UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS
ESCUELA DE SISTEMAS DE INFORMACION Y AUDITORIA

"SEGURIDAD EN EL COMERCIO ELECTRONICO"

Seminario para optar al título de Ingeniero en Información y Control de Gestión

Autores:
Freddy Acevedo Zamorano
Verónica Vargas Malebrán
Director de Seminario: Claudio Szot Meza

Semestre Otoño – 2004

INTRODUCCION

Hasta hace algún tiempo, la interacción social a nivel comercial se efectuaba cara a cara, por teléfono o bien por correo tradicional. Sin embargo, gracias a las innovaciones técnicas acontecidas en los últimos años, se ha producido el nacimiento de un nuevo tipo de comercio, el denominado comercio electrónico.

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. En definitiva, este nuevo mercado electrónico nos permite tener en nuestro domicilio una gran galería comercial por la que podemos pasear de forma fácil y rápida con el mouse de nuestro PC, y todo ello sin movernos de casa.

El comercio electrónico no es algo totalmente nuevo, si se tiene en cuenta que desde hace ya más de una década existe un protocolo denominado EDI (Electronic Data Interchange) para el intercambio electrónico de documentos. Existen muchas otras variantes de comercio electrónico, como por ejemplo el denominado home-banking, que permite al usuario realizar operaciones en sus cuentas bancarias igualmente desde su ordenador personal.

Todo lo anterior se hace posible gracias a la existencia de grandes redes digitales de comunicación a nivel mundial, que facilitan las transacciones entre las partes implicadas. Entre ellas merece especial mención la red Internet, la cual da cobertura a millones de usuarios: personas, negocios, empresas, revistas y todo tipo de sociedades.

Las ventajas del comercio electrónico son evidentes. El comprador puede ver de manera rápida todo el escaparate electrónico y no tiene que ir tienda por tienda en busca del producto deseado. Se optimiza también el tiempo de atención al cliente, que no tiene que esperar largas colas para ser atendido. Por su parte, el vendedor también se beneficia, puesto que puede ofertar sus productos sin necesidad de mostrarlos físicamente al comprador.

Pese a todo, también es cierto que este tipo de comercio presenta sus inconvenientes, algunos de ellos potencialmente peligrosos y todavía por solucionar. Entre ellos, el más importante es la falta de seguridad en los procesos de compraventa. En el caso del comercio tradicional, como se ha indicado anteriormente, la mayoría de las transacciones se efectúan cara a cara, por teléfono o por correo. Todas estas actividades pueden considerarse intrínsecamente seguras. Sin embargo, en el caso del comercio electrónico, la interacción entre comprador y vendedor se realiza a través de una red abierta (Internet), que no puede considerarse un canal de comunicación seguro a menos que se adopten ciertas medidas de protección.

El estudio y desarrollo de estas medidas de protección es precisamente uno de los objetivos fundamentales de la criptografía. Ésta proporciona al comercio electrónico las herramientas necesarias para garantizar, dado el caso, el carácter secreto de la información intercambiada (confidencialidad), así como la no manipulación de la misma entre el origen y el destino (integridad).

Una de las situaciones más preocupantes actualmente es la publicación de los datos personales y confidenciales del comprador (como por ejemplo el número de su tarjeta de crédito) en un medio totalmente abierto como es Internet. Otro tema pendiente de resolver es el de cómo obtener los resguardos que permitan realizar posteriores reclamaciones tanto al comprador como al vendedor en el caso de que alguno de ellos se sienta perjudicado por el otro una vez concluida la transacción.

Hoy día existen diferentes protocolos como el SET (Secure Electronic Transaction) o el SSL (Secure Sockets Layer) que se ocupan de que este tipo de transacciones a través de redes informáticas sean lo más seguras posibles. Sin embargo, ninguno de ellos ofrece todavía una seguridad completa, ya que únicamente son capaces de solucionar de forma parcial los problemas antes apuntados, con lo que tanto el comprador como el vendedor pueden todavía engañar. Así, por ejemplo, puede darse la situación de que el comprador pague un producto y posteriormente no lo reciba, o bien que el vendedor entregue un producto y posteriormente no pueda cobrarlo. Además, lo que es más peligroso, sin que ninguno pueda demostrar que ha sido engañado por el otro.

Después de todo lo dicho, es indudable que uno de los factores que ha contribuido en mayor medida al éxito y desarrollo del mundo empresarial en los últimos años ha sido la implantación del comercio electrónico. Esto hace pensar que su protagonismo en el futuro será incluso mayor que el que tiene hoy en día. Es igualmente cierto que la evolución futura de este tipo de comercio dependerá de forma directa de la capacidad de garantizar su seguridad mediante la criptografía, pero tampoco es conveniente que la psicosis de inseguridad electrónica nos lleve a frenar el despegue de este comercio en Internet. En definitiva, sería conveniente que empezásemos a considerar el problema del comercio electrónico no tanto como un problema de inseguridad sino más bien de confianza.

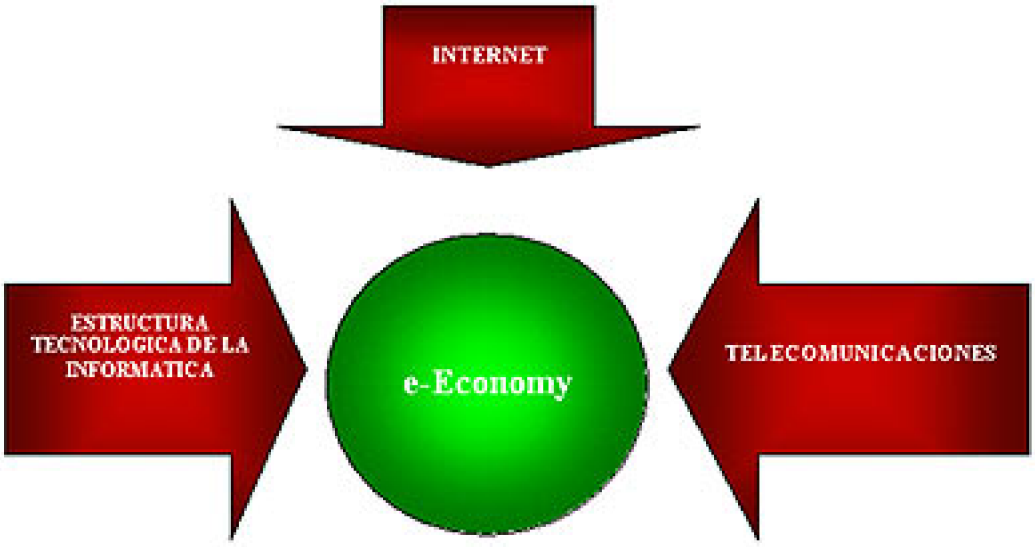
Éste será el tema principal que abarcaremos en este trabajo, en el que detallaremos y explicaremos cada una de las medidas que resguardan la seguridad de las transacciones a través de la red.

CAPITULO 1: “HACER NEGOCIOS A TRAVES DE LA WEB”

1.1. E-ECONOMY, E-BUSINNES, E-COMMERCE

1.1.1. NUEVA ECONOMIA DIGITAL: “E-ECONOMY”

La e-economy es el resultado de un cambio de mentalidad sufrida por los economistas. Vieron en Internet una herramienta para obtener ventajas competitivas sobre el resto y junto a la infraestructura de la informática y a las telecomunicaciones llegaron a lo que hoy se conoce como e-economy. En Chile esto coincidió con un periodo de ajuste económico.



Es una nueva manera de plantear los procesos productivos de las empresas y la distribución de productos, tanto para materias primas, productos semielaborados, componentes y accesorios necesarios para producirlos.

Para llegar a la e-economy es básico contar con Internet, es necesario darse a conocer al mundo por medio de la Web y ocuparla para comunicarse con los usuarios.

Además de las relaciones B2C (Business to Consumer) es importante desarrollar relaciones B2B (Business to Business). Por último es necesario transformar el modelo de negocios.

Las Tecnologías de Información y Comunicaciones (TIC), son la base de esta nueva economía, se deben considerar como un capital más y apuntan a mejorar la productividad de las empresas y de toda la economía. El desarrollo de la industria de las telecomunicaciones, y su rápida difusión han permitido eliminar las fronteras y optar a mejores posibilidades de negocios y producir nuevos productos.

De acuerdo a la Cámara de Comercio de Santiago (CCS), los sectores usuarios de TI son: financieros y telecomunicaciones, minería de exportación y el sector eléctrico. Además, presentan los mayores niveles de productividad del trabajo.

El cambio en la manera de enfrentar los negocios, nos ha llevado a la orientación hacia el cliente. Como resultado existe una permanente preocupación de optimizar los procesos y mejorar la calidad junto con reducir los costos de las transacciones, donde Internet ha sido un punto a favor del cliente. Esto ha sido interiorizado por la gran mayoría de las empresas chilenas, lo cual es apoyado por las cifras que indican que un 61.4% de las empresas tiene conexión a Internet y el 11.2% posee un sitio Web, como se detalla en el cuadro Nº 1.

Porcentaje de Empresas con Conexión a Internet y Sitio Web		
Tamaño	Internet	Sitio Web
Micro	57.6 %	8.5 %
Pequeña	77.2 %	21.1 %
Mediana	92.7 %	35.7 %
Grande	97.2 %	62.7 %
TOTAL	61.4 %	11.2 %

Cuadro Nº 1

Podemos observar que existe una brecha en el uso de TI entre los diferentes tamaños de empresas. En la microempresa vemos un retraso en la incorporación de sitios Web e Internet, pero va presentando un aumento en el uso de Internet, cuya tasa pasó del 37% al 58% y lo mismo observamos en la pequeña empresa donde la tasa aumentó de 64% a un 72%. La mediana y grande empresa presentaron aumentos bastante menores.

Al sectorizar por tamaños de empresas, es importante destacar que solo el 10% de las microempresas tienen un sitio Web, en las pequeñas este porcentaje alcanza un 21% y en las empresas medianas y grandes bordea un 36% y 60% respectivamente.

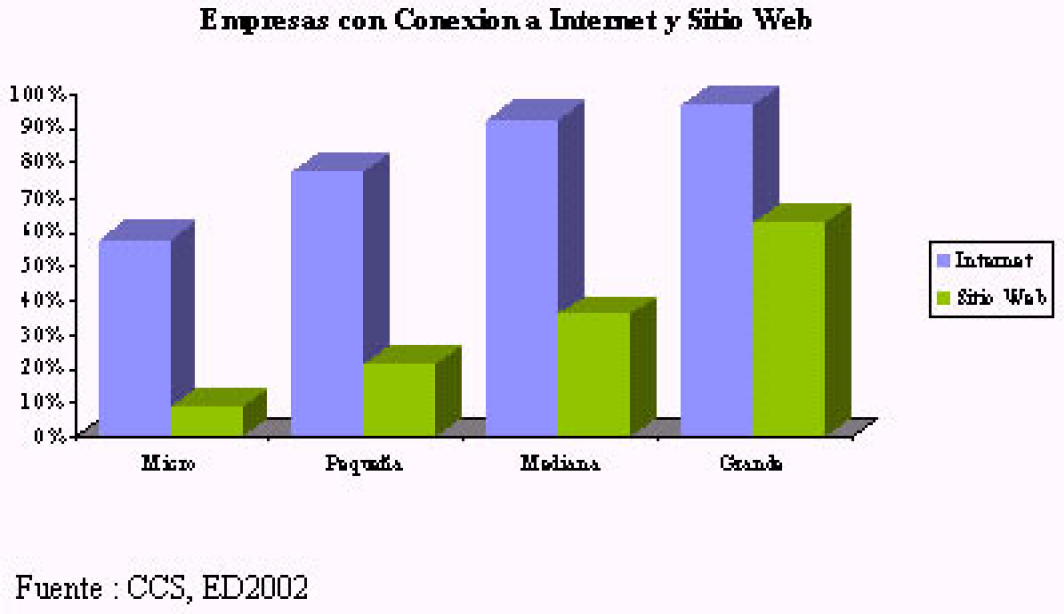


Gráfico Nº 1

La CCS estimó que el impacto de las TI en los resultados operacionales es de un 1.2% y el aporte del uso de Internet es de un 0.06%. Internet entrega a las empresas la posibilidad de encontrar proveedores y clientes en todo el mundo los 365 días del año y las 24 horas del día. Además permite a todas las empresas acceder a mejores oportunidades de negocios en el extranjero, lo que antes solo era posible a las grandes empresas.

También vemos un cambio cultural en la empresa, la relación empleado - empleador se ha visto afectada, la importancia cae sobre el primero porque él tiene el conocimiento, que es la base de la nueva economía. Ya no es imprescindible la presencia física de los trabajadores en la empresa y se ha visto modificada la jornada laboral. Existe un uso intensivo de medios electrónicos para relacionarse con los clientes y se han acelerado los cambios, tanto en la estrategia como en los procesos. La e-economy ha permitido una reducción de costos, y nos ha entregado mercados más competitivos y transparentes. También ha generado empresas que entregan servicios más específicos.

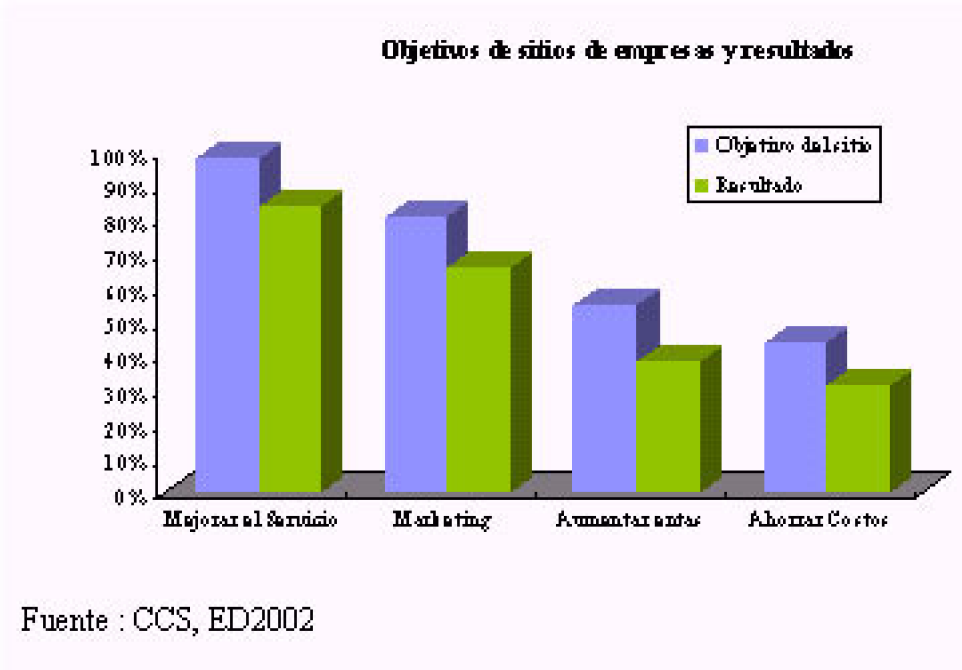


Gráfico Nº 2

De acuerdo al Centro de Comercio Digital, la conectividad de las empresas alcanzará el año 2006 un 71%.

1.1.2. E-BUSINESS

Es insertar en Internet los procesos de negocios de una empresa con el fin de realizar transacciones. Para esto, la búsqueda de nuevos clientes, incrementar las utilidades, mejorar la eficiencia y dar un mejor servicio en la creación de valor agregado para el cliente, debiera ser objetivo primordial de la organización. Las soluciones de e-business integran los procesos con el fin de obtener respuestas más rápidas y efectivas de los empleados, proveedores, etc.

El e-business implica un cambio cultural, social y económico. Uno de los problemas que debe enfrentar una empresa en camino hacia el e-business es la transición de la cultura tradicional a la nueva economía, es necesario conocer y comprender la cultura organizacional para saber como llevar la transición a cabo sin problemas.

Como resultado de estas nuevas formas de hacer negocios, llegamos a lo que hoy conocemos como e-commerce o comercio electrónico.

1.2. ¿QUE ES EL COMERCIO ELECTRONICO?

Cuando escuchamos el término “comercio electrónico” inmediatamente lo asociamos con la venta de bienes de una empresa a través de Internet, por ejemplo Falabella o Almacenes París. 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 al 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.

1.3. TIPOS DE COMERCIO ELECTRONICO

El comercio electrónico puede adoptar diversas formas fundamentales:

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 deORM (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.

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:

1. 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.

2. 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).

3. 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. 1.

CARACTERISTICAS DEL CLIENTE ON-LINE:

La red está cambiando la relación entre compradores y vendedores. Estas nuevas formas de relaciones comerciales permiten a los compradores aumentar su poder de regateo, debido a que puede comparar fácilmente entre las diferentes ofertas; y a los vendedores aumentar la información de que disponen sobre los hábitos de compra de los anteriores. Ello obliga a los vendedores a entender que el cliente "on-line" es diferente al cliente real

- Tiene acceso a Internet desde diferentes lugares y a cualquier hora del día.
- Necesitan más información sobre el producto para tomar una decisión de compra.
- El vendedor no puede influenciar sobre el proceso de compra.
- Lo importante puede que no sea lo que se vende sino cómo se vende. Se puede realizar un servicio personalizado en función del perfil de compra de cada cliente lo que además de facilitar la tarea al comprador, se aumenta el grado de fidelización del mismo.
- Es más sensible en al tema de la seguridad. Existe cierto recelo a la hora de dejar los datos referidos a una cuenta bancaria en la red para realizar transacciones digitales. Pero lo cierto es que hay pocos casos de fraude digital de los que se posea documentación, sobre todo si tenemos en cuenta los cientos de tarjetas de crédito que se pierden al día.

