certificación**. Crea los certificados que se utilizan en las transacciones de la pasarela, el vendedor y el comprador. Pueden ser los bancos, los propietarios de la marca de la tarjeta o entidades independientes.

Se relacionan entre ellos como marca la Figura 3.7

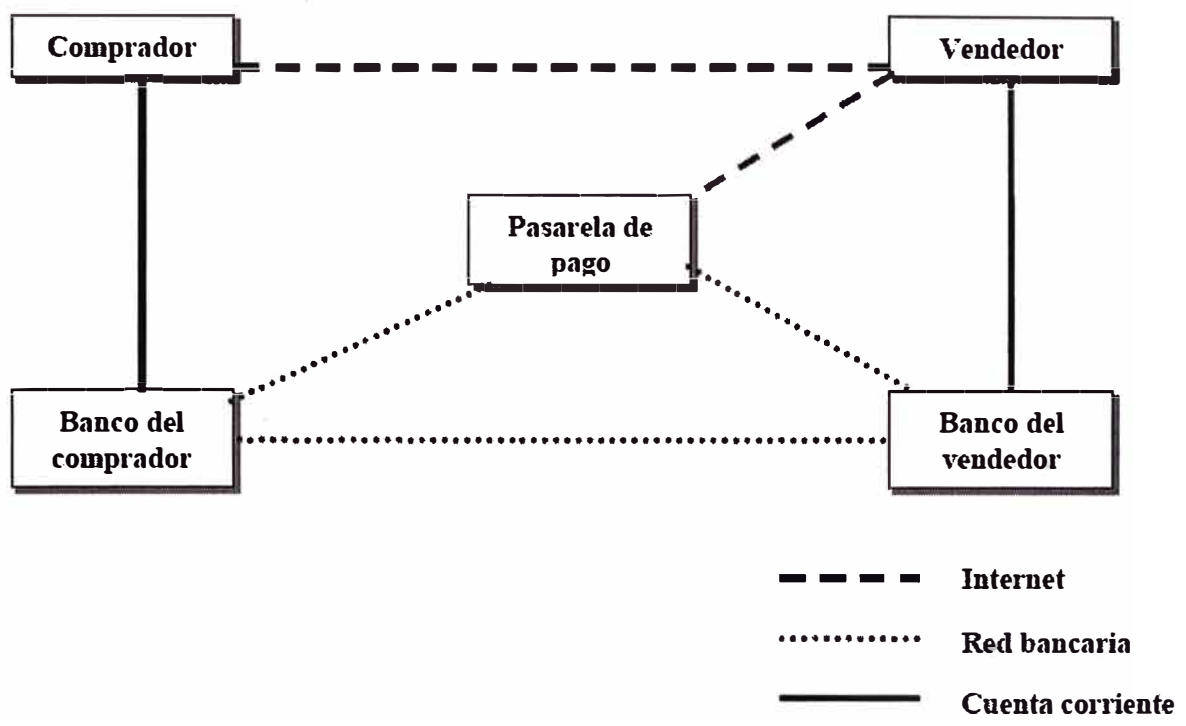


Figura 3.7 Agentes del SET

### 3.4.3 Servicios que Ofrece Set

**a) 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.

**b) 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.

**c) Integridad**: garantiza que la información intercambiada, como número de tarjeta, no podrá ser alterada de manera accidental o maliciosa mientras viaja a través de la red. Para lograrlo se utilizan algoritmos de firma digital.

**d) 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.

### 3.4.4 El Funcionamiento de SET

**Módulos de programación**

Para poder utilizar el SET se deben incorporar unos módulos de software que adaptan los programas existentes al protocolo. Se han definido 4 **módulos**:

**a) Cartera** (Wallet). Es una aplicación que se instala en el navegador del comprador como plug-in.

**b) De venta** (merchant). Se conecta a la Web del vendedor. Como se parece mucho a los actuales terminales punto de venta para tarjetas se le llama también TPV.

**c) Pasarela de pagos** (payment geteway). Cumple las funciones de este agente.

d) **Autoridad de certificación** (CA). Crea certificados de clave pública adaptados al estándar SET.

Los 4 módulos se pueden **homologar** por separado en la entidad **SETco**, actualmente ya hay varias empresas que ofrecen productos comerciales de alguno de los módulos con sello SET.

La **firma dual** es un concepto nuevo de firma inventado por el SET, para dos documentos relacionados resuelve el compromiso entre su privacidad mutua frente a la necesidad de demostrar que están relacionados comercialmente.

En una transacción SET:

- **El vendedor no debe saber los datos bancarios del comprador.**
- **El banco no debe saber la información del producto vendido.**

Pero los documentos con la información bancaria y la del producto deben estar ligados por la misma firma, de manera que se pueda comprobar que han sido generados por la misma persona y para el mismo fin. En las transacciones del SET el comprador genera dos documentos:

- **Información de pedido (OI)**. Donde se describen los datos del producto, el precio y todas las informaciones necesarias para realizar la compra. Este documento sólo puede ser visto por el vendedor.

• **Instrucciones de pago (PI)**. Donde se describen los datos bancarios del comprador y se dan instrucciones para el pago de la cantidad de venta. Este documento sólo puede ser visto por la pasarela de pago.

La firma dual del OI y el PI se realiza concatenando los resúmenes de los dos y después encriptandolos con la clave privada del comprador (ver Figura 3.8).

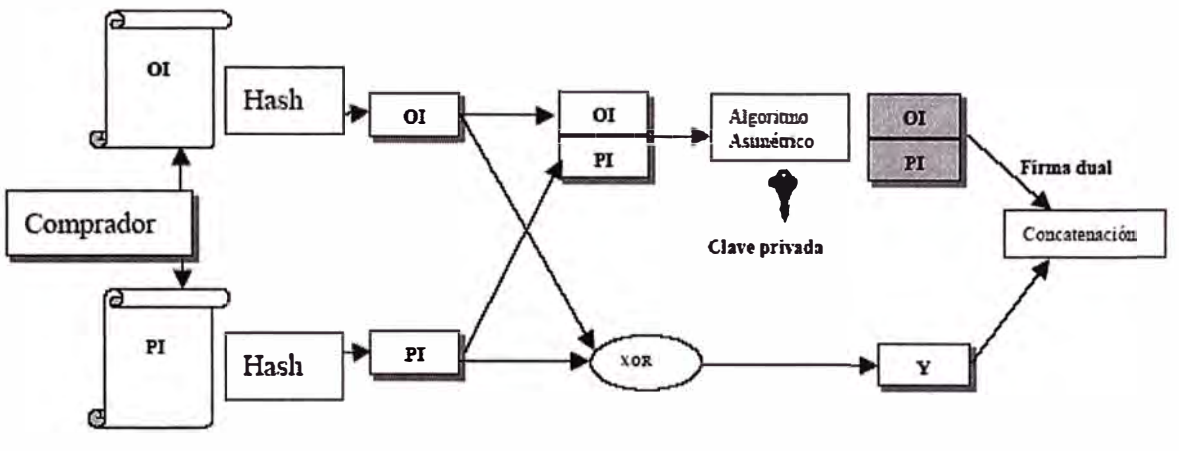


Figura 3.8 Firma Dual de SET

El comprador no se conecta directamente con la pasarela de pagos, envía al vendedor todos los documentos pero la información para la pasarela se encripta con la clave pública de la pasarela. Cuando el vendedor ha comprobado la información dirigida a él, envía la parte encriptada a la pasarela.