En la venta on-line la privacidad es importante. Derivado de lo anterior, resulta

imprescindible que el vendedor no facilite a terceros información sobre los datos o el comportamiento de los clientes.

Los expertos aseguran que la gran ventaja de esta forma de venta en línea es que no se necesitan grandes cantidades de inventario físico sino sólo rápidas soluciones de distribución.

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.

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.

CONSUMIDOR – ADMINISTRACION (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, la Administración podrá extender las interacciones electrónicas a áreas tales como los pagos de pensiones, el asesoramiento, o las devoluciones de impuestos.

1.4. VENTAJAS Y DESVENTAJAS DEL COMERCIO ELECTRONICO

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.

1.5. EL IMPULSO DEL COMERCIO ELECTRONICO 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.

1.5.1. PRINCIPIOS INHERENTES AL COMERCIO ELECTRONICO

1.5.1.1. EL SECTOR PRIVADO DEBE LIDERAR

A pesar de que los gobiernos han jugado un papel económico importante en el desarrollo de Internet, su expansión ha sido principalmente llevada por el sector privado. Por ello, para que el comercio electrónico siga floreciendo debe ser mantenida la hegemonía del sector privado. Por eso la expansión de los servicios, la mayor implicación, así como la bajada de los costes sólo podrá llegar en un mercado libre y no en un entorno estandarizado, burocratizado propio de un obsoleto concepto estatal de mercado. Los gobiernos deberán impulsar aquella industria capaz de conocer sus necesidades y limitaciones y por tanto aquella capaz de autoregularse. No obstante, allá donde los acuerdos colectivos, así como los formalismos, son necesarios, es tarea de las entidades privadas, el establecer, en la manera de lo posible, unas pautas de comportamiento que lleven hacia la organización y estructuración del mercado. A pesar de ello, en aquellas intervenciones gubernamentales (por ejemplo impuestos) o acuerdos intergubernamentales, que son necesarios para el buen equilibrio entre los operadores del mercado, una participación privada seguirá siendo fundamental para su óptimo desarrollo.

1.5.1.2. LOS GOBIERNOS DEBEN EVITAR RESTRICCIONES EN EL COMERCIO ELECTRONICO

Los operadores deben ser capaces de llevar a cabo acuerdos legítimos para la compra y venta de productos y servicios en Internet con una mínima intervención gubernamental. Una innecesaria regulación de las actividades comerciales puede distorsionar el desenvolvimiento del mercado electrónico, con un descenso de la capacidad de elección del consumidor y un aumento considerable de los costes de los productos y servicios en todo el mundo. Además hemos de tener en cuenta la rapidez con que se producen los cambios en el mundo de la tecnología, ya que, los intentos de los gobiernos para

controlarla quedan vacíos de contenido para cuando entran en vigor.

En consecuencia los gobiernos deben evitar imponer nuevas e innecesarias regulaciones, así como procedimientos burocráticos e impuestos en las actividades comerciales que se desarrollan en Internet.

1.5.1.3. CUANDO LA INTERVENCION GUBERNAMENTAL SEA NECESARIA, DEBERA ESTABLECER UNOS MINIMOS PARAMETROS DE REGULACION

En determinadas áreas los acuerdos gubernamentales serán necesarios para facilitar el comercio electrónico y la protección de los consumidores. En estos casos los gobiernos deben establecer un mínimo de regulación basado en una descentralizada intervención legal, antes que una intervención total y burocratizadora del modelo contractual comercial. Por tanto, allá donde la intervención gubernamental sea necesaria para facilitar el comercio electrónico, su arbitraje deberá garantizar la libre competencia así como proteger la propiedad intelectual, prevenir el fraude, fomentar la transparencia y facilitar la resolución de los conflictos que en él puedan surgir.

1.5.1.4. LOS GOBIERNOS DEBEN ACEPTAR LAS CUALIDADES INTRÍNSECAS DE INTERNET

La gran explosión expansiva y el éxito que ha adquirido Internet, puede ser atribuida en parte a su naturaleza descentralizada, así como a su carácter anárquico. El comercio electrónico supone un cambio significativo con respecto a la anterior regulación, por ello no debemos asumir que por ejemplo, las antiguas leyes establecidas para la regulación de las telecomunicaciones radio y televisión puedan ser utilizadas para regular la red de redes, de esta forma la regulación sólo debe ser impuesta en aquellas áreas donde exista un gran consenso. Por eso, todas las leyes y regulaciones que puedan ser aplicables al comercio electrónico deben ser revisadas o derogadas, para reflejar la necesidad de la nueva era electrónica.

1.5.1.5. EL COMERCIO ELECTRONICO EN INTERNET DEBE SER DESARROLLADO CONFORME A UNA BASE GLOBAL

La Internet esta emergiendo como un mercado global, aquella legislación que soporte las transacciones comerciales en Internet deberá ser gobernada por principios consustanciales capaces de cruzar las fronteras nacionales e internacionales.

1.6. POLITICAS A DESARROLLAR EN ACUERDOS INTERNACIONALES PARA PRESERVAR INTERNET COMO UN MEDIO SIN REGULACION.

La necesidad de creación de un medio sin regulación ha sido puesta de manifiesto a lo

largo de esta tesis. Se trata de crear un medio en el que la competencia y la posibilidad de elección del consumidor sean las bases de desarrollo del mercado global. Podríamos dividir dichas áreas en tres apartados, los cuales englobarían nueve puntos de interés necesarios para un correcto desarrollo del mercado global.

1.6.1. CUESTIONES ECONOMICAS:

En esta área tendríamos que tratar puntos tan importantes como son los impuestos aplicados a las transacciones electrónicas, así como la necesidad de encontrar un sistema o medio de pago adecuado a dichas operaciones electrónicas.

1.6.1.1. IMPUESTOS

A lo largo de cincuenta años, los Estados han negociado entre ellos múltiples reducciones arancelarias, debido a que se han dado cuenta que el comercio libre de grandes cargas e impuestos reporta mayor beneficio para la economía y para el ciudadano en general, que no un comercio sumamente controlado con cargas e impuestos arancelarios. No hay más que ver la evolución de la Comunidad Europea, y observar la pronta liberalización del comercio, así como la supresión de las barreras arancelarias que perdieron la libre circulación de personas y mercancías. En el trasladado del comercio a Internet parece obvio que se introduzcan aranceles e impuestos a los productos y servicios que en este medio se desarrollan. No obstante, hay que tener en cuenta que en Internet no existe una estructura clara y rígida de líneas geográficas que históricamente han caracterizado el comercio físico de bienes y productos. De esta forma mientras exista la posibilidad de administrar cargas arancelarias o impuestos a través de Internet, no existiría problema alguno, sin embargo y aunque los productos son enviados a su lugar de destino vía mar, tierra o aire, no ocurre lo mismo con aquellos servicios o productos que son administrados electrónicamente, como por ejemplo la distribución de software o el informe que se realiza por un despacho de abogados a determinado cliente. Por ello los Estados se han puesto manos a la obra para buscar un procedimiento o una fuente de ingresos en el comercio electrónico global, de forma que las transacciones electrónicas vía Internet puedan quedar gravadas por un impuesto o arancel. Esto supondría un retraso en la historia y una vuelta atrás en el tiempo, volviendo de nuevo a las restricciones sobre el comercio. Por ello es imprescindible declarar mundialmente mediante la WTO (World Trade Organization) o cualquier otro foro internacional, la libre circulación de bienes productos y servicios que sean distribuidos a través de Internet. Dicho principio de libre circulación debe ser establecido rápidamente antes de que los Estados impongan cargas e impuestos a las transacciones realizadas por Internet, de forma que estos acuerdos consigan la no-implantación de un mecanismo fiscal que pueda ser difícil de derribar una vez implantado en la estructura fiscal del Estado, o que por otro lado la aparición de múltiples formas de cargas fiscales haga imposible la coordinación entre estados de los impuestos a cobrar. Así se debería abogar por la no imposición de nuevas cargas fiscales a la Red, ya que dichas cargas deben ser en todo caso consistentes con los principios internacionales sobre impuestos. De esta forma no se esta diciendo que el comercio

desarrollado en Internet no debe sufrir ningún tipo de carga o impuesto, sino que en el caso de cargar o imponer trabas a las transacciones electrónicas desarrolladas en Internet, sea haga de forma conjunta e impuesta por todos los Estados para de esta forma evitar un mal desarrollo del mercado global que está floreciendo. Por tanto la imposición de cargas a dichas transacciones deberán evitar en la medida de lo posible, la doble carga del impuesto por ambos Estados, así como el establecimiento de un a estructura propia de recaudación, siendo también de gran relevancia el conseguir que dicha carga sea simple clara y fácil de comprender, de forma que todos los países involucrados puedan establecerla en sus propias estructuras sociales.

De esta forma, cualquier carga impuesta sobre una venta realizada a través de Internet deberá seguir los principios siguientes:

- No debe alterar ni impedir el comercio. Ningún sistema de recaudación deberá discriminar entre tipos de comercio, así como tampoco crear incentivos que provoquen el cambio de la naturaleza geográfica de la transacción.
- El sistema debe ser simple y transparente deberá ser capaz de aglutinar todos los ingresos, ser fácil de llevar a la práctica, así como minimizar el coste para todas las partes que intervienen.
- Por ultimo, el sistema deberá ser capaz de acomodarse a todos los países que firmen el acuerdo.

Cualquier sistema de recaudación deberá acomodar estos principios u objetivos al contexto de Internet, ya que hay que tener en cuenta varios aspectos como son: el potencial de anonimato que existe entre el comprador y el vendedor, la posibilidad de realizarse múltiples micro transacciones, la dificultad de asociar actividades online a lugares físicos etc. Estos problemas están siendo actualmente debatidos en la OECD (organización para la cooperación económica y el desarrollo) principal foro internacional para la cooperación en materia fiscal.

1.6.1.2. SISTEMAS DE PAGO ELECTRONICO

Nuevamente nos encontramos con uno de los principales problemas que existen para un correcto desarrollo del comercio electrónico global. Es de sobra conocido que las nuevas tecnologías hacen posible el pago electrónico de los productos y servicios desarrollados en Internet. Algunos de estos métodos enlazan con los actuales sistemas de pago bancarios, incluyendo tarjetas de crédito y débito, los cuales han sido aplicados a Internet con nuevas y diversas interfaces. El dinero electrónico así como la tarjeta inteligente (incorpora un microchip con posibilidad de cargar la tarjeta con la cantidad que se estime oportuna) son unos de los ejemplos de sistemas de pagos que actualmente están en proceso de desarrollo. Es por tanto el sector privado el que está invirtiendo en estas posibles formas de pago electrónico mucho esfuerzo y dinero, que a la larga compensarán a los propios comerciantes así como a los destinatarios finales del producto, es decir, al consumidor.

De esta forma los sistemas de pagos electrónicos están sufriendo constantemente cambios, que llevan al continuo perfeccionamiento de los sistemas. Por tanto el imponer

legalmente un sistema de pago obligatorio para aquellos que se dediquen a comerciar en Internet, sería incurrir en un grave error, ya que las propias tecnologías anularían todo ese esfuerzo de regulación, al quedar anticuadas dichas normas, es muy difícil desarrollar una política adecuada en tiempo y forma. De ahí que sea preferible ir probando las nuevas formas de pago que sucesivamente vayan apareciendo, al menos a corto plazo, ya que a largo plazo la propia autorregulación del mercado podría perjudicar al no cubrir todas las cuestiones que los sistemas de pagos electrónicos plantean. Por ello será necesaria una acción conjunta de los Estados para garantizar un sistema de pago seguro, que proteja a los destinatarios finales, así como una correcta implantación en el sistema legal de los contratos.

Actualmente se están estudiando en distintos foros internacionales las implicaciones que los distintos sistemas de pago pueden ocasionar. Además un buen número de organizaciones están trabajando en importantes aspectos de la banca electrónica y el pago electrónico. Sus análisis e investigaciones facilitarán una mejor comprensión de los sistemas de pagos electrónicos que afectan al comercio.

Desde este punto de vista debe existir una política común de cooperación entre los gobiernos y los sectores privados para que de esta forma, las acciones gubernamentales puedan acomodarse a las necesidades del nuevo mercado global.

1.6.2. CUESTIONES LEGALES

En general podemos afirmar que son las propias partes que operan en este mercado, las que deben ser capaces de establecer bajo qué condiciones y cláusulas se deben regular sus propias transacciones comerciales. De esta forma las propias operaciones del mercado son las que deberán definir y articular la mayoría de reglas que gobernarán el comercio electrónico. Para ello los Gobiernos deberán trabajar con firmeza en el desarrollo de reglas internacionales simples y de fácil entendimiento así como la creación de normas que sirvan para un correcto desarrollo legal del comercio electrónico en el cyberespacio.

1.6.2.1. DESARROLLO LEGISLATIVO

En concreto Estados Unidos ha adaptado su Código de Comercio (Uniform Commercial Code)al nuevo mercado emergente, posibilitando de esta forma una base reguladora de las transacciones comerciales que en él se desarrollen. Por otro lado, internacionalmente y a través de UNCITRAL (United Nations Commission on International Trade Law) se ha completado un estudio provisional sobre una ley modelo, capaz de aglutinar todos aquellos usos comerciales internacionales que puedan incidir directamente en el comercio electrónico global. Este modelo de ley, que más adelante desarrollaré, establece una serie de normas y reglas que dan veracidad y validez a los contratos realizados electrónicamente, lo cual implica el establecimiento de reglas para la formación del contrato, definir que características debe reunir un documento electrónico para ser válido, determinar los requisitos que debe reunir la firma electrónica para su correcta aceptación en el comercio, así como suministrar carácter probatorio en juicio o

en procedimientos arbitrales a todo aquello que los ordenadores puedan realizar en las operaciones comerciales.

Desde este punto de vista, nos encontramos con una serie de principios que deben gobernar en el comercio electrónico global:

- Las partes son libres para regular sus transacciones comerciales según la regulación que más se adapte a sus circunstancias.
- Las reglas deben ser tecnológicamente neutrales (no deben requerir determinadas tecnologías) además de contener previsión de futuro (no deben ocultar el uso o desarrollo de determinadas tecnologías en el futuro).
- Las reglas actuales deben ser modificadas o adaptadas al nuevo medio comercial e incluso si es necesario adoptar nuevas normativas que sean capaces de soportar el uso de las nuevas tecnologías electrónicas.
- El proceso debe abarcar tanto a aquellas empresas altamente cualificadas en lo que a tecnología se refiere como a aquellas que todavía se encuentran en desarrollo.

Estos principios deben servir de base a todos los gobiernos así como asociaciones internacionales (UNCITRAL; UNIDROIT etc.) para el desarrollo de modelos legales y principios fundamentales que eliminen la burocracia, así como las barreras legales que imposibilitan el comercio electrónico. Sus acciones deben ir encaminadas a:

- Fomentar el reconocimiento, la aceptación, así como facilitar las comunicaciones electrónicas en todos los Gobiernos partícipes.
- Fomentar reglas internacionales que soporten la aceptación de firmas electrónicas y otros procedimientos de autenticación.
- Promover un mecanismo adecuado y eficaz de resolución de controversias en materia de transacciones electrónicas.

Por último también hay que tener en cuenta para un correcto desarrollo del comercio electrónico, la posibilidad de alcanzar un grado razonable de aceptación en cuanto al grado de responsabilidad que se debe tener ante cualquier posible daño o perjuicio resultante de sus actividades. Esto unido a las distintas legislaciones de cada país en materia de competencia jurisdiccional puede incrementar los litigios y crear unos costes innecesarios que en última instancia serán satisfechos por los consumidores. Por tanto, se debe trabajar estrechamente entre todas las naciones para conseguir clarificar las reglas sobre competencia jurisdiccional, así como favorecer las disposiciones contractuales que permitan a las partes seleccionar las normas sobre responsabilidad.

Finalmente el desarrollo del comercio electrónico y sus respectivas normas de regulación, ofrecerán la posibilidad, tanto a comerciantes como a consumidores, de aprovechar la ventaja resultante de la tecnología, y de esta forma realizar tareas de forma automática que antes se venían haciendo a mano. Como por ejemplo los registros electrónicos.

1.6.2.2. PROPIEDAD INTELECTUAL

El comercio electrónico generalmente incorpora en sus ventas la licencia sobre la propiedad intelectual de lo transmitido o publicado en la Red. Para la promoción de este comercio es necesario que los compradores sepan con seguridad que su propiedad intelectual no puede ser robada y por otro lado garantizar a los consumidores que los productos adquiridos son auténticos. De ahí, que sea necesario un concierto Internacional en materias como la patente, los derechos de copia (Copyright), marcas, propiedad intelectual etc. Estos derechos requerirán un estudio pormenorizado sobre los mismos, tema que deberá ser tratado en otro momento para no desviarme del estudio que estoy desarrollando.

1.6.2.3. EL DERECHO A LA INTIMIDAD, LA PRIVACIDAD

Nos encontramos con uno de los principales derechos que deben ser satisfechos en la actual Infraestructura Global de la Información. La Unión Europea ya lo ha realizado y España con la LORTAD cumple dicha directiva. Debido a la importancia del tema reitero lo anteriormente dicho y lo abandono para un futuro tratamiento.

1.6.2.4. SEGURIDAD

La infraestructura Global de la Información debe ser segura y veraz. Los usuarios de Internet deben tener la certeza de que sus comunicaciones y datos personales están a salvo de cualquier intromisión desautorizada, así como de cualquier modificación que de los mismos se pueda hacer. Evidentemente si no se proporciona una cierta seguridad en la Red serán muy reacios a su utilización y no imaginemos si de lo que se trata es de comerciar. De ahí que una Infraestructura Global de la Información necesite:

- Una telecomunicación segura y veraz en redes de trabajo en grupo.
- Medios efectivos de protección de los sistemas de información agregada a dichos grupos de trabajo en red.
- Medios efectivos para dar autenticación y asegurar la confidencialidad de la información electrónica frente a posibles intromisiones o usos desautorizados.
- Una buena formación a todos aquellos usuarios de la Infraestructura Global de la Información para que sepan como proteger sus sistemas y sus datos.