En SET:

El vendedor recibe del comprador el OI y la firma dual.

Comprueba la autenticación del comprador y la integridad del OI. (Ver Figura 4.8)

La pasarela de pagos recibe del comprador:

• PI.

• Firma dual.

Del vendedor:

• Resumen del OI.

Con el mensaje del comprador comprueba la autenticación del comprador y la integridad del PI. Con el mensaje del vendedor comprueba la relación entre el OI enviado al vendedor y el utilizado para la firma dual recibida. (Ver Figura 4.8)

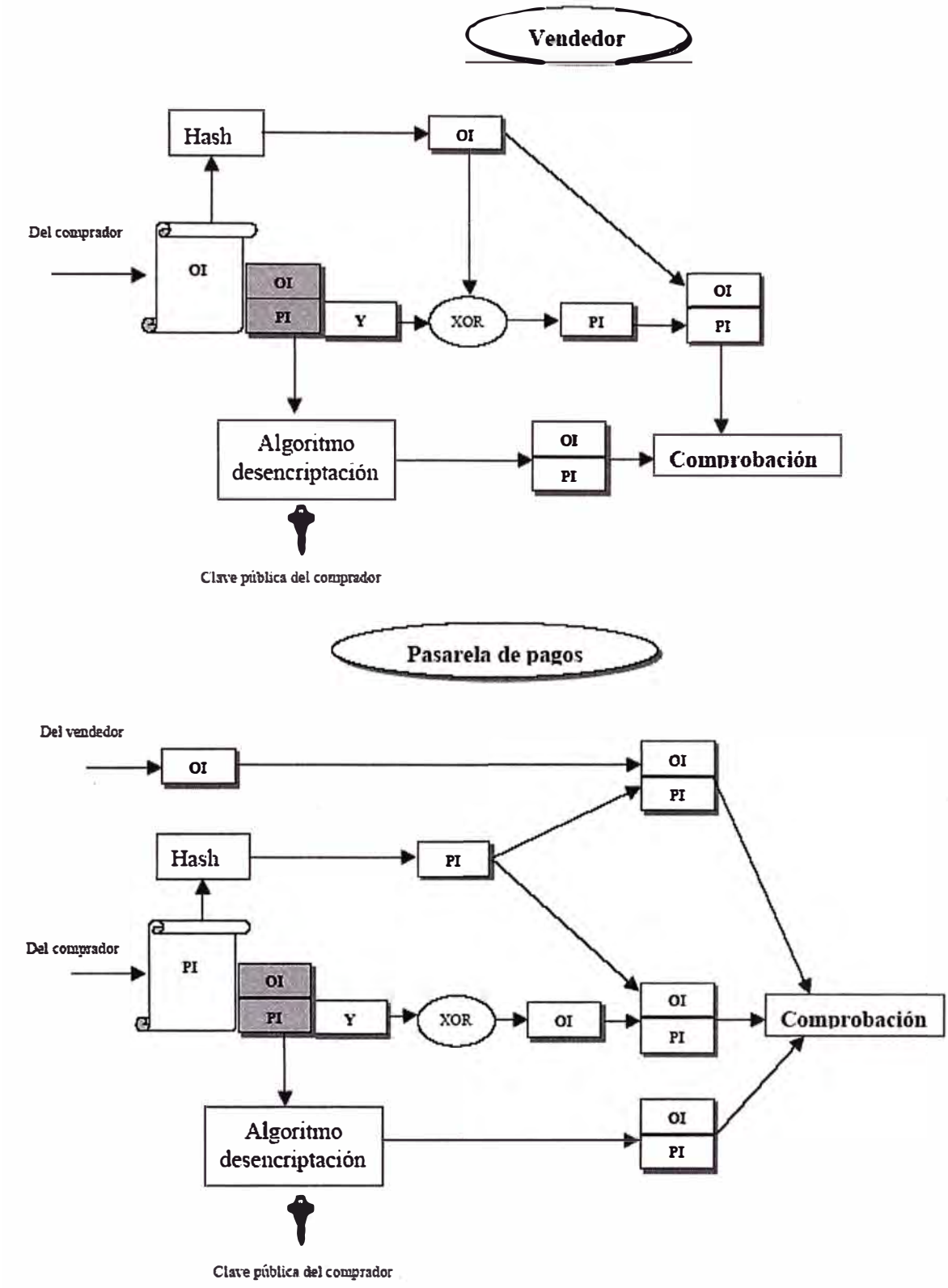


Figura 3.9 Tratamiento de los mensajes PI y OI en SET

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.

# CAPITULO IV

# COMERCIO ELECTRONICO

## 4.1 ¿Qué es el Comercio Electrónico?

Cuando escuchamos el término “comercio electrónico” inmediatamente lo asociamos con la venta de bienes de una empresa a través de Internet. La verdad es que no estamos tan alejados de la realidad porque nos referimos a un tipo especial de comercio electrónico, que es la venta electrónica. La comisión europea define el comercio electrónico como "cualquier actividad que involucre a empresas que interactúan y hacen negocios por medios electrónicos, bien con clientes, bien entre ellas, o bien con la Administración. Se incluye el pedido y pago electrónico y on-line de bienes que se envían por correo u otro servicio de mensajería, así como el envío on-line de servicios como publicaciones, software e información. Asimismo, se incluyen actividades como diseño e ingeniería cooperativa, Marketing, comercio compartido, subastas y servicios post-venta”. En palabras simples es "cualquier transacción comercial en que las partes interactúan electrónicamente en vez de por contacto o intercambio físico directo”.

Si nos referimos al comercio electrónico con un lenguaje más técnico, es el nombre con el que se define el comercio en redes informáticas de carácter privado o público. Las redes informáticas privadas son redes que permiten el acceso autentificado de usuarios a los distintos recursos de la misma mientras que las redes públicas son aquellas redes que, como la red Internet, ofrecen un acceso libre y global de información. En todo proyecto de comercio electrónico existen tres componentes o partes bien diferenciadas. Estas son el comerciante, el proveedor de contenidos y/o servicios y el cliente o visitante casual. El comerciante es aquella persona encargada de hacer llegar el producto o artículo al cliente o usuario final, el proveedor de contenidos y/o servicios es aquella persona encargada de ofrecer el soporte tecnológico necesario para permitir el

enlace entre comerciante y cliente, finalmente el cliente es aquél que llevará a cabo la compra o adquisición del artículo o servicio publicado.