No existe una fórmula mágica o técnica que pueda garantizar que la Infraestructura Global de la Información sea segura y veraz. Para alcanzar dicho objetivo se requiere un grado de tecnología muy avanzado en temas como encriptación, autenticación, controles de claves, corta fuegos, ...etc. Por tanto es mejor dejar que los propios operadores del mercado construyan sus negocios en la red antes que exigir un determinado tipo de encriptación, autenticación etc. Siendo a largo plazo aquel sistema más seguro y utilizado el que se imponga en el comercio electrónico global. En la actualidad el sector privado esta realizando fuertes inversiones en la investigación de estos campos, que en definitiva dan la seguridad al consumidor ya que elegirá aquel sistema más seguro y fiable de los muchos que el mercado ofrece. Por tanto nos encontramos con un problema de tiempo, siendo el propio mercado el que resolverá el problema al establecer por los usos

comerciales que sistema es el más seguro, es decir quién ofrece mayor autenticación en las operaciones comerciales.

Otra cuestión de suma importancia para la seguridad en la Red son los servicios de certificación, es decir, aquellos servicios que recogen las firmas digitales de los posibles comerciantes o consumidores de la red, para que de esta forma puedan saber con quién se están comunicando en Internet (el avance de la tecnología es tan impresionante que se puede estar comunicando con cierto usuario que aparenta ser una persona normal siendo un ordenador y no la persona que dice ser), es decir tener la certeza de quien está al otro lado del módem.

No obstante nos encontramos en un terreno de arenas movedizas, en el sentido de que la seguridad que se otorga al comercio electrónico con los sistemas de encriptación puede volverse en contra del propio usuario, si no se realiza una buena gestión de dichos sistemas de encriptación. Ya que el usuario puede perder su llave o clave de acceso a los datos encriptados y no tener forma alguna de recuperarlos, que unido a la posibilidad de que la encriptación sea utilizada para fines ilícitos, reabre la problemática del deber de control por parte de los Gobiernos. Estos problemas se evitarían si una determinada autoridad controlase bajo estricta confidencialidad dichos sistemas de encriptación, de forma que, en caso de perdida o deterioro de dichos sistemas de encriptación existiese la posibilidad de recuperar los datos encriptados, y a la vez poder controlar por los Estados los posibles hechos delictivos que con dicha encriptación se están cometiendo.

Nuevamente habrá que esperar a que los Estados se pongan de acuerdo en el ámbito internacional para así poder obtener una eficiente regulación en temas tan delicados como pueden ser, la encriptación y la autenticación. Mientras tanto habrá que esperar a que el sector privado utilice un buen mecanismo de telecomunicación que de garantías suficientes a las partes involucradas.

1.6.3. CUESTIONES RELATIVAS AL ACCESO AL MERCADO VIRTUAL

La exigencia del cambio no puede ser atendida por todos los Estados. El mercado pone muchas trabas al acceso de los países.

1.6.3.1. INFRAESTRUCTURA DE LAS TELECOMUNICACIONES Y TECNOLOGIAS DE LA INFORMACION

El comercio global electrónico depende mucho de la capacidad tecnológica así como de las telecomunicaciones que cada país disponga para de esta forma hacerlo efectivo, y estar al alcance de cualquier persona. Lamentablemente, en muchos países las políticas seguidas en materia de telecomunicaciones están impidiendo el desarrollo de la era digital. En algunos casos las comunicaciones son excesivamente caras, en otros se prohíbe la importación de alta tecnología, en suma se esta impidiendo una participación en el mercado global y por tanto en el comercio electrónico, es decir una libre competencia, una reducción de precios, menos posibilidad de elección para el consumidor y menos servicios ofertados.

Por ello se tiene que concienciar en los ámbitos internacionales a dichos países

reacios a la recepción del comercio electrónico, para que así se pueda conseguir una amplia cuota de mercado donde la libre competencia y la libre prestación de los servicios sean las principales bases del mercado. Mientras, habrá que conformarse con el mercado que día a día va ganando más participantes.

1.6.3.2. CONTENIDO DE LA INFORMACION

La posibilidad de que la información que se distribuye en Internet supere los límites geográficos de cada país es patente. De ahí que sea necesario tener la posibilidad de blindar el tipo de información a recuperar en la Red para evitar que personas menores de edad puedan ver cierta información que para su corta edad puede ser perjudicial. Esta posibilidad ya se ha materializado. Dentro de Internet existen navegadores que pueden limitar cierta información no aconsejable, así como ofrecer servicios de certificación de la mayoría de edad para así acceder a la información.

Existen cuatro áreas prioritarias de preocupación:

1. Regulación del contenido: Las Compañías que desean ofrecer sus servicios en Internet, así como dar acceso a la red, están seriamente preocupadas por la posible responsabilidad en que pueden incurrir ante la circulación de su información por distintos países, los cuales prohíben determinado tipo de información. Hay determinados países que por su cultura o sociedad difieren a la occidental y que por tanto han adoptado leyes para restringir el acceso a cierto tipo de información, cuyo contenido consideran perjudicial para su sociedad. Estas políticas adoptadas no por pocos países están limitando seriamente el comercio electrónico y su globalidad. Por ello hay que plantearse la posibilidad de regular esta materia, para de esta forma evitar el rechazo a Internet y por tanto la no inclusión en el mercado global de ciertos países comprensiblemente reacios a que dicha información desembarque en su población. Temas como la pornografía, la violencia, y aquellos otros temas que vulneren los más íntimos derechos de la personalidad humana deben al menos ser tratados sensiblemente. Muchas veces es el propio sistema el que rechaza dichos contenidos de información, como por ejemplo el web de ETA. Dicho web fue bombardeado por los hackers, además de ser criticado profundamente hasta que el servidor que ofrecía dicha información dejó de publicar dicha web.
2. Cuotas de contenido extranjero: Algunos países quieren limitar el contenido de la información difundida en Internet, limitando la difusión y acceso a los contenidos de Internet, para de esta forma difundir contenidos propios de su país. Sería más aconsejable mantener restricciones al contenido de Internet a través de una autoridad gubernativa antes que estructurar y regular la difusión. Esta política es errónea y perjudica gravemente al comercio electrónico, siendo más practico enseñar a promover la diversidad del contenido incluyendo la cultura y la lengua del país antes que limitar o censurar la difusión.
3. Regulación de la publicidad: La publicidad tiene un papel muy importante a desarrollar en el comercio electrónico, ya que los productos y servicios serán ofrecidos a una gran audiencia. En muchos países se restringe la publicidad, el

tiempo, la duración, el tipo de anuncio, etc. Este tipo de restricciones por muy fundamentadas que estén en las preocupaciones sociales y culturales del país a quien representen, no pueden justificar una innecesaria regulación de Internet. Sin embargo es patente la existencia de cierta publicidad engañosa o incluso publicidad dañina para ciertos sectores de la población como pueden ser los niños. De ahí que las reglas del país de origen deban servir como base para el control de la publicidad en Internet y paliar los bloqueos de las legislaciones nacionales así como las posibles barreras comerciales.

4. Regulación para prevenir el fraude: Recientemente han existido casos de difusión de información fraudulenta sobre compañías y sus productos. Para un correcto desarrollo de Internet tanto en su potencial cultural como en la parte comercial hay que garantizar al consumidor de que los productos ofrecidos en Internet están adecuadamente representados, es decir que ellos obtendrán realmente lo que han pagado, y en caso contrario serán indemnizados. Este es un área donde la intromisión de los gobiernos demás de apropiada se hace necesaria.

1.6.3.3. ESTANDARES TECNICOS

Los estándares técnicos son una pieza clave en el éxito comercial de Internet, ya que permitirá que los productos y servicios de diferentes vendedores puedan ser utilizados por todos los consumidores. Promocionan la competencia y reducen la incertidumbre. Por otro lado la imposición de determinados estándares, por determinados países pueden actuar como barreras o aranceles para el comercio electrónico en Internet ya que las innovaciones tecnológicas avanzan muy rápido y la sola imposición de estándares técnicos puede impedir la innovación tecnológica.

De esta forma para asegurar el buen crecimiento del mercado global en Internet, será necesario que dichos estándares acrediten fiabilidad, interoperabilidad, y facilidad de uso en áreas como: pagos electrónicos, seguridad (confidencialidad, autenticación, integridad de los datos, acceso control etc.), infraestructura de servicios seguros (autoridad que dé certificado de llave pública), sistemas electrónicos administradores del Copyright, videoconferencias, tecnologías en redes de alta velocidad e intercambios digitales de datos.

No necesariamente tiene que ser un estándar único para cada producto o servicio distribuido en Internet, y tampoco deben ser impuestos estándares técnicos. En algunos casos, múltiples estándares competirán por su aceptación en el mercado. En otros casos, distintos estándares serán utilizados para diferentes circunstancias.

La prevalencia de estándares voluntarios en Internet y el proceso de aceptación general del desarrollo de los estándares están proporcionando un rápido desarrollo. Estos estándares florecen gracias al desarrollo de un sistema no burocrático gestionado por la práctica de distintas organizaciones. Estas organizaciones necesitan previamente desplegar sus sistemas con la incorporación de un estándar técnico para posteriormente ser aceptado formalmente, además, éste proceso de desarrollo de los estándares técnicos puede envolver estándares ya establecidos. Solo un pequeño número de países está dejando en manos del sector privado el desarrollo de los estándares técnicos. La

mayoría de Estados confían dicha tarea a las organizaciones gubernamentales, cayendo en el grave error del atasco tecnológico, ya que se constituyen impedimentos para la entrada de información que sea distribuida con otro tipo de estándar tecnológico. Por ello es importante para el desarrollo del comercio electrónico llegar a un consenso internacional, en el que se establezca la hegemonía del sector privado.

CAPITULO 2: “PAGO ELECTRONICO Y TIPOS DE PAGO ELECTRONICO”

Respecto del Comercio Electrónico se dice que es indispensable para su utilización efectiva salvaguardar la seguridad de las transacciones que se realizan, así como proteger en todo momento la privacidad de los usuarios de la Internet.

Sin embargo existe un tema de igual o mayor importancia que los antes mencionados, que es el referido a la forma en que el dinero se traslada del comprador al vendedor, es decir los medios de pagos utilizados para que las transacciones electrónicas sean eficaces, tema que si bien se encuentra planteado, no goza de un tratamiento acorde a su importancia.

Antes de dar paso al tema de nuestro interés debemos explicar un poco aquello de la “eficacia de la transacción electrónica”, pues creemos que puede ser motivo de ciertas dudas.

Debemos señalar que una transacción electrónica no es más que un contrato celebrado mediante medios electrónicos, a través de la red. En nuestra legislación el contrato, sea este de cualquier naturaleza, es el acuerdo de voluntades destinadas a crear, regular, modificar, o extinguir una relación jurídica patrimonial, entendida esta última como el vínculo legal de contenido económico que va surgir entre los contratantes.

La mayoría de transacciones que se hacen por la red son enajenaciones. También suele contratarse locaciones de servicios, como son los contratos de prestación de

servicios o de obra, aunque estos últimos menos frecuentes.

Debemos decir entonces, que se trata de un contrato obligacional, en el cual existe una prestación que es transferir la propiedad de un bien a cambio de una contraprestación, que es el pago del dinero. Igual sucede en los contratos de prestación de servicios donde lo que constituye la prestación es la realización de un servicio.

Para ser gráficos y que no quede duda alguna de lo antes dicho, pongámonos en el ejemplo siguiente: nos encontramos frente a la computadora navegando por la Internet, y decidimos entrar a una tienda virtual y adquirir un producto, en el momento en que determinamos el bien que vamos adquirir y admitimos el precio propuesto, seguido de darle un click al recuadro que dice acepto, estamos llevando a cabo una transacción electrónica, que como hemos señalado para el presente ejemplo, no es más que una compraventa.

De haber hecho click en el recuadro que dice acepto surgen obligaciones tanto para el vendedor, que es la tienda virtual que hemos visitado, como para el comprador que somos nosotros.

La principal obligación de la tienda virtual será transferirnos la propiedad del bien adquirido vía Internet y de haberlo pactado el envió satisfactorio del bien a nuestro domicilio, asumiendo la tienda el riesgo del bien hasta la entrega. De otro lado tenemos nosotros como compradores la obligación del pago del precio, obligación que interesa para el presente trabajo.

Como ya hemos señalado anteriormente, el pago es una obligación de una de las partes, que se materializa no solo en dinero sino también en especie. El concepto de pago no es solo el que podemos tener en mente, el de retribución monetaria, ya que esta contraprestación puede realizarse mediante la entrega de otro bien, sea este mueble, inmueble, fungible o no, o mediante la realización de alguna actividad en favor de la otra parte. En el derecho civil se entiende efectuado el pago solo cuando se ha ejecutado íntegramente la contraprestación.

Sin embargo debemos aclarar, que respecto al tema de nuestro interés, el concepto civilista de pago no satisface las necesidades de la Internet, y es que, si bien podemos utilizar lo que pago denota, es imposible pensar que en la contratación electrónica donde el consumidor, tiene como hemos advertido antes, un escaso o nulo poder de negociación, que este pueda cancelar una transacción mediante un servicio o un bien distinto al dinero, y menos aún cuando hablamos de transacciones masificadas.

Es necesario, definir el pago desde el punto de vista del Comercio Electrónico, el cual este va a poseer características propias y a su vez interesantes.

Podemos entender como Pago Electrónico aquel mecanismo mediante el cual se ejecuta la contraprestación de una obligación asumida a través de la Internet, es decir mediante la contratación electrónica.

Según la segunda disposición de la Comisión de las Comunidades Europeas, el Pago Electrónico es definido como cualquier operación de pago realizada con una tarjeta de pista magnética o con un microprocesador incorporado, en un grupo terminal de pago electrónico o terminal de punto de venta.

El Pago, contraprestación por la obligación asumida se caracteriza, por ser únicamente en dinero, no pudiendo ser en especie como ya hemos señalado anteriormente, prohibición que se ha gestado por motivo de la costumbre comercial que impera en Internet.

Una vez que ya tenemos claro que es el Pago Electrónico, debemos analizar cómo es que vamos a llevar a cabo este pago, pues los medios convencionales que nosotros conocemos no son admisibles en la red, y es que por más que poseamos en este momento el efectivo suficiente para comprar el bien deseado en una tienda virtual, de nada servirá, ya que no podremos adquirir el producto, pues dentro de las opciones de pago no se encuentra el efectivo, y esto se debe a que al ser una transacción mediante medios electrónicos, el efectivo no cancela la obligación que estaríamos asumiendo con respecto al precio, pues la inseguridad que el dinero llegue al vendedor representaría un costo adicional como factor aleatorio, y entonces comprar en Internet sería más costoso y menos eficiente que una compra cara a cara.

Para solucionar ese problema, existen hoy en día los llamados Medios de Pago Electrónico, aceptados en la mayoría, por no decir en la totalidad de tiendas virtuales y páginas de la Internet, medios que agilizan las transacciones y procuran brindar la seguridad necesaria para llevar a delante el comercio electrónico.

Podemos decir entonces que los Medios de Pago Electrónico son mecanismo para efectuar la contraprestación llamada pago, a través de la Internet, ya que no es posible que el dinero en efectivo circule, por lo que se utilizan sistemas seguros que permitan al obligado a la contraprestación cumplirla cabalmente y al vendedor recibir el dinero por la prestación realizada, sea cual fuere la prestación.

En el futuro la utilización masiva de estos Medios de Pago, tendrá una importante repercusión en la política monetaria a nivel mundial y obligará a asegurar la estabilidad de los precios y la función del dinero.

Sin embargo, para que estos Medios sean totalmente eficaces, necesitaremos desarrollar normas que garanticen su funcionamiento, así como la confidencialidad de las transacciones, y la adecuada protección al comerciante y sobre todo al consumidor final.

Para un mejor análisis de los antecedentes, y a fin de resumir los aspectos más destacados de esta operación, distinguiremos en el comercio electrónico lo siguiente:

1. Red que se utiliza.
2. Transferencias electrónicas de fondos internacionales y nacionales.
3. Medio de pago.

2.1. REDES

Se pueden clasificar en dos tipos:

2.1.1 ABIERTAS

No existe normativa legal o administrativa que regule actualmente el comercio electrónico y la transferencia de información, fondos y valores electrónicos en redes abiertas.

2.1.2 CERRADAS

Existen normas específicas dictadas fundamentalmente por la autoridad administrativa que regulan la transferencia electrónica de valores relacionados con planillas electrónicas previsionales, de salud, de derechos aduaneros, declaraciones de exportación e importación, etc.

Junto con lo anterior, contractualmente los bancos e instituciones financieras han creado y reglamentado la operación de redes cerradas de transferencias electrónicas de información y fondos que son operadas por sociedades de apoyo al giro bancario, tales como Redbanc S.A., Transbank S.A.. Estas instituciones operan entre otras, las siguientes redes:

- Red Bancaria Interconectada (RBI)
- Red de Servicios Financieros (RSF)
- Red de Servicios Empresariales (RSE)
- Red de Terminales de Puntos de Ventas (POS)
- Red de ATM (cajeros automáticos)

Todas estas redes permiten la transferencia electrónica de información y fondos entre instituciones financieras, empresas, personas naturales (tarjeta de crédito y de débito), comercio e instituciones afiliadas.

Su operación está debidamente regulada por contratos de operación entre las instituciones prestadoras de los servicios y las personas naturales o jurídicas que los utilizan, salvaguardando debidamente los derechos y obligaciones de cada participante y creando mecanismos que permiten solucionar las controversias que se presenten.

Junto con la anterior la autoridad administrativa ha normado las relaciones contractuales generadas entre los bancos e instituciones y sus clientes en algunos aspectos del comercio electrónico. Así la operación de tarjetas de crédito y débito se encuentra reglamentada en forma general por el Banco Central en el Compendio de normas financieras, capítulos III. J. 1. y III. J. 2.

Se ha reglamentado la emisión y operación de la Tarjeta con provisión de fondos o Tarjeta inteligente, en el capítulo III. J.3. del compendio citado en el párrafo anterior.

2.2. TRANSFERENCIA ELECTRONICA DE FONDOS

INTERNACIONALES Y NACIONALES.

Los pagos que se realicen hacia y desde el exterior a través del Comercio Electrónico pueden ser desarrollados por entidades públicas y privadas, no existiendo una regulación específica a su respecto.

En efecto, las normas sobre cambios internacionales, establecidas en el Compendio de normas de cambios internacionales, circular Número 26 de 10 de abril de 1990 y sus modificaciones, emitido por el Banco Central de Chile, no contempla, ninguna disposición que regula la operación que se realice a través del comercio electrónico.

Del mismo modo, el Compendio de normas financieras, circular número 3013 del 22 de Enero de 1979 y sus modificaciones, emitido por el Banco Central de Chile se refiere muy tangencialmente al tema tratado, al reglamentar, como ya señalamos, en los capítulos III. J.1, 2 y 3, la emisión u operación de tarjetas de crédito, débito y de pago con provisión de fondos, respectivamente.

Tratándose de particulares, la legislación chilena, regula en alguna medida la actuación de los bancos y sociedades financieras en las operaciones bancarias e interbancarias, transferencia electrónica de información y fondos, de la recopilación de normas, bancos y financieras de la Superintendencia de Bancos e Instituciones Financieras.

Sobre este particular, vale la pena destacar lo siguiente:

- Que estas normas se aplican a la prestación de servicios bancarios y operaciones interbancarias, que se efectúen a través de un computador conectado con redes de comunicación propias o de terceros.
- Que dichos servicios comprenden tanto la transferencia electrónica de fondos como cualquier otra operación que utilice documentos o mensajes electrónicos.
- Que por transferencia electrónica de fondos se entienden aquellas operaciones que originen cargos o abonos de dinero en cuenta, tales como, órdenes de pago para abonar cuentas de terceros.
- Por último, la norma citada señala en el caso de los bancos y financieras, los requisitos de operación, seguridad y confiabilidad de los sistemas que deben utilizar para operar esta clase de transferencias.

2.3. MEDIOS DE PAGO

Cuando accedemos a una tienda virtual y deseamos comprar algún producto, podemos observar que las opciones de pago incluyen los siguientes medios: tarjeta de crédito, débito o cuenta corriente, etc. Lo que nos queda en claro es que los billetes o las monedas no tienen validez en la Red, tal como lo advertimos anteriormente.

A continuación desarrollaremos algunos de los Medios de Pago con mayor uso en la

Internet.

2.3.1. TARJETA DE CREDITO

Debemos comenzar señalando que la tarjeta de crédito es un instrumento de crédito que permite diferir el cumplimiento de las obligaciones monetarias asumidas con su sola presentación, sin la necesidad de previamente provisionar fondos a la entidad que asume la deuda, que generalmente son bancos u otra empresa del sistema financiero.

La tarjeta de crédito es el medio de pago más usado entre los ciberconsumidores. Esto se debe básicamente a su fácil uso, característica esencial de este medio de pago, y por la seguridad que brinda tanto al vendedor, ya que existe alguna entidad financiera que respalda al consumidor, así como para el consumidor ya que frecuentemente las tarjetas de crédito se encuentran amparadas por seguros. Asimismo, existe la confianza generalizada que las operaciones que se realizan utilizando tarjetas de crédito, están más que probadas y cuentan con todas las garantías.

Es fundamental tener en cuenta que para que la Tarjeta de Crédito tenga validez, esta debe contener la denominación de la empresa que emite la tarjeta, así como el sistema de tarjeta de crédito al que pertenece; numeración codificada de la tarjeta; nombre del usuario de la tarjeta y su firma; fecha de vencimiento y la indicación expresa del ámbito geográfico de validez. En caso de faltar este requisito, se entiende sin admitir prueba en contra que su validez es internacional.

2.3.2. TARJETA DE DEBITO

Son tarjetas plásticas, magnetizadas y numeradas, que sirven para realizar compras de bienes y/o servicios a través de la Internet, en las tiendas virtuales en las que se permita el uso de estas tarjetas.

Estas tarjetas se encuentran asociadas a una cuenta, que no genera intereses a favor del cliente ni gastos de mantenimiento, es decir a diferencia de la tarjeta de crédito, la entidad emisora no abre una línea de crédito, sino lo que va a responder por las obligaciones asumidas son los ahorros que se posean en una cuenta.

Es necesario para poder utilizar la tarjeta de débito, acreditar en la cuenta de ahorros fondos suficientes para comprar el producto y cubrir los gastos que esto produce, como por ejemplo el envío; todo esto antes de realizar la operación de compra por Internet.

Para realizar la compra, se debe digitar el número de la tarjeta y la fecha de vencimiento de la misma, previa verificación que la tienda acepte este tipo de tarjetas y que sea una zona segura.

2.3.3. DINERO ELECTRONICO O DIGITAL

El dinero electrónico o digital es un sistema para adquirir créditos de dinero en cantidades relativamente reducidas. Este sistema consta de unidades o símbolos de valor monetario,

debidamente cifrado que representa cantidades de dinero, que asumen forma digital; unidades que pueden ser convertidas en dinero físico. Este dinero electrónico se almacena en la computadora y se transmiten a través de redes electrónicas para ser gastado al hacer compras electrónicas a través de Internet.

Teóricamente, el dinero electrónico o digital podría utilizarse para cancelar compras por montos pequeños. Sin embargo, la mayoría de los comerciantes que aceptan dinero electrónico hasta el momento, lo emplean como una alternativa a otras formas de pago de adquisiciones de precio un tanto superior.

El Dinero Electrónico funciona de la siguiente manera (para el consumidor):

El primer paso es afiliarnos a un banco que ofrezca este sistema de Dinero Electrónico, luego debemos suscribir un contrato con alguna empresa proveedora del sistema, la cual nos proporcionará el software para instalarlo en la computadora. Este software permite bajar el dinero electrónico al disco duro de la computadora. La adquisición inicial de dinero se realiza contra una cuenta bancaria o una tarjeta de crédito.

Una vez instalado el software en la computadora, procederemos a realizar nuestras compras en la red, asegurándonos que la tienda virtual que escojamos acepte dinero electrónico o digital. Una vez escogido el producto y listos a realizar la compra, debemos simplemente hacer click en el botón de pago y el software de la tienda generará una solicitud de pago describiendo la mercancía, el precio, la fecha y la hora.

Una vez generada la solicitud y siempre que aceptemos, el software resta la cantidad del precio y crea un pago que es enviado al banco, verificado y luego depositado en la cuenta de la tienda virtual. Una vez que se ha concluido este proceso se notifica a la tienda virtual y esta envía la mercancía que hemos comprado.

Entre los sistemas de dinero electrónico o digital usados en la actualidad tenemos el CyberCash, pariente de CyberCoin, E-cash, DigiCash, Minipay, entre otros.

Actualmente, el dinero electrónico se enfrenta a algunas cuestiones desalentadoras, debido que para poner este sistema de pago en funcionamiento, los consumidores han de instalar en su computadora programas específicos; que representan un costo adicional a corto plazo. Asimismo, existen pocas tiendas virtuales que poseen estos programa con lo cual no se puede utilizar en toda la red; además de provocar una acumulación de pequeñas facturas que no es del agrado de gran cantidad de los consumidores.

2.3.4. TARJETAS INTELIGENTES O SMARTS CARDS

En pleno desarrollo, las tarjetas chip o tarjetas inteligentes son aquellas que poseen una capacidad de almacenar información en un chip que incorporan.

Fundamentalmente esta información suele ser:

- Una identificación que incluye determinadas claves cifradas.
- Una cantidad de dinero disponible.

Antes de comprar es preciso cargarlas con dinero a través de un cajero automático u otro medio. Tras realizar esta operación funcionan como si contuvieran dinero en efectivo. Este tipo de tarjetas son ideales para realizar micropagos, tanto en el comercio del mundo físico como en el virtual. No obstante, su utilización en el comercio electrónico requiere de un dispositivo conectado a la computadora personal, un módem o línea de teléfono que permita su lectura y actualización al realizar transacciones por la red. En contrapartida, la existencia de "inteligencia" local posibilita su utilización para múltiples aplicaciones: cupones de descuento, aplicaciones de fidelización y almacenamiento de datos específicos del cliente.

2.3.5. TARJETA MONEDERO

Es una tarjeta que sirve como medio de pago por las características físicas que posee; ya que puede ser recargable o de lo contrario se puede desechar si ya no nos encontramos interesados en su uso.

Esta Tarjeta Monedero es una tarjeta plástica que contiene un chip que almacena cierta cantidad de información en su memoria equivalente al monto de dinero que servirá para la operación, es decir al valor pre-pagado que posee la tarjeta, el cual se va descontando después de realizar las compras.

Su funcionamiento es similar a las tarjetas pre-pago que conocemos, que se utilizan para activar los celulares. Es muy sencillo, cada tarjeta tiene un valor preestablecido, y posee una clave que identifica cada tarjeta. Cuando vamos a comprar en la Internet, debemos fijarnos que la tienda a la que recurrimos acepte estas tarjetas, de ser así, a la hora de efectuar el pago, ingresamos e número secreto de la tarjeta, y el precio se cancela respecto a nosotros, automáticamente. Luego la compañía que emite estas tarjetas paga el valor de lo acordado a la tienda virtual, utilizando políticas propias de estas compañías.

En México, Visa Cash es la primera tarjeta monedero que se cargan a partir de efectivo, o mediante una tarjeta de crédito o débito de banda magnética en terminales situados en sucursales bancarias, cajeros automáticos o terminales de carga atendidos.

2.3.6. TARJETA RELACIONISTA

Es una tarjeta que posee un microcircuito que permite la coexistencia de diversas aplicaciones en una sola tarjeta, es decir que funcione como tarjeta de crédito, tarjeta de débito, dinero electrónico, etc. Esta tarjeta presentará en un sólo instrumento la relación global entre el cliente y su banco.

Actualmente, VISA tiene como proyecto la creación de esta tarjeta, pues para esta firma la tarjeta relacionista expresa perfectamente la idea que poseen sobre la tarjeta del futuro.

2.3.7. CONTRARREMBOLSO

Es el único medio de pago utilizado en el comercio electrónico que implica la utilización de dinero en efectivo. Hoy día es uno de los medios de pago preferidos por el consumidor en general, pues garantiza la entrega de los bienes antes del pago. Desde el punto de vista del vendedor este medio de pago conlleva dos inconvenientes fundamentales: el retraso del pago y la necesidad de recolectar físicamente el dinero por parte de quien realiza la entrega.

CAPITULO 3: “SEGURIDAD EN LA TRANSACCION”

3.1. ASPECTOS QUE DAN SEGURIDAD EN LA RED

Tal y como avanzan las tecnologías cada vez es más frecuente encontrarnos con portales que nos ofrecen productos y servicios a través de la Red. Y poco a poco los usuarios empezamos a dar uso a este tipo de servicios, aunque todavía nos sentimos reticentes a revelar nuestros datos privados y bancarios así como así.

Esto puede deberse a la falta de seguridad que en unos casos está ausente y en otros no sabemos hasta que punto es fiable.

Pero también se corre un riesgo cuando se compra en una tienda normal o se come en un restaurante y se paga con la tarjeta de crédito. De hecho existen muchos fraudes al respecto. Cada transacción que se realiza en el comercio tradicional y en el comercio electrónico está expuesta a un riesgo.

Cuando se realiza una transacción por Internet y se envían los datos personales (nombre, dirección, número de tarjeta de crédito, etc.) deberíamos plantearnos si pueden ser interceptados durante la transmisión (entre comprador y vendedor) por alguien que no sea el vendedor. Ese "alguien" ¿Podría utilizar estos datos para suplantar nuestra

identidad?.

Igualmente el vendedor quiere asegurarse de que los datos que recibe son verdaderos, es decir, necesita saber que el comprador es quien dice ser. Es por estas razones que se han desarrollado los sistemas de transacciones seguras.

La incorporación de mecanismos, técnicas y algoritmos adecuados para realizar transacciones electrónicas se hace necesaria para evitar los riesgos a los que nos exponemos. La firma digital, por ejemplo, no es más que un tipo de encriptación, en la cual se realiza un control sobre el flujo de información (por ejemplo de un contrato, de un número de tarjeta de crédito, etc.). Se usan para verificar al proveedor de una determinada información y que la información firmada (el pedido, el número de tarjeta, etc.) no ha sido alterada.

Se puede hablar en este sentido de cuatro aspectos básicos de seguridad: autentificación, confidencialidad, integridad y el no-repudio.

CONFIDENCIALIDAD

La confidencialidad es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipularla. Igual que antes, los usuarios pueden ser personas, procesos, programas, etc.

Para evitar que nadie no autorizado pueda tener acceso a la información transferida y que recorra la Red se utilizan técnicas de encriptación o codificación de datos.

Hay que mantener una cierta coherencia para determinar cuál es el grado de confidencialidad de la información que se está manejando, para así evitar un esfuerzo suplementario a la hora de decodificar una información previamente codificada.

INTEGRIDAD

La integridad de la información corresponde a lograr que la información transmitida entre dos entidades no sea modificada por un tercero y esto se logra mediante la utilización de firmas digitales.

Mediante una firma digital se codifican los mensajes a transferir, de forma que una función, denominada hash, calcula un resumen de dicho mensaje y se añade al mismo.

La validación de la integridad del mensaje se realiza aplicándole al original la misma función y comparando el resultado con el resumen que se añadió al final del mismo cuando se calculo por primera vez antes de enviarlo.

Mantener la integridad es importante para verificar que en el tiempo de viaje por la Red de la información entre el sitio emisor y receptor nadie no autorizado ha modificado el mensaje.

AUTENTIFICACION

La autentificación es el proceso de verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información. Por entidad se entiende tanto personas, como procesos o computadoras.

Existen varias formas de poder autentificarse:

- basada en claves
- basada en direcciones
- criptográfica

De estas tres posibilidades la más segura es la tercera, ya que en el caso de las dos primeras es posible que alguien escuche la información enviada y pueden suplantar la identidad del emisor de información.

Desde otro punto de vista se puede hablar de formas de autentificarse, como puede ser a través de la biometría (huellas digitales, retina del ojo, la voz, etc.), por medio de passwords o claves, y por último utilizando algo que poseamos, como un certificado digital.

Se llama autentificación fuerte a la que utiliza al menos dos de las tres técnicas mencionadas en el párrafo anterior, siendo bastante frecuente el uso de la autentificación biométrica, que como se indicó antes se basa en la identificación de personas por medio de algún atributo físico.

NO-REPUDIO

Los servicios de no-repudio ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información recibida.

Con este aspecto conseguimos que una vez que alguien ha mandado un mensaje no pueda renegar de él, es decir, no pueda negar que es el autor del mensaje.

Para el comercio electrónico es importante ya que garantiza la realización de las transacciones para las entidades participantes.

Se aplica en ambos lados de la comunicación, tanto para no poder rechazar la autoría de un mensaje, como para negar su recepción.

Es necesario identificar la información que debe conocer cada una de las entidades participantes en el proceso de comercio electrónico y con ello permitir la privacidad de forma fraccionada a las partes autorizadas para su uso.

El no repudio se consigue mediante los certificadosy lafirma digital.

La combinación de estos cuatro aspectos mencionados, que son la confidencialidad, integridad, autentificación y no-repudio, garantiza en cierto grado la seguridad en las transacciones electrónicas.

Conocer y aplicar conceptos, técnicas y algoritmos para implementar un sistema de seguridad es imprescindible para minimizar riesgos y así poder asegurar al usuario que el comercio electrónico es un mecanismo seguro en el cual puede confiar siempre que se trate con la delicadeza que requiere.

Confidencialidad → Encriptación

Integridad → Firma Digital

Autenticidad → Certificado Digital

No-repudio → Certificado y Firma Digital

3.1.1. ENCRIPTACION

El futuro del comercio electrónico, de las comunicaciones electrónicas y del almacenamiento digital de datos dependerá en gran medida de la capacidad de los sistemas para proteger la información y controlar los accesos, asegurar la integridad de los datos transmitidos o almacenados y proporcionar garantías de autenticidad. Estos requisitos ya existían en la etapa preinformática y se inventaron soluciones adecuadas para ellos. Sin embargo, la velocidad y el alcance universal de la economía digital incrementan la importancia de estos temas. En particular, si se quiere que el comercio electrónico se afiance, los usuarios se tienen que fiar de los sistemas y confiar en que no van a correr riesgos inaceptables. Hay que recalcar que la elevada velocidad de los sistemas electrónicos y su capacidad para enviar rápidamente grandes cantidades de datos exigen todavía más la necesidad de protección.

Aunque cierta regulación para proteger la información y limitar el acceso, conforme con la ley y ampliamente aplicable (como la relativa al fraude) puede ser de gran valor, la regulación por sí sola, ya sea por parte de los gobiernos o por parte de industria (autorregulación) no puede dar una solución adecuada a las necesidades de la protección de los datos y de la protección de la infraestructura de la información.

La codificación criptográfica es el medio más práctico para evitar accesos no deseados o no autorizados a los datos e información almacenados en ordenadores o transmitidos por las redes informáticas y los sistemas de telecomunicaciones. También es un medio de asegurar la integridad de los datos o de la información y la autenticidad de la fuente, y lo que quizá sea más importante, permite a los individuos proteger sus propios datos e informaciones, más que confiar en otros o confiar en los sistemas jurídicos para solucionar los problemas.