En resumen, la idea es, realizar transacciones económicas, de compra o venta, en forma ágil, rápida y directa entre comprador y vendedor, favorecida por la comodidad y facilidad de utilización por parte de los usuarios en Internet. La evolución de la informática, y el fin del aislamiento del usuario que ha provocado Internet generan múltiples aplicaciones, que corroboran el futuro de este medio. El Comercio Electrónico, el dinero electrónico, el monedero electrónico, son conceptos y términos que ya empiezan a ser reconocidos cotidianamente, y que poco a poco se irán intercalando en el uso y costumbres sociales y económicas.

### 4.2 Arquitectura del Comercio Electrónico

El comercio electrónico abarca todos los conceptos relacionados con procesos de mercado entre entidades físicas o jurídicas a través de redes telemáticas. Por los tipos de usuarios se pueden diferenciar dos grandes grupos:

**a) Comercio entre empresas**. Se caracteriza por tener un segmento de clientes posibles limitado, así permite utilizar tecnologías que no necesariamente han de ser estándares al alcance de cualquiera.

**b) Comercio entre empresas y usuarios domésticos anónimos**. El segmento de clientes es toda la red, en la mayoría de casos Internet, y únicamente está limitado geográficamente por los servicios de transporte del producto. Es conveniente utilizar sistemas estándares y muy extendidos.

Como en todas las transacciones, en el comercio electrónico intervienen varios agentes que se deben comunicar. Los **agentes mínimos** en un sistema de comercio electrónico son:

- **Comprador**. Adquiere el producto o servicio.
- **Comerciante**. Vende el producto o servicio.
- **Entidades y servicios financieros**. Autorizan los pagos y realizan los movimientos de dinero entre comprador y comerciante.

Además las **entidades y servicios financieros** pueden ser diversos en la misma transacción:

- **Banco del comprador**.
- **Banco del vendedor**.
- **Pasarela entre bancos**.
- **Marca de la tarjeta de crédito o débito si se utiliza**.

• **Broker para micropagos**.

También puede haber entidades implicadas en la seguridad como una autoridad de certificación, o en la logística como las empresas de transportes. Todos los agentes de la transacción han de estar comunicados mediante la red o físicamente, aunque un sistema ideal sólo utilizaría la red. Dependiendo del medio de pago y del sistema de seguridad se utilizarán unos agentes o otros.

Una transacción siempre se realiza con estas cuatro fases:

**1.** El comprador obtiene los datos del producto o servicio del vendedor.

**2.** Se solicita la autorización de pago del comprador.

**3.** Se confirma la autorización y se paga al vendedor (en algunos sistemas el pago puede realizarse después de la cuarta fase).

**4.** Se entrega el producto o servicio mediante un transporte físico o por la red.

Existen diversas **formas de pago** en el comercio electrónico que se pueden agrupar en cuatro familias:

• **Dinero electrónico**.

• **Sistemas de crédito y débito**.

• **Tarjetas de crédito y débito**.

• **Sistemas de micropagos**.

Los **protocolos de seguridad** más utilizados actualmente son:

• **SSL/TLS**. Es un protocolo de seguridad para cualquier aplicación de Internet y, por lo tanto, se puede utilizar en el comercio electrónico. Está muy extendido y actualmente todos los navegadores comerciales lo implementan.

• **SET**. Es un protocolo especialmente diseñado para el comercio electrónico con tarjetas de crédito. Actualmente se encuentra en su fase de desarrollo.

Un caso particular del comercio electrónico es cuando la cantidad a pagar es más pequeña que los costes de transacción, en estos casos se deben utilizar sistemas especiales denominados de **micropagos**.

### 4.3 Requisitos del Comercio Electrónico

El principal requisito en una transacción de comercio electrónico es la seguridad, como en todas las transacciones que implican el manejo de dinero. Pero hay otros

requisitos aconsejables para que los sistemas de comercio electrónico sean comparables a los de monedas y billetes, sino no se aplican puede que el comercio electrónico no sea atractivo para los usuarios. Estos son:

• **Anonimato**. Con monedas o billetes la identidad del comprador no es conocida por los vendedores. Para poder mantener también en el comercio electrónico el derecho propio de los humanos a la intimidad, nadie excepto el banco propio deberían conocer la identidad del comprador y éste no debería conocer la naturaleza de la compra.

• **Flexibilidad**. Poder aceptar diferentes medios de pago para todas las situaciones posibles de usuarios de Internet.

• **Convertibilidad**. Poder transformar los diferentes sistemas de pago sin necesidad de realizar una compra, como pasa con las divisas y las cuentas de los bancos.

• **Eficiencia**. El coste del sistema de comercio no debe ser mayor que el precio del producto o servicio.

• **Ser divisible**. Como las monedas o billetes poder dividir la posibilidad de compra en fracciones más pequeñas.

• **Transferible**. Poder pasar el poder de compra de una persona a otra sin necesidad de realizar una transacción, igual que se puede prestar o regalar el dinero tradicional.

**El único sistema de pago que cumple todos los requisitos es el dinero electrónico**.

### 4.3.1 Dinero Electrónico

Estos sistemas deben cumplir todos los requisitos comentados en el apartado 1.2, 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 valúa depende de la longitud del número y se pueden fraccionar cambiándolos en la entidad. Los usuarios los piden por la red a la entidad a cambio de un cargo a su cuenta o tarjeta y los utilizan o dan 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, así como prestar. Estos sistemas ya se utilizan en las compras físicas, pero para Internet se deberían construir ordenadores con lectores adecuados.

### 4.3.2 Sistemas de Crédito y Débito

En estos sistemas el usuario debe tener una cuenta con la entidad que gestiona los pagos, esta cuenta puede recibir dinero real o estar conectada a una cuenta real de un banco y recibir cargos por las compras.

Pueden ser de:

- **Débito**. Se debe tener dinero en la cuenta para cubrir el gasto.
- **Crédito**. La entidad puede dar crédito hasta el día del pago completo o fraccionado.

Los usuarios se deben dar de alta en el sistema y abrir la cuenta, después reciben un password o otra manera de identificarse. Al realizar compras en las tiendas virtuales que permiten este forma de pago se debe indicar el password o identificador y entonces se comprueba si el pago está autorizado.

Utilizan este sistema entre otras las entidades: NetCheque, NetBill, FirstVirtual, InfoCommerce, Virtu@lCash, etc... Probablemente cada vez se utilizarán menos debido a la tendencia hacia sistemas universales que no dependen de darse de alta en una entidad. Pueden servir para realizar micropagos.