Además, esta codificación puede ser integral para los datos/información -en vez de una defensa periférica- es en cierto modo más fiable que los "firewalls" (cortafuegos) y proporciona mayores garantías. También se puede utilizar para proteger los sistemas utilizados en las redes privadas.

En paralelo con la revolución de la información, la codificación criptográfica ha sufrido en los últimos años cambios revolucionarios. Entre ellos se encuentran:

- Su uso ya no queda limitado al ámbito militar, diplomático y del espionaje, sino que empresarios y particulares la utilizan habitualmente. En efecto, en la actualidad se reconoce como indispensable en el uso de las tecnologías informáticas y de las comunicaciones para los más diversos fines, incluyendo, por supuesto, los necesarios para el comercio electrónico.
- Los militares y los espías ya no son los únicos expertos en este tema. Los gobiernos ya no son los únicos empresarios posibles para los criptógrafos y, verdaderamente, parece que para los criptógrafos y los expertos de hoy en día, los puestos de trabajo gubernamentales son considerablemente menos atractivos que los del mundo universitario, de las empresas informáticas y de otro tipo de empresas.

- El desarrollo de la criptografía de clave pública ha hecho que la codificación criptográfica sea más fácil y más práctica para numerosas aplicaciones.
- La criptografía *fuerte* (es decir, la codificación criptográfica que es imposible de descifrar) está ampliamente distribuida, a pesar de los enormes esfuerzos por parte de algunos gobiernos -sobre todo del norteamericano- para impedir su proliferación.

Dada su importancia para numerosos usos, entre los que se encuentra el comercio electrónico, es probable que en el futuro se produzca una fuerte demanda comercial de codificación. Probablemente, en el futuro se producirán más avances en este campo en el sector privado que en la Administración. Como suele ocurrir con los avances en la mayor parte de los ámbitos relacionados con las tecnologías de información, ahora que ya hemos superado las etapas iniciales de mayor riesgo, será el sector comercial el responsable de los nuevos desarrollos en tecnologías cifradas y en otros medios de protección de datos. Además el sector privado consigue cada vez más fácilmente atraer a los mejores, más brillantes y más innovadores criptógrafos, programadores y pensadores del área, ahora se dispone de enormes cantidades de capital para proyectos, algunos de los cuales entrañan considerable riesgo. Aquí se incluyen, por supuesto, las tecnologías para la protección de sistemas e información. El enorme crecimiento y desarrollo del comercio electrónico, del que ahora somos testigos, y el gran interés mostrado por el sector empresarial ponen de manifiesto que lo que se necesita en este sector se podrá conseguir. La potencia del mercado lo impulsa y la proliferación de capacidades y productos lo asegura.

3.1.1.1. METODOS DE ENCRIPTACION

La criptografía tradicional se basa en el concepto de que tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave secreta.

Los métodos de *cifrado simétrico* usan una misma clave para cifrar y descifrar. Suponiendo que dos interlocutores comparten una clave secreta y de longitud suficientemente grande, el cifrado simétrico permite garantizar la confidencialidad de la comunicación entre ellos. Este esquema es poco adecuado cuando una parte establece comunicaciones ocasionales con muchas otras con las que no tenía una relación previa, como ocurre frecuentemente en el comercio electrónico, ya que antes de poder establecer cada comunicación sería necesario intercambiar previamente por algún procedimiento seguro la clave que se va a utilizar para cifrar y descifrar en esa comunicación. Por ejemplo, un consumidor que quisiera comprar a través de Internet necesitaría intercambiar una clave secreta diferente con cada uno de los vendedores a los que quisiera acceder.

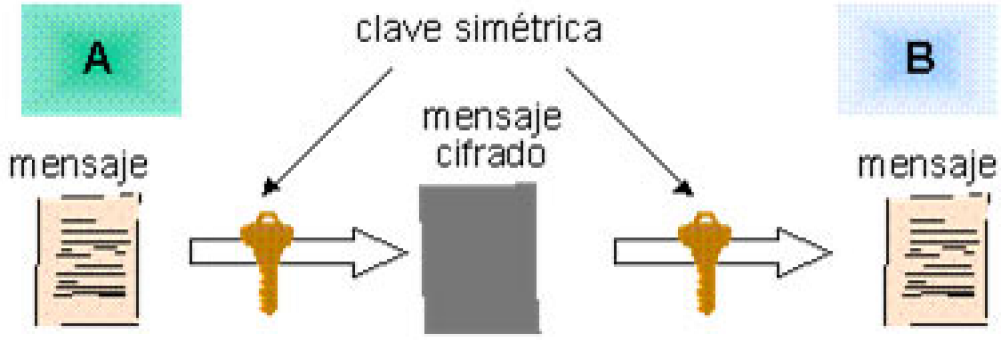


Gráfico. Cifrado / descifrado simétrico

El principal problema consiste en conseguir que ambas partes conozcan la misma clave sin que ningún tercero se entere. Si la clave es interceptada, quien la conozca podrá luego utilizarla para leer todos los mensajes encriptados.

La Criptografía con clave secreta ha tenido dificultades para brindar la seguridad necesaria en este aspecto.

Existe un acuerdo generalizado acerca de que el sistema que mayor seguridad brinda en la actualidad a las transacciones electrónicas e intercambio electrónicos de datos, es el de la Criptografía de Clave Pública, basado en algoritmos asimétricos. Nace en 1976 en la Universidad de Standford, Estados Unidos, con el propósito de resolver el problema de la administración de claves.

Los métodos de *cifrado asimétrico* usan parejas de claves con la propiedad de que lo que se cifra con una cualquiera de las claves de una pareja sólo se puede descifrar con la otra clave de la pareja. En el caso más simple, con este sistema un interlocutor sólo necesita tener una pareja de claves que puede utilizar para comunicarse de forma segura con cualquier otro interlocutor que disponga a su vez de otra pareja de claves. Cada interlocutor hace pública una de sus claves (será su clave pública) y mantiene en secreto la otra (su claveprivada). Por ello, el cifrado asimétrico se denomina también cifrado de clave pública. La clave privada (o las claves privadas si el usuario utiliza varias parejas de claves para diferentes propósitos) puede guardarse en el ordenador del usuario o en una tarjeta inteligente.

Por la propiedad de las parejas de claves citada antes, para enviar un mensaje de forma confidencial a un destinatario basta cifrarlo con la clave pública de ese destinatario. Así sólo él podrá descifrarlo mediante la clave privada que mantiene en secreto. No es necesario que el remitente y el destinatario intercambien previamente ninguna clave secreta. El remitente sólo necesita averiguar la clave pública del destinatario. Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.

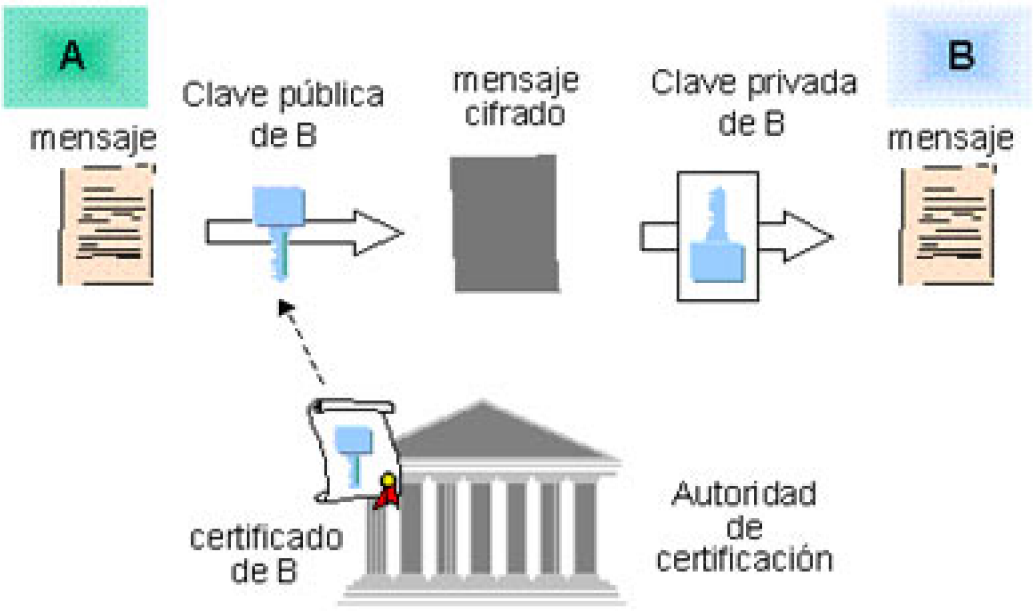


Gráfico. Cifrado asimétrico con consulta de clave pública a autoridad de certificación y descifrado con clave privada del destinatario

Por este medio, se obtienen transacciones seguras y auténticas, con la certeza de la integridad de los datos y la imposibilidad de repudio por parte del emisor. Pero para poder cumplir con estos principios, la Criptografía de Clave Pública debe basarse en una adecuada infraestructura de manejo de claves y productos adecuados, que permita identificar en forma indubitada a particulares y corporaciones con sus claves públicas, a través de terceras partes confiables (las Autoridades Certificantes).

El sistema requiere una infraestructura grande y compleja, pero esencial: sin ella los usuarios no podrán saber con quién están tratando en la red, a quién le están enviando dinero, quién firmó un documento, o si la información fue interceptada y alterada durante la transmisión.

Por ello, los usuarios demandarán una fuerte infraestructura de administración o manejo de claves basadas en autoridades certificantes que operen bajo estrictas normas predeterminadas.

Otro método es la encriptación mediante códigos de integridad, en el cual se utilizan funciones matemáticas que derivan de una huella digital a partir de un cierto volumen de datos (una huella tiene de 128 a 160 bits). Es teóricamente posible encontrar dos mensajes con idéntica huella digital; pero la probabilidad es ínfima. Si se manipulan los datos la huella cambia; y modificar los datos de forma tan sabia para obtener la misma huella es algo computacionalmente inabordable en un plazo razonable.

Y complementando éste método se encuentra la encriptación mediante firma digital, método mediante el cual dado un mensaje, basta calcular su huella digital y cifrarla con la clave secreta del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser(autenticación). Las firmas digitales suelen ir asociadas a una fecha. La fecha de

emisión (y posiblemente la fecha de vencimiento de validez) suelen proporcionarse en texto claro, e incorporarse al cálculo de la huella digital, para ligarlas irrenunciablemente.

3.1.2. FIRMA DIGITAL

La incorporación de las nuevas tecnologías de la información hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades. El avance de su implantación en todas nuestras actividades ha provocado cambios de tal magnitud que podemos afirmar que la sociedad actual está inmersa en la era de la revolución informática. Este avance no es sólo cuantitativo, sino de algo más importante, que podemos acceder a todo tipo de información y obtener con ello el beneficio correspondiente.

La información ha sido calificada como un auténtico poder de las sociedades avanzadas, ya tenía su importancia en la antigüedad, pero con el desarrollo de la telemática su valor ha crecido de forma tal que se dirige a un futuro prometedor para unos e incierto para otros.

El comercio una vez más toma la delantera e innumerables transacciones económicas se vienen realizando a través de los medios electrónicos, sin más soporte legal que el pacto entre las partes. La contratación electrónica en su más puro sentido, poco a poco se viene abriendo paso y crece de forma espectacular. Una vez más los hechos caminan delante del Derecho, entendiendo éste como Derecho positivo.

Muchas veces sucede que cuando tratamos de reconducir estos nuevos hechos a las figuras jurídicas existentes nos encontramos con dificultades. Las viejas instituciones jurídicas que, a través de los siglos han ido incorporando nuevas realidades sociales, cuando tienen que hacerlo respecto a estas nuevas tecnologías, en cierto modo chirrían y las admiten con reservas. Así ocurre cuando tratamos de adaptar el concepto de firma, tal como antiguamente se concebía, al nuevo campo de las transferencias electrónicas.

3.1.2.1. FIRMA ANALOGICA (MANUSCRITA)

En la antigua Roma, los documentos no eran firmados. Existía una ceremonia llamada *manufirmatio*, por la cual, luego de la lectura del documento por su autor o el notarius, era desplegado sobre una mesa y se le pasaba la mano por el pergamino en signo de su aceptación. Solamente después de cumplir esta ceremonia se estampaba el nombre del autor.

En el Sistema Jurídico Visigótico existía la confirmación del documento por los testigos que lo tocaban (chartam tangere), signaban o suscribían (firmatio, roboratio, stipulatio). La firma del que da el documento o librador es corriente, pero no imprescindible. Los documentos privados son, en ocasiones, confirmados por documentos reales. Desde la época euriciana las leyes visigodas prestaron atención a las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobación de escrituras. La "subscriptio", representaba la indicación del nombre del signante y la fecha, y el "signum", un rasgo que la sustituye si no sabe o no puede escribir. La "subcriptio" daba pleno valor probatorio al documento y el "signun" debía ser

completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, éste es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido.

En la Edad Media, la documentación regia viene garantizada en su autenticidad por la implantación del sello real. Sello que posteriormente pasó a las clases nobles y privilegiadas.

La firma es definida en la doctrina como el signo personal distintivo que, permite informar acerca de la identidad del autor de un documento, y manifestar su acuerdo sobre el contenido del acto.

La Real Academia de la Lengua define la firma como: "Nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice".

Otra definición de firma puede ser: "Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice.

3.1.2.1.1. CARACTERISTICAS DE LA FIRMA ANALOGICA

De las anteriores definiciones se desprenden las siguientes características:

- Identificatíva: Sirve para identificar quién es el autor del documento.
- Declarativa: Significa la asunción del contenido del documento por el autor de la firma. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.
- Probatoria: Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.

3.1.2.1.2. ELEMENTOS DE LA FIRMA ANALOGICA

Hemos de distinguir entre:

- Elementos formales

Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la firma.

- La firma como signo personal

La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

- El animus signandi

Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad de contratar.

· Elementos funcionales

Tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función:

· Identificadora: La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. La identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones. La firma manuscrita expresa la identidad, aceptación y autoría del firmante. No es un método de autenticación totalmente fiable. En el caso de que se reconozca la firma, el documento podría haber sido modificado en cuanto a su contenido -falsificado- y en el caso de que no exista la firma autógrafa parece que ya no exista otro modo de autenticación. En caso de duda o negación puede establecerse la correspondiente pericial caligráfica para su esclarecimiento.
· Autenticación: El autor del acto expresa su consentimiento y hace propio el mensaje. Destacando:

– Operación pasiva que no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado.
– Proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo.

3.1.2.2. FIRMA DIGITAL (ELECTRONICA)

Desde el punto de vista técnico, como alternativa a la firma manuscrita sobre papel se ofrecen las firmas electrónicas y/o digitales.

En el comercio electrónico el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas, que pueden ser remplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica, dentro del que tiene cabida, como categoría particular, el de firma digital.

Las firmas digitales basadas sobre la criptografía asimétrica podemos encuadrarlas en un concepto más general de firma electrónica, que no presupone necesariamente la utilización de las tecnologías de cifrado asimétrico. Aunque, generalmente, varios autores hablan indistintamente de firma electrónica o de firma digital.

La firma digital tiene los mismos cometidos que la firma manuscrita, pero expresa, además de la identidad y la autoría, la autentificación, la integridad, la fecha, la hora y la recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, GAMAL, PGP, DSA, LUC, etc.), técnicas de sellamiento electrónico y funciones Hash, lo que hace que la firma esté en función del documento que se suscribe (no es constante), pero que la hace absolutamente inimitable mientras no se tenga la clave privada con la que está

encriptada, verdadera atribución de la identidad y autoría. La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no-violación del secreto.

Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. En este concepto amplio y tecnológicamente indefinido de firma, tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (p. ej. la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación, aparte de su nula aportación respecto de la integridad del mensaje.

Algunas definiciones más exactas de firma digital podrían ser podrían ser:

- “La firma digital supone una serie de características añadidas al final de un documento. Es elaborada según procedimientos criptográficos, y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor.”
- “Es una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y de reconocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo, cuya utilización obliga a la aparición de lo que denomina entidad de certificación que será capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, al tener no solamente una formación informática, sino también jurídica.”

3.1.2.2.1. FIRMA, VERIFICACION Y ADMINISTRACION DE CLAVES

Según los técnicos, la firma digital es en la actualidad el único mecanismo que permite asegurar en un medio tan inseguro como las redes abiertas (Internet, por ejemplo), la identidad de las personas o computadoras que contratan o intercambian mensajes e información, y que dicha información no ha sufrido alteraciones durante la transmisión.

Para comprender su funcionamiento y utilización debemos apartarnos por un momento de la idea de un documento en soporte papel y su firma. La firma digital es utilizada para todo tipo de información, ya se trate de texto, sonido o imágenes.

Como adelantáramos, la firma digital está basada en la utilización de la criptografía de clave pública, es decir, en algoritmos matemáticos que operan a través del juego de un par de claves, privada y pública, las que se encuentran íntimamente vinculadas.

Toda persona que quiera “firmar” digitalmente información para su posterior transmisión debe generar su propio par de claves. Recalcamos que la bondad de la criptografía de clave pública radica en que no se necesita compartir la clave: la clave privada queda en poder del usuario y es la utilizada para “firmar”. Sólo la clave pública se publicita y es utilizada para verificar la firma.

La firma digital no se asemeja en nada a la firma tradicional. El proceso de creación del par de claves lo realiza un software especial: en general, la clave privada queda almacenada en el hardware del usuario y se activa por medio de una contraseña, aunque

también puede ser almacenada en otros dispositivos como una tarjeta inteligente.

Las claves no son otra cosa que una combinación de letras y números, es decir un conjunto de bits, que a su vez constituyen un conjunto de ceros y unos. La creación de una firma digital implica combinar los caracteres que conforman la clave privada del usuario con los caracteres del documento o información al que se le quiere adosar la firma. Este nuevo conjunto de caracteres obtenido a partir de la mezcla de los caracteres del documento/información con los de la clave privada, es lo que constituye la firma digital. En dicha mezcla quedan comprendidos todos los caracteres que conforman el documento, incluso los espacios en blanco, de forma tal que cada combinación (clave privada más documento, es decir, firma) es única para cada documento. Como se advierte, también es muy importante la longitud de la clave.

Una vez obtenida la firma, el suscriptor / emisor la transmite conjuntamente con el documento. Asimismo transmite su clave pública para ser utilizada en el proceso de verificación.

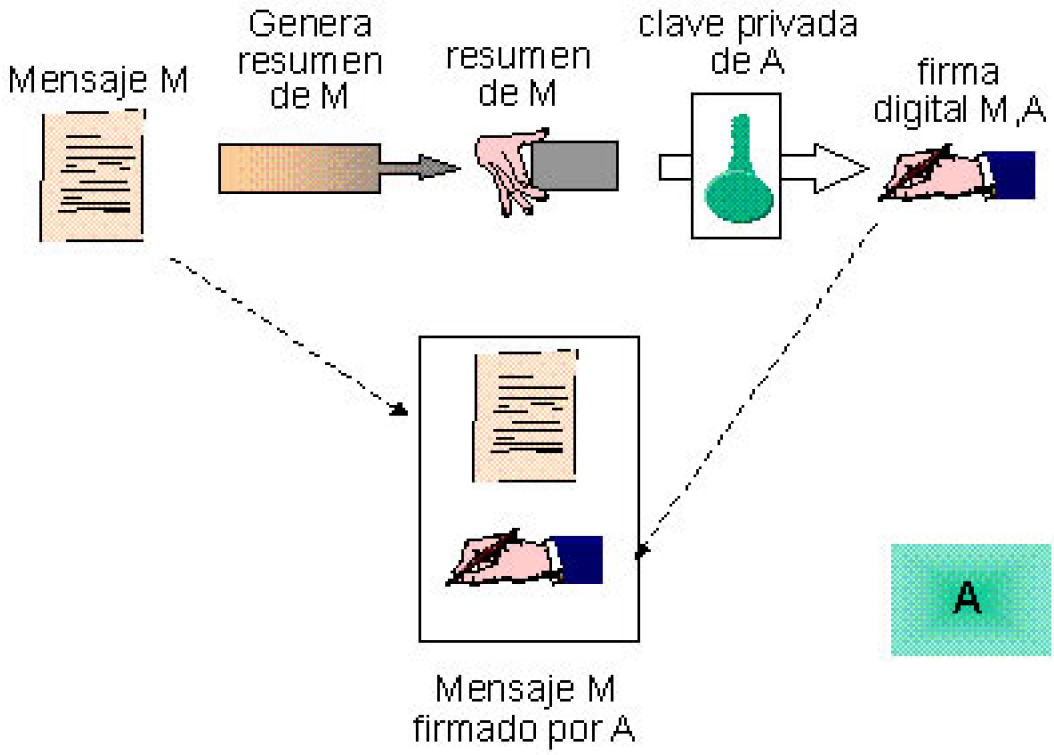


Gráfico. Generación de la firma digital de un mensaje

El destinatario recibe el documento con la firma digital y la clave pública del suscriptor. Procede entonces a iniciar el proceso de verificación de la firma digital adosada al documento recibido. Aplica la clave pública del suscriptor a la firma digital. Como resultado de este proceso se obtiene una serie de caracteres que son comparados con los que conforman el documento transmitido. Si los caracteres coinciden, la firma es válida, y garantiza que fue aplicada por el titular de la clave privada que se corresponde con la clave pública utilizada para la verificación y que el documento no ha sido alterado. Cabe señalar que todo este proceso se realiza automáticamente y en pocos segundos.

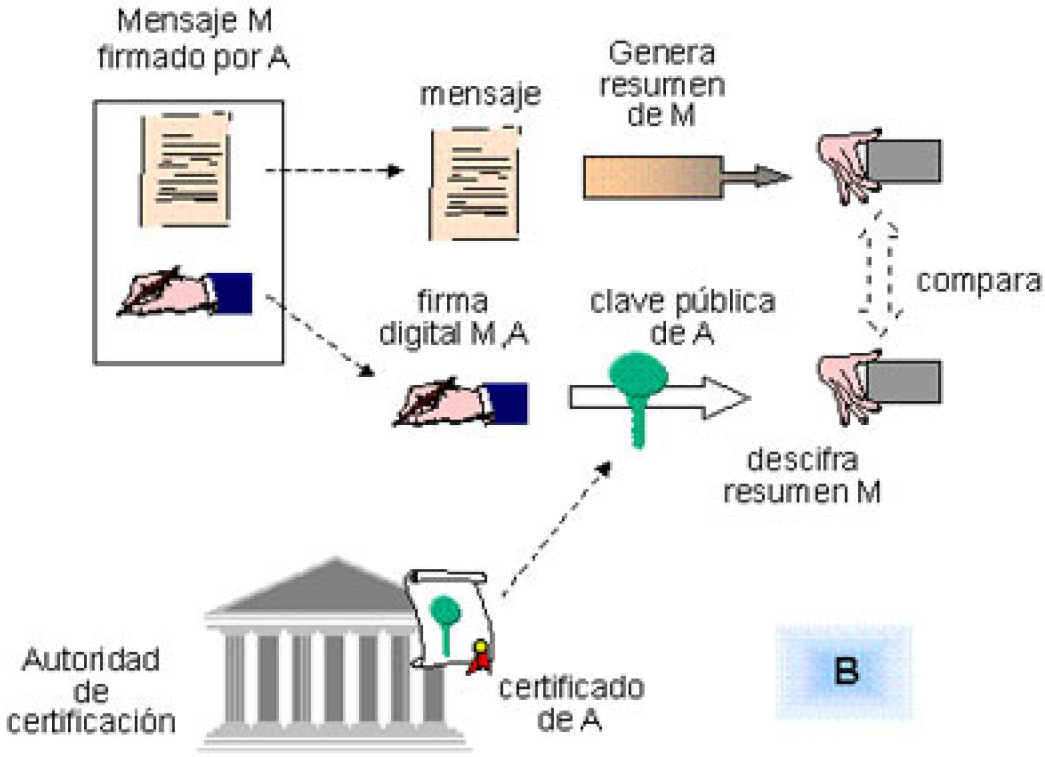
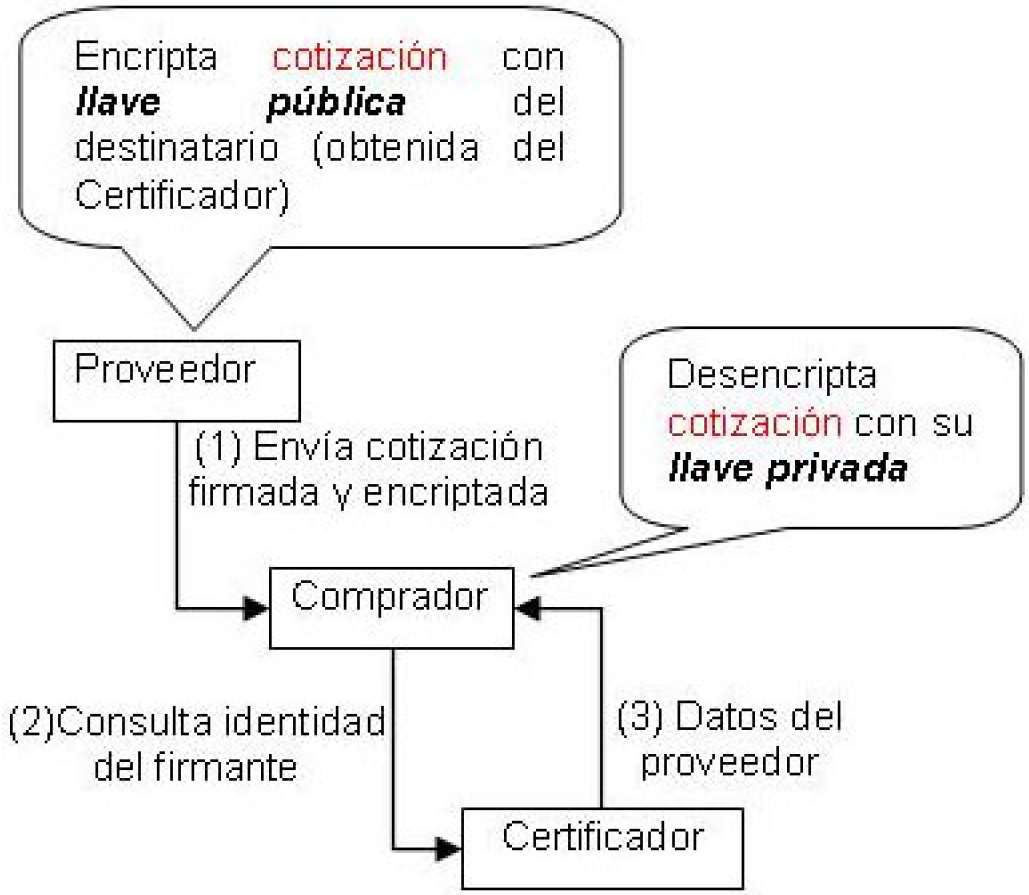


Gráfico. Comprobación de una firma digital

Si la firma es válida, el titular de la clave privada utilizada para firmar el documento/información no puede desconocerla. Pero podría suceder que alguna persona se haya apoderado de su clave privada y haya firmado por él. De allí que resulte indispensable la existencia de un sistema de administración de claves que establezca reglas claras y concretas sobre el funcionamiento y utilización de las claves, de forma tal que se puedan atribuir válidamente efectos a determinadas situaciones preestablecidas.

La administración de claves se realiza a través de “Autoridades Certificantes”. Aquél que desee ingresar en el sistema deberá registrar su clave pública ante la autoridad certificante. Dicha autoridad, previa constatación de la identidad del solicitante, emitirá un certificado que vinculará a dicha persona con su clave pública. El certificado tiene una vigencia determinada (de 1 a 3 años, por ejemplo) y contiene detalles relacionados con la validez de la clave pública.

La autoridad certificante debe registrar las claves públicas en un registro, que debe estar organizado de una manera tal que permita ser consultado "on line".



Si una persona ve comprometida su clave privada debe realizar la denuncia a la autoridad certificante quien procederá a revocar el certificado que vincula dicha clave privada a la clave pública que surge del certificado.

Volviendo al proceso de verificación de la firma digital, el receptor sólo puede verificar la firma recibida conjuntamente con el documento / información con la clave pública del emisor. Por tal motivo el suscriptor / emisor envía el documento con la firma digital y el certificado emitido por la autoridad certificante de donde surge su clave pública. Previo a la verificación de la firma, el receptor debe proceder a verificar la validez del certificado comunicándose con la autoridad certificante que ha emitido el certificado. En el ejemplo dado, denunciado el compromiso de la clave privada, y revocado el certificado por la autoridad certificante, al realizarse el proceso de verificación de la validez del certificado, la autoridad certificante indicará que el certificado ha sido revocado, por lo que el receptor no aceptará la firma del documento.

Como en la práctica no es viable que todos los usuarios estén certificados por la misma autoridad, surge la necesidad de que unas autoridades de certificación certifiquen a su vez a otras, bien de forma jerárquica (las autoridades de un nivel jerárquico son certificadas por otras de nivel superior hasta llegar a una autoridad raíz) o mediante certificaciones cruzadas entre autoridades del mismo nivel (de forma que cada una acepta como fiables los certificados emitidos por la otra). La infraestructura necesaria para el uso de los sistemas de clave pública, incluyendo las autoridades de certificación,

se llama Infraestructura de Clave Pública (PKI: Public Key Infrastructure).

La firma digital no brinda confidencialidad a la transmisión, ya que el documento se envía sin encriptar. Esto significa que el mensaje puede ser interceptado y leído por un tercero durante su transmisión. La importancia de esta aclaración radica en el hecho que las claves también pueden ser utilizadas para cifrar los mensajes.

Después de firmado digitalmente un documento se podría encriptar dicha información con la clave pública del destinatario. Esto significa que los caracteres de la información a transmitir (documento, firma digital y certificado de clave pública) se mezclan con los de la clave pública del destinatario, obteniéndose una combinación de caracteres ininteligibles. Sólo el destinatario, mediante la aplicación de su clave privada, que únicamente él conoce y que corresponde a la clave pública con la que yo he cifrado el mensaje, podría descifrar el mensaje.

Como hemos visto, la bondad de este sistema radica en el secreto de la clave privada. Dado que la firma digital no implica ocultar el mensaje, no resulta necesario el registro de claves privadas. Hay quienes consideran que los sistemas que contemplan la utilización de las claves para el encriptado de los mensajes pueden ser utilizados para cometer actos ilícitos. Por tal motivo los gobiernos ejercen fuertes presiones para que se registren las claves privadas, de forma tal que si las circunstancias lo requieren, se podría acceder a dichas claves para descifrar los mensajes.

Las bondades del sistema de firma digital, -no repudio e inalterabilidad del mensaje- en la actualidad sólo son oponibles entre las partes si existe un acuerdo previo.

Es necesario tener en cuenta lo expresado para comprender que la firma digital no ha sido ideada en base al concepto tradicional de firma, y mucho menos teniendo en cuenta las particularidades de un ordenamiento jurídico determinado.

Nos encontramos frente a un mecanismo técnico que presenta ciertos atributos que se asemejan a los de la firma tradicional que puede ser utilizado eficientemente y sin mayores complicaciones o exigencias para cierto tipo de operaciones, pero que necesita de un estudio profundo y seguramente complementado con otro tipo de sistema, para extender su utilización a actos de mayor trascendencia y envergadura. En este caso, la solución que adopta cada país o región seguramente difiere según las características del sistema de derecho imperante en ellos.

3.1.2.2.2. CARACTERISTICAS DE LA FIRMA DIGITAL

De las anteriores definiciones podemos destacar las siguientes características:

- Debe permitir la identificación del signatario. Entramos en el concepto de "autoría electrónica" como la forma de determinar que una persona es quien dice ser.
- No puede ser generada más que por el emisor del documento, infalsificable e inimitable.
- Las informaciones que se generen a partir de la firma electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla.
- La aposición de una firma debe ser significativa y va unida indisociablemente al

documento a que se refiere.

- No debe existir dilación de tiempo ni de lugar entre aceptación por el signatario y la aposición de la firma.

Además, la firma digital debe cumplir con los siguientes requisitos:

- Estar vinculada únicamente al firmante.
- Ser capaz de identificar al firmante.
- Estar creada de un modo o utilizando un medio que está únicamente bajo el control del firmante.
- Estar vinculada a los datos a los que se refiere de tal forma que si los datos son alterados la firma electrónica es invalidada.

3.1.2.2.3. LEY DE FIRMA DIGITAL

3.1.2.2.3.1. EN CHILE

A través de esta iniciativa el comercio electrónico y la transparencia del aparato público, deberían comenzar a desarrollarse enormemente, ya que significa, entre otras cosas, el primer paso para adecuar el código civil, comercial y penal, a la realidad de Internet. Así, se otorga a los contratos, trámites o transacciones que se hagan por Internet, la misma validez que los suscritos en papel, permitiendo identificar a quien los realice con mayor seguridad y certeza.

La ley define a la Firma electrónica como cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor.

Pero como lo anterior no es suficiente para comprobar la identidad del autor y de un documento firmado de esta forma, la ley hace una distinción con lo que define como “Firma electrónica avanzada”, es decir, “aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría”. Es aquí cuando empieza a jugar un rol muy importante el uso de tecnología que es lo que finalmente permitirá contar con certificados que aseguren que estos criterios sean posibles.

Dado lo anterior, se establece que la firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, pero que los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

Las excepciones a lo anterior se darán en los casos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico; cuando la ley requiera la concurrencia personal de alguna de las partes; y en los actos

relativos al derecho de familia.

Sólo las empresas que prestan servicios de certificación podrán dar la firma electrónica avanzada, ya que serán las únicas acreditadas por la Subsecretaría de Economía. Un ejemplo de ellas es una entidad vinculada a la Cámara de Comercio de Santiago, y que actualmente se encuentra operando. Por otra parte, no olvidemos que sociológicamente estamos hablando del salto del mundo del papel y la firma manual al mundo digital. Cuando un documento escrito en papel cuenta con la firma de alguien se presume que el firmante ha realizado una declaración de voluntad y asume como suyo un documento; cuando un documento electrónico —una orden de compra, una factura, etc.- cuenta con un mensaje incorporado o añadido —el certificado digital emitido por una Entidad Certificadora idónea y calificada- que indica que está firmado electrónicamente, se presume que el documento es obra del titular de la firma electrónica.

3.1.2.2.3.1.1 EL POR QUE DE SU RECIENTE INCORPORACION

Existe un tema de índole política-estratégica-económica que hace muy poco se ha solucionado, y que ha servido para que finalmente se avance en esta materia. Durante años sólo existieron en el mundo software de encriptación o de criptografía llamada ‘blanda’, esto es, que sólo permitían limitados niveles de seguridad (hasta 64 bits). Eso se debía a que Estados Unidos dictó leyes prohibiendo la exportación de esos programas, declarando querer evitar que actividades ilícitas como el tráfico de drogas o el comercio sexual en Internet estuvieran amparadas o protegidas tecnológicamente. La razón de fondo era que el país del norte quería centralizar y monopolizar el uso de la llamada ‘criptografía dura’ o de mayor cantidad de bits. Luego fueron presionados por la Unión Europea para permitir la exportación de software de hasta 128 bits, lo que se logró con creces.