### 4.3.3 Tarjetas de Crédito o Débito

Son los más utilizados y posiblemente los que se extiendan más en el futuro. Se trabaja con una tarjeta de crédito o débito cargando la compra como si se hubiera hecho en una tienda física. No cumple los requisitos de anonimato, aunque el sistema de seguridad SET permite que el vendedor no conozca los datos de la tarjeta del comprador y el banco los datos del producto o servicio comprado.

### 4.3.4 Sistemas de Micropagos

Los micropagos en comercio electrónico ocurren cuando el precio del producto o servicio es muy pequeño y puede ser menor que coste de la transacción realizada mediante los métodos habituales.

La característica fundamental de estos sistemas es bajar mucho los costes de la transacción a costa de pérdida de seguridad. Su principio se basa en que las transacciones son tan pequeñas que no resultan atractivas para realizar un ataque, así los esfuerzos realizados por el ladrón no compensan el valor del robo.

Se utilizan unos intermediarios llamados **Brokers**. Es normal que un comprador realice muchos micropagos a muchos vendedores diferentes y que un comerciante reciba muchas compras de poco valor de muchos compradores diferentes. Gestionar estas interacciones múltiples entre compradores y vendedores por muy poco margen de beneficio no interesa a ninguna de las partes. Así se utilizan brokers que concentran todas las compras de un comprador y todas las ventas de un comerciante y así simplifican el modelo (Ver Figura 4.1)

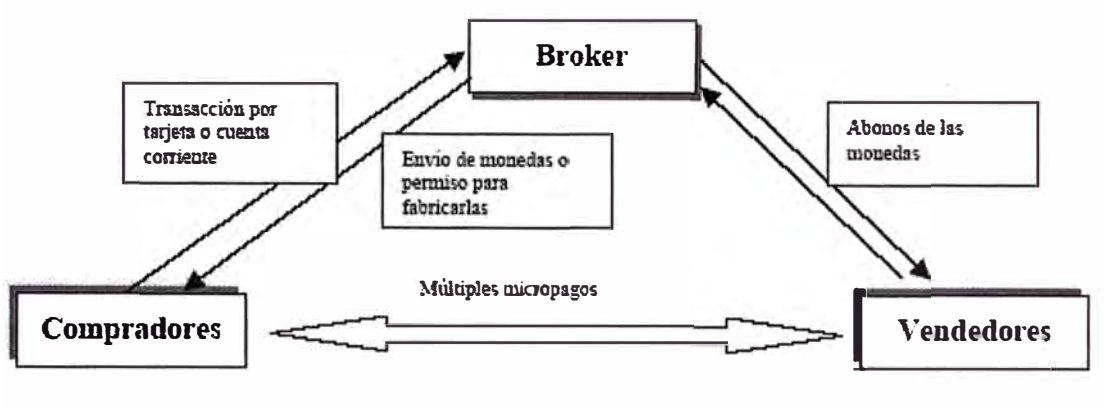


Figura 4.1 Arquitectura de un Sistema de Micropagos

Actualmente no existe un estándar para realizar micropagos sino que existen varios sistemas que compiten para ser el futuro estándar, algunos ya se están utilizando. Unas características comunes a la mayoría son:

• **Utilización de dinero electrónico**. Utilizan sistemas con características de dinero electrónico (ver apartado 1.3 *Dinero electrónico*). Las unidades de transacción se llaman **monedas electrónicas** y pueden ser generadas por el broker o por el comprador que posee un permiso firmado por el broker.

• **Cambio**. Los vendedores tienen la posibilidad de devolver cambio o las monedas se pueden fragmentar.

• **Detección de doble pago**. Para detectar la doble utilización de las monedas electrónicas los vendedores mantienen una base datos con los mensajes moneda recibidos, esto se debe mantener hasta la caducidad de estos mensajes. Esta prestación obliga en la mayoría de sistemas a editar monedas especificas para un vendedor y, por lo tanto, se pierde la flexibilidad de sistema universal.

• **Cifrado débil**. Para aumentar la velocidad de proceso y facilitar la gestión de claves no se acostumbra a utilizar encriptación de clave pública, pero si se utiliza, se procura minimizar el número de ejecuciones del algoritmo. Normalmente la seguridad se implementa mediante funciones Hash con o sin clave.

Algunos de los sistemas más conocidos son:

• **Millicent**. Las monedas electrónicas se denominan *scrips*. La seguridad se basa en una clave secreta compartida entre el vendedor y el broker. No utiliza encriptación sólo funciones Hash con clave. Los *scrips* están marcados para un comprador y un vendedor determinados, se compran al Broker.

• **MicroMint**. Permite diferentes formas de monedas: anónimas (poca seguridad), marcadas para el comprador y marcadas para el vendedor. Como seguridad solamente utiliza la propiedad de resistencia a colisiones de las funciones Hash. Las monedas se compran al broker.

• **Payword**. Las monedas son cadenas de resúmenes realizados por funciones Hash, denominadas *Paywords*, cada elemento de la cadena es la función Hash del anterior y el primero es un número aleatorio. Los Payword son generados por el comprador y sirven para cualquier vendedor. Para generar Paywords se debe poseer un certificado de clave pública firmado por el broker, donde aparece la cantidad máxima que se puede gastar en una transacción. Es un sistema de crédito donde el broker responde del cliente (como las tarjetas). En cada compra se realiza una única encriptación de clave pública.

• **SubScrip**. Utiliza un mensaje llamado ticket que es específico para un vendedor y un comprador. El ticket se actualiza en el vendedor después de cada compra, restando la cantidad pagada del total. El vendedor mantiene una base de datos de los tickets y sus últimos valores. Los Brokers generan los tickets.

Tabla 4.1 Comparación de los 4 Sistemas

| | Millicent | MicroMint | Payword | SubScrip |
|---|---|---|---|---|
| Encriptación | NO | NO | SI | NO |
| Hashing | SI, con clave | SI | SI | NO |
| Monedas especificas de venddedor | SI | Depende | No | Si |
| Monedas especificas del comprador | Si | Depende | Si | Si |
| Genera las monedas | Broker | Broker | Comprador | Broker |

## 4.4 Tipos de Comercio Electrónico

El comercio electrónico puede adoptar diversas formas fundamentales:

### 4.4.1 Empresa – Empresa (B2B)

Se trata de todas aquellas actividades en las que un proveedor vende algún producto o servicio a un cliente industrial o profesional. Se puede extraer un gran rendimiento a la Red en este sentido ya que Internet hace posible la disminución de los costes de transacción entre las empresas, en otras palabras, encontrar proveedores, negociar con ellos y coordinar los suministros puede hacerse más barato mediante Internet.

De esta forma, un proveedor puede poner en su web todo un catálogo de productos de manera que sus clientes puedan hacer sus pedidos de manera más cómoda y personalizada. Incluso pueden crearse páginas con catálogos personalizados para cada cliente en las que se especifiquen los productos que adquiere habitualmente y los precios a los que se ofrecen dichos productos en función de su volumen de compras.

**Tipos de Mercados B2B**

Existen cuatro grandes tipos de mercados negocio-a-negocio, los cuales se definen en función de dos variables:

Qué compran las empresas:

- Inputs de fabricación o suministros verticales, que suelen ser específicos para cada tipo de sector industrial y se trata de las materias primas y/o componentes para poder fabricar.
- Inputs de operación o suministros horizontales. Se trata de productos o servicios que aunque no son transformados en el proceso de manufactura para generar ouputs finales, son necesarios para llevar adelante las actividades (material de oficina, informática, billetes de avión, mantenimiento de instalaciones, etc.)

Cómo compran las empresas:

Para adquirir los inputs que precisan, ya sean de fabricación o de operación, las empresas utilizan dos tipos principales de procedimientos:

- Suministro sistemático. Determinados inputs se precisan de manera regular para lo cual las empresas poseen una serie de proveedores a los que les une una relación estable negociada en unas determinadas condiciones.
- Suministro puntual (spot sourcing). Utilizada para los inputs que se adquieren en momentos puntuales para satisfacer una demanda inmediata. En este caso se buscan soluciones entre los proveedores que no necesariamente conocen, porque normalmente lo que prima es un suministro rápido al menor coste posible.

Combinando los valores de estas dos dimensiones se identifican cuatro tipos básicos de mercados B2B:

- Centros de ORM (operaciones, reparaciones y mantenimiento). Son mercados que permiten la compra sistemática de inputs de operación. Los productos y servicios que precisan regularmente para sus operaciones: material de oficina, productos informáticos de consumo.
- Yield managers. Mercados verticales que permiten la compra puntual de inputs de operación.
- Bolsas (exchanges). Mercados específicos de sector donde se pueden encontrar y adquirir puntualmente inputs de fabricación. Son lugares donde la oferta y la demanda se encuentran para satisfacer necesidades puntuales y que frecuentemente funcionan mediante mecanismos de subasta.
- Centros de catálogo. Mercados donde las empresas pueden cubrir sus demandas regulares de inputs de fabricación. Se trata de espacios donde proveedores y empresas se encuentran para la satisfacción de suministros a un costo de transacción inferior al habitual.

Cada uno de estos tipos de mercado posee unas ventajas singulares respecto al procedimiento equivalente “en el mundo real”. Quizá por ello el número de mercados **B2B** existentes en el mundo ha crecido de manera muy rápida.

Actualmente, la gran atención del comercio electrónico entre empresas se centra en compañías conocidas y establecidas que han modificado sus modelos de negocio estableciendo un canal directo con el consumidor final. Las empresas se están dando cuenta de que Internet trae consigo un cambio en el modelo de relación con sus proveedores y clientes, que está imprimiendo a estas relaciones un carácter más abierto y un enfoque más colaborativo.

### 4.4.2 Empresa – Consumidor (B2C)

Es la modalidad de comercio electrónico más conocida popularmente, debido a los sectores que involucra: la empresa y sus clientes, se trata del método más conocido como venta electrónica, que usualmente se realiza a través de la World Wide Web de Internet. Existen ya en la actualidad muchos tipos de galerías que ofrecen a través de Internet todo tipo de bienes consumibles, desde computadores a vinos, vehículos, materiales, libros, etc.

Existen tres modelos de negocios diferentes:

**a) Tienda virtual (e-Shop)**.

Se trata de un establecimiento instalado en la red en la que se actúa como intermediario en la venta de productos propios o de terceros. Estas compañías resuelven todo lo relativo al acto de compra: oferta del producto, disponibilidad del producto en almacén, entrega física del producto, sistemas seguros de pago, etc.

Entre sus beneficios destacan la posibilidad de creación de nuevas oportunidades de ventas e ingresos; la recuperación a corto plazo de la inversión inicial y la reducción de costes directos de ventas en personal, teléfono, etc.

Sus características básicas son:

- Sistema en base de datos.
- Configurado para llevar a cabo ventas de productos y servicios.
- Fácil de usar, con un sistema de navegación intuitivo, con simple método de facturación.
- Configurado para publicar nombres de productos, descripciones, e imágenes.
- Capacidad de búsquedas en base a número, nombre, o descripción de productos.
- Número ilimitado de productos.
- Catálogo de productos personalizado.
- Capacidad de promociones especiales.
- Análisis de ventas y datos de clientes.
- Pago automatizado con tarjeta de crédito en tiempo real.

**b) Subasta virtual (eAuction)**

Es la implantación electrónica de un mecanismo de remates on-line. Este servicio se acompaña de una presentación multimedia de los productos expuestos. Dentro de la subasta virtual pueden ofrecerse los mecanismos de pago y entrega necesarios para cerrar el proceso.

Su modelo de negocio gira en torno a la organización de un lugar de contacto entre compradores y vendedores y al cobro de una comisión por cada transacción realizada. Este modelo de negocio que permite poner en contacto particulares que compran y venden se denomina C2C (Consumer to Consumer).

**c) Centro comercial virtual (eMall)**

Los centros comerciales virtuales congregan a una serie de tiendas virtuales que ofrecen sus productos y servicios bajo un nombre de marca común. Su principal ventaja es que permiten gestionar un sólo proceso de compra para todas las tiendas presentes: un sólo carrito, un sólo pago y una sola entrega. Suelen disponer de un medio de pago garantizado. Estas agrupaciones pueden abarcar un único segmento de mercado o tener una presencia general.

### 4.4.3 Consumidor – Consumidor (C2C)

Se refiere a las transacciones privadas entre consumidores que pueden tener lugar mediante el intercambio de correos electrónicos o el uso de tecnologías P2P (Peer to Peer)

Un método sencillo para que las empresas se inicien en el comercio electrónico consiste en colocar una oferta especial en el sitio Web y permitir a los clientes realizar sus pedidos on-line. No es preciso hacer los pagos vía electrónica.

### 5.4.4 Empresa – Administración (B2A)

Aquí se cubre todo tipo de transacciones entre las empresas y las organizaciones gubernamentales. Esta categoría es bastante importante ya que se piensa que a través de ella se podrá promover la calidad, la seriedad y el crecimiento del comercio electrónico.

La e-administración es un servicio a través del cual tanto ciudadanos como empresas pueden realizar en Internet algunos de los trámites administrativos que hasta ahora realizaban en las oficinas públicas.