3.1.2.2.3.2 . LA REGULACION DE LA FIRMA ELECTRONICA EN EL CONTEXTO INTERNACIONAL

Con el fin de constatar la tendencia mundial en el proyecto de ley, a continuación se sintetizan las principales regulaciones.

3.1.2.2.3.2.1. LA LEY DE UTAH

A finales de la década de los setenta, el gobierno de los EE.UU. publicó el Data Encryption Standard (DES) para sus comunicaciones de datos sensibles pero no clasificados. El 16 de abril de 1993, el gobierno de los EE.UU. anunció una nueva iniciativa criptográfica encaminada a proporcionar a los civiles un alto nivel de seguridad en las comunicaciones: el proyecto Clipper. Esta iniciativa está basada en dos elementos fundamentales:

- Un chip cifrador a prueba de cualquier tipo de análisis o manipulación (el Clipper chip o EES (Escrowed Encryption Standard)), y
- Un sistema para compartir las claves secretas (KES -Key Escrow System) que, en

determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y que permite conocer las comunicaciones cifradas por él.

El valor probatorio de la firma ha sido ya admitido en Utah, primer estado en dotarse de una Ley de firma digital. La firma digital de Utah (Digital Signature Act Utah de 27 de febrero de 1995, modificado en 1996) se basa en un la criptografía asimétrica.

Esta ley establece la presunción de que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumplen ciertas existencias; una de las exigencias es que la firma digital sea verificada por referencia a una clave pública incluida en un certificado válido emitido por una autoridad de certificación con licencia.

Posteriormente surgieron proyectos legislativos en Georgia, California, Washington y otros estados norteamericanos.

Estas leyes, por su uniformidad, han sido consideradas muy eficaces para promover el comercio electrónico y la nueva economía, ya que si el contenido de las leyes difiere en cada estado, sería difícil su aplicación a un entorno global como Internet.

Por ello, se ha realizado también un esfuerzo por conseguir un modelo supraestatal que pueda ser seguido por las leyes nacionales, tarea que ha sido desarrollada por organismos internacionales como la UNCITRAL.

3.1.2.2.3.2.2. EL MODELO DE UNCITRAL

La ley modelo de UNCITRAL, de 1996, tiene como objeto formular ciertas recomendaciones para que los Estados las consideren cuando promulguen o revisen sus leyes que tengan como objeto regular o fomentar el comercio electrónico.

En este sentido, esta ley modelo tiene como principal objetivo superar ciertos obstáculos jurídicos que dificulten el empleo cada vez mayor del comercio electrónico, los que consisten en la imposición de requisitos de documentación tradicional con soporte de papel.

De esta manera, la ley modelo adopta un nuevo criterio: el del "equivalente funcional".

Dicho criterio consiste en reconocer que la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente a la del papel y, en la mayoría de los casos, mayor.

Por todo lo anterior, en su artículo 5º, señala que no se podrán negar efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos. Asimismo su artículo 7º hace equivalente u homologa la firma manuscrita a la electrónica. Por último, en su artículo 10º, se reconoce la admisibilidad y fuerza probatoria de los mensajes de datos.

3.1.2.2.3.2.3. LA LEY ALEMANA

En Europa, el primer país que aprobó una ley sobre la materia, ha sido Alemania, en 1997. Dicha ley de firma electrónica se refiere, especialmente, a los requisitos del

contenido de los certificados de clave de firma y las condiciones mínimas que ha de satisfacer un servicio de certificación para poder emitir certificados. Con ello busca facilitar el uso de la firma electrónica y el comercio electrónico.

3.1.2.2.3.2.4. LA DIRECTIVA DE LA UNION EUROPEA

Frente alproblema de la seguridad de las comunicaciones electrónicas en la Unión Europea se constató la existencia de diversas iniciativas locales y, por ende, la necesidad de adoptar un marco legal común, armonizado u homogéneo para regular y reconocer el uso y los servicios de certificación de firmas digitales, solamente tratándose de redes abiertas como Internet y de forma neutral desde el punto de vista tecnológico, es decir, sin inclinarse –en la ley misma- por algún sistema de firma digital determinado como por ejemplo podría ser la criptografía de llave pública.

Cabe pues consignar que la normativa se refiere a dos temas centrales: la definición y el reconocimiento jurídico de la firma electrónica y la delimitación de quienes pueden ser Entidades Certificadoras.

En ella se define el concepto *“firma electrónica”* como la firma en forma digital integrada en unos datos, anexa a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple con cuatro requisitos copulativos, a saber:

- Estar vinculada al signatario de manera única;
- Permitir la identificación del signatario;
- Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control;
- Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos. Dicho de otro modo, se la define como el conjunto de dígitos o números que aseguran que el creador de la misma es quien efectivamente ha aprobado el contenido del documento firmado.

Respecto a los efectos legales de la firma electrónica, la ley apuntó a instituir un marco jurídico armonizado, para garantizar la eficacia jurídica o que no se negara validez, obligatoriedad y admisibilidad probatoria a una firma distinta de la manuscrita -debiendo surtir los mismos efectos jurídicos-, presentada en forma de datos electrónicos pero basada en un certificado reconocido o expedido por un proveedor de servicios de certificación competente. La regulación propuesta debe entenderse sin perjuicio de los requisitos de forma establecidos por las leyes nacionales en materia de celebración de contratos ni de las normas que determinan cuando él se considera concluido.

Respecto a los Proveedores de Servicios de Certificación de firma electrónica, se estima innecesario un marco reglamentario dentro de sistemas cerrados, la Directiva sólo considera requisitos esenciales mínimos particularmente relacionados con su responsabilidad al expedir los certificados frente a los terceros o “consumidores” que utilicen sus servicios, de manera tal que existan normas comunes y armonizadas precisamente respecto a dicha responsabilidad y que se permita el reconocimiento de

firmas y certificados digitales al interior de toda la Comunidad Europea. Los Estados miembros velarán porque sean responsables, ante cualquier persona de buena fe que confíe en el certificado, acerca de aspectos tales como la veracidad de la información contenida en el certificado reconocido a partir de la fecha de su expedición, la existencia de dispositivos de creación y verificación de firma, que se puedan establecer límites a los usos del certificado, etc.

Una norma de particular importancia, es la contenida en el artículo 6º de la Directiva. Dicho precepto señala que los servicios de certificación serán responsables, ante cualquier persona que de buena fe haya confiado en el certificado, acerca de su conformidad con la ley y la veracidad de su contenido. Esta responsabilidad se encuentra objetivizada, toda vez que el prestador de servicios de certificación se exime de responsabilidad en cuanto demuestra haber actuado siempre con la máxima diligencia para comprobar la información proporcionada por la persona certificada, invirtiéndose de este modo la carga de la prueba.

3.1.2.2.3.2.5. LA LEY ESPAÑOLA

Las leyes europeas nacionales que han seguido la Directiva, han optado por el sistema parcial y minimalista para regular la nueva economía.

El mejor ejemplo de esta tendencia es el Real Decreto Ley 14/1999, de 17 de septiembre de 1999, sobre firma electrónica de España.

Esta ley crea un sistema en que los usuarios certifican la firma electrónica avanzada con prestadores de servicios de certificación, quienes llevan el registro de las claves públicas. Los prestadores pueden emitir certificados reconocidos en conformidad con la ley o no, y depende de los usuarios la preferencia por unos y otros; pero los certificados reconocidos para ser tales, han de cumplir una serie de requisitos establecidos en la ley.

La autoridad es el Ministerio de Fomento, el que controla, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos, de las obligaciones establecidas en la ley y su reglamento, vigilando asimismo el cumplimiento, por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las reglas legales mínimas.

3.1.2.2.3.2.6. LA LEY DE ITALIA

La Ley de 15 de marzo de 1997 número 59, es la primera norma del ordenamiento jurídico italiano que recoge el principio de la plena validez de los documentos informáticos.

Se define la firma digital como el resultado del proceso informático (validación) basado en un sistema de claves asimétricas, que permite al suscriptor transmitir la clave privada y al destinatario transmitir la clave pública, respectivamente, para verificar la procedencia y la integridad de un documento informático o de un conjunto de documentos informáticos (artículo 1º apartado b). En el reglamento la firma digital está basada exclusivamente en el empleo de sistemas de cifrado llamados asimétricos.

Regulan la Ley y el Reglamento entre otras cosas: La validez del documento informático; el documento informático sin firma digital; el documento informático con firma digital; los certificadores; los certificados; autentificación de la firma digital; el "cybernotary"; los actos públicos notariales; la validación temporal; la caducidad, revocación y suspensión de las claves; la firma digital falsa; la duplicidad, copia y extractos del documento; y la transmisión del documento.

3.1.2.2.3.2.7. LA LEY FEDERAL NORTEAMERICANA

En Estados Unidos, recientemente, se ha promulgado la ley federal sobre Firmas Electrónicas en el Comercio Nacional y Global (Electronic Signatures in Global and National Commerce Act).

Siguiendo los criterios expuestos, establece una regla general de validez para todos los actos o transacciones celebrados por medios electrónicos. Vale decir, ninguna ley, reglamento o norma podrá negar valor legal a un acto o contrato por el sólo hecho que su firma está en una forma electrónica. Además, esta ley introduce un interesante capítulo sobre ciertos derechos básicos que deben tener los consumidores que van a realizar transacciones por medios electrónicos.

3.1.2.2.3.2.8. LA OCDE

La Recomendación de la OCDE (Organización para la Cooperación y Desarrollo Económico) sobre la utilización de criptografía (Guidelines for Cryptography Policy) fue aprobada el 27 de marzo de 1997. Esta recomendación no tiene fuerza vinculante y señala una serie de reglas que los gobiernos debieran tener en cuenta al adoptar legislación sobre firma digital y terceros de confianza, con el fin de impedir la adopción de diferentes reglas nacionales que podrían dificultar el comercio electrónico y la sociedad de la información en general.

3.1.3. 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 pues 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.

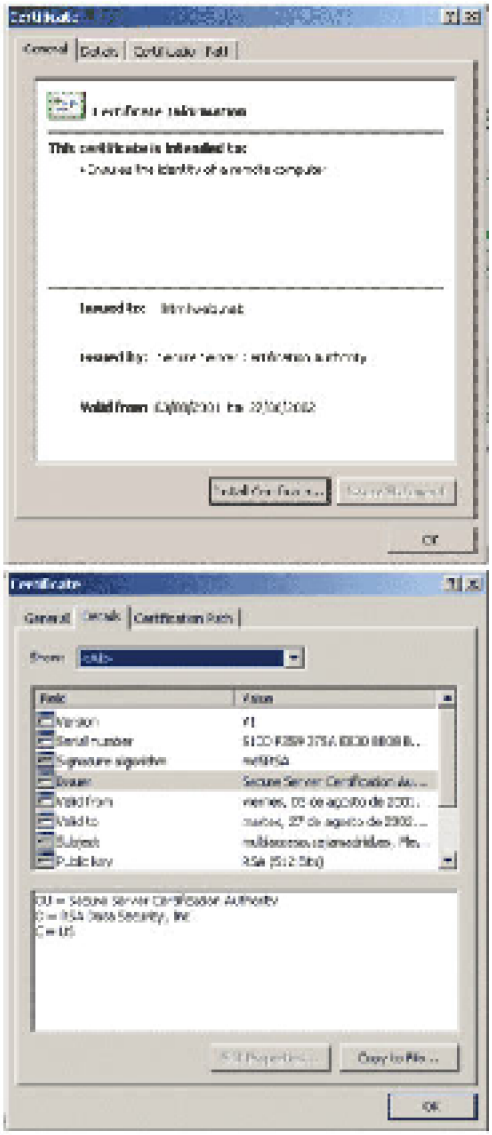
La solución a este problema la trajo la aparición de los Certificados Digitales o Certificados Electrónicos, documentos electrónicos basados en la criptografía de clave

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 Certificadoras.

El sistema es análogo a otros de uso común, como la cédula de identidad, en el que una autoridad de confianza (el estado o la policía) atestigua que la persona portadora de dicho documento es quién dice ser.

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 es el siguiente:



Los datos que figuran generalmente en un certificado son:

1. Versión: versión del estándar X.509, generalmente la 3, que es la más actual.

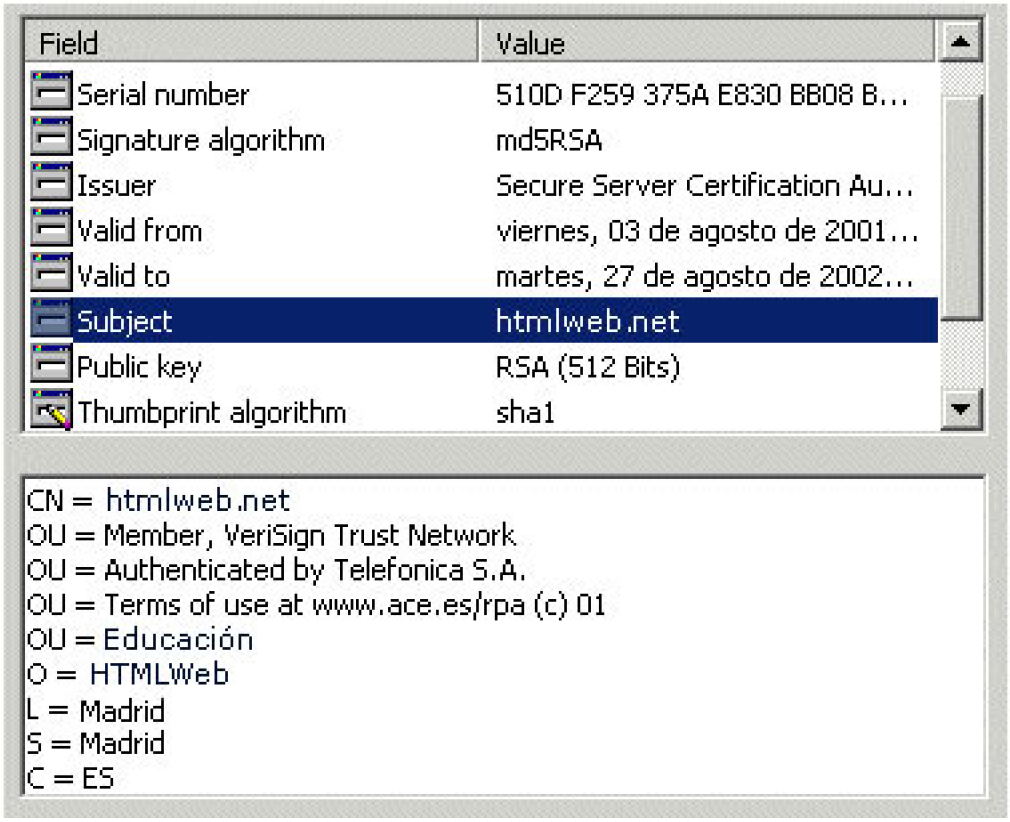
2. Número de serie: número identificador del certificado, único para cada certificado expedido por una AC determinada.

3. Algoritmo de firma: algoritmo criptográfico usado para la firma digital.

4. Autoridad Certificadora: datos sobre la autoridad que expide el certificado.

5. Fechas de inicio y de fin de validez del certificado. Definen el periodo de validez del mismo, que generalmente es de un año.

6. Propietario: persona o entidad vinculada al certificado. Dentro de este apartado se usan una serie de abreviaturas para establecer datos de identidad. Un ejemplo sería:



CN	Nombre común del usuario
OU	Información varia
O	Organización
L	Ciudad
S	Estado (provincia)
C	País
E	Correo electrónico
UID	ID de usuario

7. Llave pública: representación de la llave pública vinculada a la persona o entidad

(en hexadecimal), junto con el algoritmo criptográfico para el que es aplicable.

8. Algoritmo usado para la misma para obtener la firma digital de la Autoridad Certificadora.

9. Firma de la Autoridad Certificadora, que asegura la autenticidad del mismo.

10. Información adicional, como tipo de certificado, etc.

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.

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.

3.1.3.1. 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 fácil 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 los 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 pues 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, 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 que certifique el momento de la recepción 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 autenticidad de la respuesta recibida.

3.1.3.2. EMISION DE CERTIFICADOS DIGITALES

Los certificados digitales, como ya hemos dicho, son emitidos por las Autoridades de Certificación, entidades consideradas de confianza probada, como la internacional Verisign o en Chile e-cert. 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, confeccionando 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 al computador. 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.

3.1.3.3. 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:

1. 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.

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

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

4. 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.

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

Toda persona o entidad que desee obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor), más costará el certificado.

3.1.4. AUTORIDAD O ENTIDAD DE CERTIFICACION DE LAS CLAVES

La creciente interconexión de los sistemas de información, posibilitada por la general aceptación de los sistemas abiertos, y las cada vez mayores prestaciones de las actuales redes de telecomunicación, obtenidas principalmente de la digitalización, están potenciando formas de intercambio de información impensables hace pocos años. A su vez, ello está conduciendo a una avalancha de nuevos servicios y aplicaciones telemáticas, con un enorme poder de penetración en las emergentes sociedades de la información. Así, el teletrabajo, la teleadministración, el comercio electrónico, etc., están modificando revolucionariamente las relaciones económicas, administrativas, laborales de tal forma que en pocos años serán radicalmente distintas de como son ahora.

Todos estos nuevos servicios y aplicaciones no podrán desarrollarse en plenitud a no ser que se les dote de unos servicios y mecanismos de seguridad fiables. Dentro del sistema de seguridad que indicamos, para que cualquier usuario pueda confiar en otro usuario se deben establecer ciertos protocolos. Los protocolos sólo especifican las reglas de comportamiento a seguir.