Con este servicio el usuario se beneficia de numerosas ventajas:

- Ahorro de tiempo en gestiones y colas ya que muchas operaciones se pueden realizar íntegramente a través de un ordenador desde la oficina o desde el propio hogar.
- Permite descargar numerosos formularios y modelos de procedimientos administrativos. De esta forma, los usuarios se ahorran tener que acercarse a las oficinas públicas para recoger determinados documentos o para preguntar los pasos a seguir en una operación.
- La e-administración no tiene horario, es decir, permite que los usuarios accedan a los servicios a cualquier momento del día o de la noche, incluso en días festivos.
- Las oficinas virtuales son puntos continuos de información actualizada. A través de las páginas de la administración podemos saber las últimas novedades en materia de legislación, subvenciones, cursos de formación y todo tipo de información útil para empresas.

### 4.4.5 Consumidor – Administración (C2A)

Esta categoría es la que más dificultades parece encontrar para su emergencia. Sin embargo, a medida que crezcan y se extiendan las categorías anteriores, el gobierno podrá extender las interacciones electrónicas a áreas tales como los pagos de pensiones, el asesoramiento, o las devoluciones de impuestos.

## 4.5 Ventajas Y Desventajas Del Comercio Electrónico

El comercio electrónico ha llevado a la reestructuración de industrias y empresas, lo que genera una serie de ventajas, que analizaremos para las dos formas más importantes de comercio: B2B y B2C.

**Business To Business**

El Comercio Electrónico B2B presenta una serie de ventajas frente al comercio tradicional, algunas de éstas son:

- **Negociar con los clientes:** Este es un aspecto muy importante ya que se puede tener, en el caso de fabricantes, un contacto directo con los clientes finales, aspecto no siempre posible en los mercados tradicionales. Además el contacto es directo y no se verá afectado por los denominados "ruidos", factores que impiden una correcta comunicación.
- **Negociar con los proveedores:** Al igual que en la negociación con los clientes, Internet permite un trato directo con los proveedores. Un aspecto no muy extendido es incluir en la Web de la empresa una página donde se pueda recibir propuestas de posibles proveedores. En dicha página o sección deberá aparecer una lista de los productos que se desea recibir información así como datos relativos a los mismos o a las condiciones económicas, etc.
- **Relación on-line:** Uno de los aspectos más destacados del comercio electrónico es la relación que existe entre oferente y demandante. Dicha relación puede llegar a ser tan directa (salvando las distancias), como la que existiría si el vendedor se desplazase hasta la oficina o empresa de su cliente. Vía Internet se puede presentar catálogos de productos y/o servicios, personalizando la oferta a cada perfil de los clientes, con lo que además de conseguir un trato más directo y personalizado (aspecto muy valorado por cualquier cliente), se consigue satisfacer mas correctamente sus necesidades.
- **Servicio pre y post venta:** Otro aspecto a destacar es la posibilidad de emplear, ya sea la Web o el correo electrónico, como una ayuda a la red de ventas o al servicio post venta o técnico, ofreciendo desde la Web toda aquella información que puedan necesitar los clientes.
- **Reducción de costos:** Todo lo comentado hasta el momento tiene un claro y significativo resultado y no es otro que la reducción de costos, dado que se evitan desplazamientos innecesarios, envío de información, etc. Todo ello además permite que la red de ventas y/o el servicio técnico puedan diversificar su trabajo.

**Business To Consumer**

Este aspecto del comercio en Internet está muy extendido, aunque los expertos pronostican un incremento superior en el B2B, hoy por hoy se puede afirmar que donde mayor éxito se está obteniendo en cuanto a número de empresas y volumen de negocio es en el B2C.

Algunas de las ventajas de esta categoría son:

- **Prolongación del negocio:** Internet puede ser una clara prolongación del negocio. Las oportunidades que presenta Internet como mercado son inmensas. Internet permite llevar el producto a un mercado potencial a nivel mundial.
- **Personalizar el trato:** Otra gran ventaja es la de poder personalizar el trato que se de a cada uno de los clientes. De esta forma el cliente al sentirse diferenciado del resto se sentirá más cómodo en la Web.
- **Formas de pago más ágiles:** En Internet una norma imperante en este tipo de relaciones es la de cobrar antes del envío del producto, por lo que los riesgos y costos financieros son nulos.

A pesar de las múltiples ventajas, el comercio electrónico no está exento de problemas, algunos trasladados del comercio tradicional y otros derivados de su naturaleza digital. Entre ellos:

- **Globalización:** Una empresa puede a través de las redes globales comunicarse con otra empresa del otro extremo del mundo, pero este tipo de contacto no es suficiente ya que de por medio hay un problema de globalización, por ejemplo, ¿cómo se enterará y comprenderá las tradiciones y reglas de negocio de otra empresa que se encuentra inserta en una cultura totalmente diferente?, ¿Cómo será respetada y soportada la diversidad lingüística?. La solución de estas y otras interrogantes similares hará del comercio electrónico global una realidad práctica.
- **Apertura Contractual y Financiera:** El hecho de realizar un pedido con su consiguiente pago en forma electrónica abre una serie de problemas en el sentido de las leyes a las cuales se acogerá el contrato y si se mantendrá en secreto y según las normas tributarias de que país se desarrollará la transacción, en el caso que intervengan empresas de distintos países.

- **Propiedad:** Un problema importante, especialmente para el caso de bienes que pueden distribuirse electrónicamente y pueden ser fácilmente copiados. La protección de la propiedad intelectual y de los derechos de copia es un tema aún por solucionar.
- **Privacidad y Seguridad:** Se necesitan mecanismos eficaces para garantizar la seguridad de las redes abiertas. Además se debe asegurar que las partes que intervienen en una transacción posteriormente no puedan negar su participación.
- **Interconectividad e Interoperatividad:** El comercio electrónico requiere acceso universal, lo que implica una normalización para la interconexión e interoperabilidad de las redes.
- **Riesgo:** Algo que puede limitar el crecimiento del comercio electrónico es la falta de iniciativas y recursos.
- **Información:** La dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor (y del comprador) en una relación electrónica.

### 4.6 El Impulso del Comercio Electrónico Global

Las nuevas tecnologías están produciendo un gran efecto en el mundo comercial. Sectores como el mercado del software, productos lúdicos (vídeos, juegos de ordenador, canciones etc.), servicios de información, servicios técnicos, servicios financieros, así como profesionales están experimentando un crecimiento acelerado en la última década. Un incremento de estas transacciones se ha producido notablemente a través de la red. La infraestructura global de la información tiene suficiente potencial como para revolucionar el comercio en todas estas áreas, ya que con una reducción dramática de los costes de la transacción se permite el florecimiento de nuevas técnicas transaccionales. Además, se revolucionarán las técnicas de marketing así como publicitarias. Nos encontramos con que los consumidores serán capaces de poder comprar desde su propia casa una gran variedad de productos tanto a los fabricantes como a los distribuidores en el ámbito mundial. Serán capaces de ver estos productos en sus ordenadores o televisores, podrán acceder a la información existente sobre los mismos, podrán visualizar los productos de múltiples formas (por ejemplo podrán desde construir una habitación en su pantalla, rellenándola con muebles hasta pasear por el supermercado seleccionando los productos expuestos en sus mostradores virtuales), así como solicitarlos y pagarlos de la forma más sencilla, es decir desde sus casas.

La rapidez con que se están produciendo estos cambios nos hace pensar que el comercio en Internet puede llegar a suponer un movimiento de billones de dólares en los próximos años. Debido a este gran potencial que adquirirá el comercio en las próximas décadas, será necesario buscar un desarrollo armónico del mismo, entre todos los operadores económicos, así como gobiernos y estados de todo el mundo, de forma tal, que se asienten las bases estructurales para un mercado de estas características.

Las posiciones a adoptar deberán pasar por la construcción de un mercado no regulado, orientado al comercio electrónico, que facilite la transparencia y agilidad predicable de un mercado no virtual. Dichas posiciones deben respetar la naturaleza del medio, así como la libre competencia que representa dicho mercado, de forma que, la posibilidad de elección del consumidor se incremente, consolidando un nuevo mercado digital altamente competitivo.

No obstante, muchos comerciantes así como consumidores o usuarios están todavía dudando en conducir sus grandes negocios a través de Internet, debido principalmente a la falta de una ley predecible, capaz de poder regular las transacciones que se produjeren en dicho mercado. Esta postura se observa sobretodo en ámbitos comerciales internacionales donde, son muy relevantes para el comerciante las directrices a seguir en materias como la ejecución de los contratos, la responsabilidad, la protección de propiedad intelectual, la privacidad o derecho a la intimidad, la seguridad y otras tantas materias que han introducido tanto en el comerciante como en el consumidor un cierto estado de precaución.

Al mismo tiempo que la Internet se extiende muchas compañías y sociedades así como usuarios de la red, están preocupados ante la posibilidad de que algunos gobiernos impongan extensas regulaciones en el comercio electrónico que se desarrollan en la red. Con estas acciones pueden llegar a facilitar el comercio electrónico o lo que no es lo mismo, reprimir o retener su desarrollo. El saber cuando actuar o lo que es más importante, no actuar, será crucial para el desenvolvimiento del comercio electrónico. Por ello, y ante el surgimiento de una infraestructura global de la información, con un mercado sin fronteras en el cual todo el mundo tiene acceso, es de suma importancia llegar a un acuerdo internacional entre todos los operadores que intervienen en dicho surgimiento. De esta forma, es conveniente establecer una serie de principios y políticas sobre las que incidir para que se facilite el camino hacia el crecimiento del comercio en Internet.

## 4.7 Facturación Electrónica

El proceso de facturación es casi siempre crítico para cualquier empresa, ya que es un punto obligado de la relación tanto con sus clientes como sus proveedores. En la actualidad las empresas destinan a este proceso grandes cantidades de recursos y están obligadas a realizar muchas tareas en forma manual, dado que los documentos deben generarse en papel. Un buen proceso administrativo de estos documentos tiene como consecuencia no sólo ser un buen control de compras y ventas, sino también en el cumplimiento de sus obligaciones tributarias. Sin embargo, esto es difícil de lograr en un proceso basado en papeles.

### ¿Qué es una Factura Electrónica y cuáles son sus beneficios?

Una Factura Electrónica es una representación informática de un documento tributario, generado electrónicamente y que reemplaza al documento emitido en papel. Una Factura Electrónica permite, al mismo tiempo, dar validez tributaria a operaciones comerciales efectuadas a través de documentos generados y soportados electrónicamente.

Algunos de los beneficios de una Factura Electrónica o Documento Tributario Electrónico (DTE):

- Mejorar los procesos de negocios de los contribuyentes.
- Disminuir sustantivamente los costos del proceso de facturación.
- Potenciar la gestión electrónica de los documentos.
- Posibilidad de imprimir el documento en papel corriente y no prefoliado.
- Mayor resguardo de la información.
- Liberar para siempre el espacio físico de almacenamiento para los documentos en papel.
- Verificación de la validez de la Factura Electrónica a través del sitio web.
- Facilitar el desarrollo del comercio electrónico en nuestro país, contribuyendo de esta manera a impulsar la agenda tecnológica y de modernización del país.

### ¿Qué requisitos debe cumplir una factura electrónica para que sea válida fiscal y legalmente?

Para que una factura electrónica sea válida sólo debe cumplir con dos requisitos: garantizar la autenticidad de origen y la integridad de su contenido. Esto quiere decir

poder identificar unívocamente al emisor y que tener la certeza de que el documento recibido no haya sido alterado. Ambos requisitos se dan por satisfechos si al generar la factura electrónica el emisor le incorpora una firma electrónica que cumpla con las especificaciones mínimas establecidas por las autoridades tributarias.

### 4.8 Marco Legal

La situación del Perú con respecto al Comercio Electrónico tiene una posición expectante, ya que se un medio que ha empezado a desarrollarse con prontitud.

Normas Técnicas Peruanas Publicadas por **INDECOPI**:

Las normas emitidas por el INDECOPI, trata sobre el código de barras y el Intercambio Electrónico de Datos EDI.

Tabla 5.2 Normas Técnicas Peruanas Publicadas por INDECOPI

| NTP | Descripción | Resolución |
|---|---|---|
| NT-ISO/IEC 17799:2004 | EDI. Tecnología de la información. código de buenas prácticas para la gestión de la seguridad de la información | R.M. 224-2004-PCM |

**Congreso de la Republica**

En el Congreso de la Republica, el comercio electrónico es un tema que se encuentra en debate, no habiendo llegado a un acuerdo que pueda darnos una normatividad definida.

Leyes Vigentes en el Perú:

- Ley Nº 27419 del 25 de enero del 2001: Ley sobre la notificación por coreo electrónico. Modificación de los Artículos 163º y 164º del Código Procesal Civil.
- Ley Nº 27269: Ley de Firmas y Certificados Digitales del 8 de mayo del 2000. Esta Ley contiene 16 artículos divididos en los siguientes rubros:

  De la firma digital

  Del titular de la firma digital

- De los certificados digitales
- De las entidades de certificados y de registro
- Además de 3 disposiciones complementarias, transitorias y finales.

- Decreto Supremo Nº 066-2001-PCM
- Ley Nº 27291: Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos paral comunicación de la manifestación de voluntad y la utilización de la firma electrónica del 23 de junio del 2000.
- Ley Nº 27309: Ley que incorpora los delitos informáticos al Código Penal del 15 de Julio del 2001
- Ley Nº 27323: Ley que modifica el Decreto Ley Nº 26126 – Ley Orgánica de CONASEV, el Decreto Legislativo Nº 604 – Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, el Decreto Legislativo Nº 681 – Normas que regulan el uso de tecnologías avanzadas en materia de archivo y documentos y el Decreto Legislativo Nº 861 – Ley de Mercado de Valores del 22 de julio de 2000.

## CONCLUSIONES Y RECOMENDACIONES

1) En un mundo globalizado, de rápidos avances que transforman la forma en que vivimos y competimos, es vital usar la tecnología de la información y la comunicación como herramienta para el desarrollo de la nación.

2) La seguridad de un sitio web es el eje fundamental de la confianza del comercio electrónico. Ganar la confianza de los clientes en línea es esencial para el éxito de un comercio electrónico. De hecho, muchas personas limitan deliberadamente sus transacciones en línea porque no confían plenamente en los procesos del comercio electrónico. Simplemente, estas personas temen por la seguridad de la información de carácter personal y financiera que se transmite en Internet.

3) SSL (Secure Sockets Layer) es el estándar mundial de la seguridad en la Web. La tecnología SSL se utiliza para cifrar y proteger información que se transmite en la Web mediante el omnipresente protocolo HTTP. SSL proporciona a los usuarios de un sitio web la seguridad necesaria para acceder a un sitio fiable, y evita la interceptación o falsificación de datos con información personal. La mayoría de los sistemas operativos, aplicaciones web y hardware de servidores son compatibles con SSL.

4) La instalación de certificados SSL aumenta la seguridad de las transacciones de comercio electrónico con su sitio web y facilita el envío de información personal en Internet. Los navegadores disponen de mecanismos de seguridad incorporados para evitar que los usuarios envíen de forma inconsciente información personal a través de canales poco seguros. Si un usuario intenta enviar información a un sitio no seguro (que carece de certificado SSL), el navegador mostrará de forma predeterminada un mensaje de advertencia que hará desconfiar al usuario de la seguridad del sitio.

5) 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

6) La gran ventaja del protocolo SET es que ofrece autenticación de todas las partes implicadas (el cliente, el comerciante y los bancos, emisor y adquiriente); confidencialidad e integridad, gracias a técnicas criptográficas robustas, que impiden que el comerciante acceda a la información de pago (eliminando así su potencial de fraude) y que el banco acceda a la información de los pedidos (previniendo que confeccione perfiles de compra); y sobre todo gestión del pago, ya que 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.

7) El comercio electrónico nos brinda beneficios en ahorros en los costos de transacción y almacenamiento, mayor eficiencia y agilidad, incentivo y empuje a una nueva economía.

8) Las instituciones bancarias son las que han realizado mayor avance en comercio electrónico con la implantación de sus operaciones bancarias por medio de Internet (banca por Internet), preocupándose con prioridad en el tema de seguridad y privacidad de la información.

# ANEXO A

## GLOSARIO DE TERMINOS

**Autoridad de Certificación**: servicio ofrecido por su banco (o la entidad delegada) para firmar digitalmente claves públicas que le son remitidas por un navegador o el software del servidor del comerciante.

**Carrito de la compra**: elemento de un catálogo en línea que mantiene una relación de los artículos que ha decidido comprar. Al terminar la compra, se pasa por la caja virtual y se paga el conjunto usando SET.

**Certificado digital:** clave pública que ha sido firmada por una autoridad de certificación confiable (como por ejemplo su banco) para identificar a los comerciantes y compradores cuando hagan uso de esta clave. Contiene además datos personales de identificación del usuario. Estos certificados se usan para la protección de la información de pago.

**Clave Privada**: clave que debe permanecer secreta, ya que permite descifrar los mensajes recibidos cifrados con la clave pública, así como firmar mensajes. Ver Criptografía de Clave Pública.

**Clave Pública**: clave que otras personas pueden conocer para enviar mensajes cifrados a su propietario o para verificar la firma de mensajes firmados por él. Ver Criptografía de Clave Pública.

**Criptografía de Clave Pública:** utiliza dos claves, una pública (conocida por todos) y otra privada (sólo conocida por el propietario), matemáticamente relacionadas, de manera que mensajes cifrados con una de ellas sólo pueden ser descifrados si se conoce la otra.

**Firma digital**: sirven para asegurar la integridad y la autenticidad de los mensajes. Representan el equivalente digital de la firma convencional dibujada a mano.

**Firma dual**: aplicación novedosa de las firmas digitales introducida por SET. Consiste en firmar los mensajes de manera que tanto el comerciante como el banco puedan verificar su integridad y autenticidad, pero sin acceder a los contenidos destinados a la otra parte.

**Logo SET**: es el sello que le indica que el comerciante está usando software que ha superado con éxito el test de Certificación de Software SET.

**Monedero digital**: constituye el remedio digital de la cartera o monedero donde almacena sus tarjetas de crédito y su identificación personal. En el monedero digital, toda esta información se encuentra protegida por una contraseña que usted establece. Es el encargado de efectuar diligentemente todos los pasos del protocolo SET una vez ha pulsado el botón de Pagar.

**SET**: el protocolo SET (Secure Electronic Transaction) es un estándar desarrollado por Visa y MasterCard para dotar de máxima seguridad a los pagos en línea por Internet y otras redes abiertas.

**SSL**: el protocolo Secure Socket Layer (SSL), desarrollado por Netscape, permite la creación de un canal cifrado entre el servidor Web y el navegador, por el cual se puede transmitir información de forma segura en uno y otro sentido.

## BIBLIOGRAFÍA


(1) Minoli, Daniel. Minoli Emma. "Web Commerce Technology Handbook" McGraw Hill Series on Computer Communications. 1998

(2) MERKOW, Mark. BRETTHAUPT, Jim WHELEER, Ken. "Building Set Applications for Secure Transactions". Wiley Computer Publishing. 1998.

(3) DAVARA RODRIGUEZ, Miguel Angel. "Factbook de Comercio Electrónico". Segunda Edición.

(4) RAMIO AGUIRRE, Jorge. "Seguridad Informática y Criptografía" Universidad Politécnica de Madrid. Tercera Edición Marzo 2003. Documento de libre distribución en Internet www.criptored.upm.es

(5) Mohmmed j. Kabir. "La Biblia de Servidor Apache 2" Anaya Multimedia

(6) Autoridad de Certificación SSL
http://www.verisign.com/

(7) Articulo SET a Fondo:
http://www.idg.es/iworld/articulo.asp?id=103068&sec=iworld

(8) Seguridad en el comercio electrónico
http://www.iec.csic.es/criptonomicon/susurros/susurros08.html

(9) Seguridad en la transacción
http://www.htmlweb.net/seguridad/ssl/ssl_1.html