Existen diferentes tipos de protocolos en los que intervienen terceras partes confiables (Trusted Third Party, TTP):

- Los protocolos arbitrados. En ellos una AC o Autoridad de Certificación participa en la transacción para asegurar que ambos lados actúan según las pautas marcadas por el protocolo.
- Los protocolos notariales. En este caso la AC, además de garantizar la correcta operación, también permite juzgar si ambas partes actuarán por derecho según la evidencia presentada a través de los documentos aportados por los participantes e incluidos dentro del protocolo notarial. En estos casos, se añade la firma (digital) del notario a la transacción, pudiendo éste testificar, posteriormente, en caso de disputa.
- Los protocolos autoverificables. En estos protocolos cada una de las partes puede darse cuenta si la otra actúa deshonestamente, durante el transcurso de la operación. La firma digital en sí, es un elemento básico de los protocolos autoverificables, ya que no precisa de la intervención de una Autoridad de Certificación para determinar la validez de una firma.

3.1.4.1. ¿QUE ES UNA AUTORIDAD DE CERTIFICACION?

Es esa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actuaría como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información. Sin embargo ¿quién autoriza a dicha autoridad?, Es decir, ¿cómo sé que la autoridad es quién dice ser?, ¿Deberá existir una autoridad en la cúspide de la pirámide de autoridades certificadoras que posibilite la autenticación de las demás?.

En USA la ley de Utah sobre firma digital da una importancia fundamental a las Autoridades Certificantes, definidas como las personas facultadas para emitir certificados. Pueden ser personas físicas o empresas o instituciones públicas o privadas y deberán obtener una licencia de la Division of Corporations and Commercial Code. Están encargadas de mantener los registros directamente en línea de claves públicas.

Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser fiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que certifique la validez de su clave. Esta solución da origen a diferentes niveles o jerarquías de CAs.

En cuanto a los Certificados, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.

Contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un Registro (Repository), considerado como una base de datos a la que el público puede acceder directamente en línea para conocer acerca de la validez de los mismos. Los usuarios o firmantes son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante.

La Autoridad Certificante puede emitir distintos tipos de certificados:

- Certificados de identificación: identifican y conectan un nombre a una clave pública.
- Certificados de autorización: ofrecen otro tipo de información correspondiente al usuario, como por ejemplo la dirección comercial, antecedentes, catálogos de productos, etc.
- Otros certificados colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para dar fe de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido.
- Otros certificados permiten determinar día y hora en que el documento fue digitalmente firmado (Digital time-stamp certificates).

El interesado en operar dentro del esquema establecido por la ley, deberá, una vez creado el par de claves, presentarse ante la autoridad certificante (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita “firmar” el documento de que se trate. Por ejemplo, para realizar una operación financiera de importancia con un banco, éste puede requerir al interesado un certificado del que surja, además de la constatación de su identidad, el análisis de sus antecedentes criminales o financieros. Esto quiere decir que la firma digital del interesado sólo será aceptada por la

otra parte si cuenta con el certificado apropiado para la operación a realizar.

Los Repository o Registros son la base de datos a la que el público puede acceder on line para conocer la validez de los certificados, su vigencia o cualquier otra circunstancia que se relacione con los mismos. Dicha base de datos debe incluir, entre otras cosas, los certificados publicados en el repositorio, las notificaciones de certificados suspendidos o revocados publicadas por las autoridades certificantes acreditadas, los archivos de autoridades certificantes autorizadas y todo otro requisito exigido por la División. Para ser reconocido, el repositorio debe operar bajo la dirección de una autoridad certificante acreditada.

¿QUE SON LOS SERVIDORES DE CERTIFICADOS?

Son aplicaciones destinadas a crear, firmar y administrar certificados de claves, y que permiten a una empresa u organización constituirse en autoridad de certificación para sostener sus propias necesidades. Los productos más famosos son Netscape Certificate Server y OpenSoft.

3.1.4.2. REQUISITOS DE LAS AUTORIDADES DE CERTIFICACION SEGUN EL GRUPO DE TRABAJO SOBRE COMERCIO ELECTRONICO DE LA COMISION DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL.

El plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/UNCITRAL), que celebró su 29º periodo de sesiones en New York del 28 de marzo al 14 de Junio de 1996. Examinó el proyecto de ley Modelo sobre distintos aspectos del intercambio electrónico de datos (EDI), aprobándolo con la denominación de Ley Modelo sobre comercio electrónico. Tras un debate la Comisión encomendó al Grupo de Trabajo, ahora denominado "sobre Comercio Electrónico" que se ocupara de examinar las cuestiones relativas a las firmas digitales y las autoridades de certificación.

La Comisión pidió a la secretaria que preparara un estudio de antecedentes sobre cuestiones relativas a las firmas digitales y a los proveedores de servicios, basándose en un análisis de las leyes que se estaban elaborando en varios países. Dicho estudio quedó recogido en el documento A/CN.9/WGIV/WP.71 de 31 de Diciembre de 1996. El grupo de trabajo celebró su 31 periodo de sesiones en New York del 18 al 28 de febrero de 1997 centrando su debate en el proyecto de prácticas internacionales uniformes sobre autenticación y certificación de la Cámara de Comercio Internacional y las directrices sobre firmas digitales publicadas por la American Bar Asociation (contenido de dicho debate se encuentra en el anexo 1).

Dentro de esta sesión se abrió el debate sobre la necesidad o no de autorización y del establecimiento de requisitos, ya sean referidos a la propia entidad o al certificado. A tal efecto se ofreció el debate a partir de los criterios que se mencionan en el párrafo 44 del WP.71:

- Independencia (ausencia de interés financiero o de otro tipo en las transacciones

subyacentes).

- Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de pérdida
- Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados.
- Longevidad (conservación de certificados).
- Aprobación del equipo y los programas.
- Mantenimiento de un registro de auditoria y realización de auditorias por una entidad independiente.
- Existencia de un plan para casos de emergencia.
- Selección y administración del personal.
- Disposiciones para proteger su propia clave privada
- Seguridad interna.
- Disposiciones para suspender las operaciones, incluida la notificación a los usuarios.
- Garantías y representaciones.
- Limitación de la responsabilidad.
- Seguros.
- Capacidad para intercambiar datos con otras autoridades certificadoras.
- Procedimientos de revocación.

El valor otorgado por el grupo de trabajo sobre estos principios es el de factores a tener en cuenta en la confiabilidad de una determinada Autoridad de Certificación.

3.1.4.3. FUNCIONES DE LAS AUTORIDADES DE CERTIFICACION

Las funciones de una Autoridad de Certificación deben ser, entre otras, las siguientes:

- Generación y Registro de claves.
- Identificación de Peticionarios de Certificados.
- Emisión de certificado.
- Almacenamiento en la AC de su clave privada.
- Mantenimiento de las claves vigentes y revocadas.
- Servicios de directorio.

3.1.4.4. EJEMPLO DE ENTIDAD DE CERTIFICACION (VERISIGN)

VeriSign es una de las empresas que brinda servicios de certificación. Estos servicios han sido diseñados básicamente para brindar seguridad al comercio electrónico y a la utilización de la firma digital. Para el logro de este objetivo, las autoridades de emisión (Issuing Authorities, "IA") autorizadas por VeriSign funcionan como terceras partes

confiables, emitiendo, administrando, suspendiendo o revocando certificados de acuerdo con la práctica pública de la empresa.

Las IA facilitan la confirmación de la relación existente entre una clave pública y una persona o nombre determinado. Dicha confirmación es representada por un certificado: un mensaje firmado digitalmente y emitido por una IA.

El proceso de certificación incluye servicios de registro, "naming", autenticación, emisión, revocación y suspensión de los certificados. Esta empresa ofrece tres niveles de servicios de certificación. Cada nivel o clase de certificados ofrece servicios específicos en cuanto a funcionalidad y seguridad. Los interesados eligen entre estos grupos de servicios el que más le conviene según sus necesidades, debiendo especificar qué clase de certificado desean. Dependiendo de la clase de certificado requerido, los interesados pueden solicitarlos y obtenerlos electrónicamente siguiendo las instrucciones detalladamente indicadas, o deberán concurrir personalmente a una Autoridad de Registro Local o LOCAL REGISTRATION AUTHORITY (LRA), o a un delegado, que puede ser un notario. Pueden existir varias "IA" para cada uno de los distintos niveles. Cumplidos los requisitos exigidos se emite el certificado o se envía un borrador para su aceptación por el interesado, según el caso.

TIPOS DE CERTIFICADOS

- Certificados Clase 1: son emitidos y comunicados electrónicamente a personas físicas, y relacionan en forma indubitable el nombre del usuario o su "alias" y su dirección de E-mail con el registro llevado por VeriSign. No autentican la identidad del usuario. Son utilizados fundamentalmente para Web Browsing y E-mail, afianzando la seguridad de sus entornos.

En general, no son utilizados para uso comercial, donde se exige la prueba de identidad de las partes.

- Certificados Clase 2: son emitidos a personas físicas, y confirman la veracidad de la información aportada en el acto de presentar la aplicación y que ella no difiere de la que surge de alguna base de datos de usuarios reconocida. Es utilizado para comunicaciones intra-inter organizaciones vía E-mail; transacciones comerciales de bajo riesgo; validación de software y suscripciones on line. Después del acuerdo del usuario, realizado on line ante una LRA, los datos contenidos en la aplicación son confirmados comparándolos con una base de datos reconocida. Teniendo en cuenta dicha confirmación la LRA puede aprobar o rechazar la aplicación. En caso de aprobación, la conformación es enviada por correo. Debido a las limitaciones de las referidas bases de datos, esta clase de certificados está reservada a residentes en los Estados Unidos y Canadá.
- Los Certificados Clase 3: son emitidos a personas físicas y organizaciones públicas y privadas. En el primer caso, asegura la identidad del suscriptor, requiriendo su presencia física ante una LRA o un notario. En el caso de organizaciones asegura la existencia y nombre mediante el cotejo de los registros denunciados con los contenidos en bases de datos independientes. Son utilizados para determinadas

aplicaciones de comercio electrónico como “electronic banking” y ELECTRONIC DATA INTERCHANGE (EDI). Como las autorizadas por VERISIGN firman digitalmente los certificados que emiten, la empresa asegura a los usuarios que la clave privada utilizada no está comprometida, valiéndose para ello de productos de hardware. Asimismo, recomiendan que las claves privadas de los usuarios sean encriptadas vía software o conservadas en un medio físico (smart cards o PC cards).

CAPITULO 4: “SEGURIDAD EN LA TRANSMISION”

La seguridad de este tipo se basa en el hecho de poder encriptar los mensajes que se envían por a red entre un servidor y un cliente y que solo ellos puedan descifrar los contenidos a partir de una clave común conocida solo por los dos.

Como vimos anteriormente, toda transacción segura por la red debe contemplar los aspectos de Autenticidad, Integridad, Confidencialidad y No Repudio. Son varios los sistemas y tecnologías que se han desarrollado para intentar implementar estos aspectos en las transacciones electrónicas, siendo sin duda SSL el más conocido y usado en la actualidad. SSL permite la Confidencialidad y la Autentificación en las transacciones por Internet, siendo usado principalmente en aquellas transacciones en la que se intercambian datos sensibles, como números de tarjetas de crédito o contraseñas de acceso a sistemas privados. SSL es una de las formas base para la implementación de soluciones PKI (Infraestructuras de Clave Pública).

4.1. SSL - SECURE SOCKET LAYER

Secure Socket Layer es un sistema de protocolos de carácter general diseñado en 1994 por la empresa Nestcape Communcations Corporation, y está basado en la aplicación

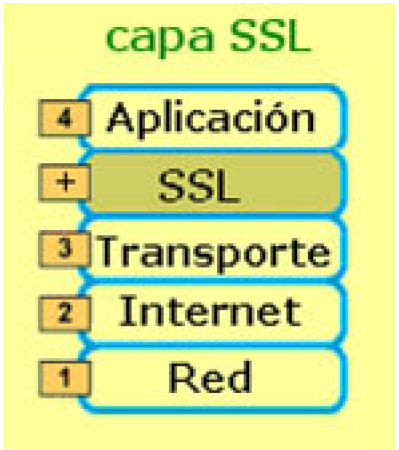
conjunta de Criptografía Simétrica, Criptografía Asimétrica, certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet. De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se 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.

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket (nombre de máquina más puerto), de forma transparente al usuario y a las aplicaciones que lo usan.

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).



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 resúmenes usados 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 difícil de romper. Se aplica 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. Es 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.
- 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 (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. 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 intercambiados (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.

Además, las páginas que proceden de un servidor SSL vienen implementadas mediante protocolo HTTP seguro, por lo que su dirección, que vemos en la barra de direcciones del navegador, empezará siempre por https, como por ejemplo:

https://www. santandersantiago .cl/transa/segmentos/sneutro/index.asp

Por último, cuando estamos en una conexión segura podemos ver el certificado del servidor acudiendo al menú “Archivo” del navegador y pinchando en “Propiedades”. En la parte inferior tenemos una opción “Certificados” que nos mostrará el del servidor actual.

Vamos a ver a continuación de forma detallada el proceso completo de trabajo de SSL.

4.1.1. PROTOCOLOS SECURE SOCKET LAYER

Para establecer una comunicación SSL es necesario que previamente el cliente y el servidor realicen un proceso de reconocimiento mutuo y de petición de conexión que, al igual que en otros tipos de comunicaciones, recibe el nombre de apretón de manos o Handshake, que en este caso está controlado por el Protocolo SSL Handshake, que se encarga de establecer, mantener y finalizar las conexiones SSL. Durante el mismo se negocian los parámetros generales de la sesión y los particulares de cada conexión.

Concretamente, y de forma general, el protocolo comienza con el saludo del cliente al servidor, conocido como Client Hello, por el que se informa al servidor de que se desea establecer una comunicación segura con él. SSL soporta solicitudes de conexión por puertos diferentes al utilizado normalmente para este servicio. Junto con este saludo inicial, el cliente envía al servidor información de la versión de SSL que tiene

implementada, de los algoritmos de encriptación que soporta, las longitudes de clave máximas que admite para cada uno de ellos y las funciones hash que puede utilizar. También se le solicita al servidor el envío de su Certificado Digital X.509 v3, con objeto de verificar el cliente la identidad del mismo y recoger su clave pública. En este momento se asigna un identificador a la sesión y se hace constar la hora y fecha de la misma.

Como medida adicional, el cliente envía asimismo una clave numérica aleatoria, para que se pueda establecer una comunicación segura mediante otros protocolos o algoritmos en el caso de que el servidor web no posea un Certificado Digital.

En este paso no se intercambia en ningún momento información sensible, tan sólo información necesaria para establecer la comunicación segura.

A continuación, el servidor SSL responde al cliente en el proceso que se conoce con el nombre de Server Hello, enviándole su Certificado Digital (con su llave pública) e informándole de su versión de SSL, de los algoritmos y longitudes de clave que soporta.

Generalmente se obtiene el conjunto de algoritmos, longitudes de clave y funciones hash soportados por ambos, eligiéndose entonces los más fuertes. Si no hay acuerdo con los algoritmos a usar se envía un mensaje de error.

A veces, y si la comunicación posterior así lo exige, el servidor solicita al cliente su Certificado Digital, en el mensaje llamado CertificateRequest. Esto sólo suele ocurrir en SSL cuando los datos a transferir sean especialmente sensibles y precisen la previa autenticación del cliente. Si es el caso, el cliente debe contestar al servidor mediante el mensaje CertificateVerify, enviándole entonces su certificado.

En este momento el cliente verifica la validez del Certificado Digital del servidor, desencriptando el resumen del mismo y comprobando su corrección, verificando que ha sido emitido por una Autoridad Certificadora de confianza, que esté correctamente firmado por ella y que el certificado no esté revocado. También se comprueba que la fecha actual está dentro del rango de fechas válidas para el certificado y que el dominio (URL) que aparece en el certificado se corresponde con el que se está intentando establecer la comunicación segura. Si alguna de estas validaciones falla, el navegador cliente rechazará la comunicación, dándola por finalizada e informando al usuario del motivo del rechazo.

En caso de que el servidor no tenga un Certificado X.509 v3 se puede utilizar un mensaje ServerKeyExchange para enviar la clave pública sin certificado, en cuyo caso queda en manos del cliente la elección de si acepta la llave o no, lo que finalizaría el proceso.

Como medida adicional de seguridad, el cliente genera una clave aleatoria temporal y se la envía al servidor, que debe devolvérsela cifrada con su clave privada. El cliente la descifra con la llave pública y comprueba la coincidencia, con lo que está totalmente seguro de que el servidor es quién dice ser. Y un proceso análogo a éste, pero en sentido inverso, se requiere si es necesaria la autenticación del usuario ante el servidor.

Si todo está correcto el cliente genera un número aleatorio que va a servir para calcular una clave de sesión correspondiente al algoritmo de encriptación simétrico negociado antes, conocida con el nombre de clave maestra, que es enviada al servidor

de forma segura encriptándola asimétricamente con la llave pública del mismo que aparece en el Certificado Digital. Esta clave maestra se usará para generar todas las claves y números secretos utilizados en SSL.

Con esto servidor y cliente se han identificado y tienen en su poder todos los componentes necesarios para empezar a transmitir información cifrada simétricamente.

Se pasa entonces el control al subprotocolo Change Cipher Spec, iniciándose la conexión segura.

Así y todo, para que empiecen las transmisiones de datos protegidos se requiere otra verificación previa, denominada Finished, consistente en que cliente y servidor se envían uno al otro una copia de todas las transacciones llevadas a cabo hasta el momento, encriptándola con la llave simétrica común. Al recibir esta copia, cada host la desencripta y la compara con el registro propio de las transacciones. Si las transacciones de los dos host coinciden significa que los datos enviados y recibidos durante todo el proceso no han sido modificados por un tercero. Se termina entonces la fase Handshake.

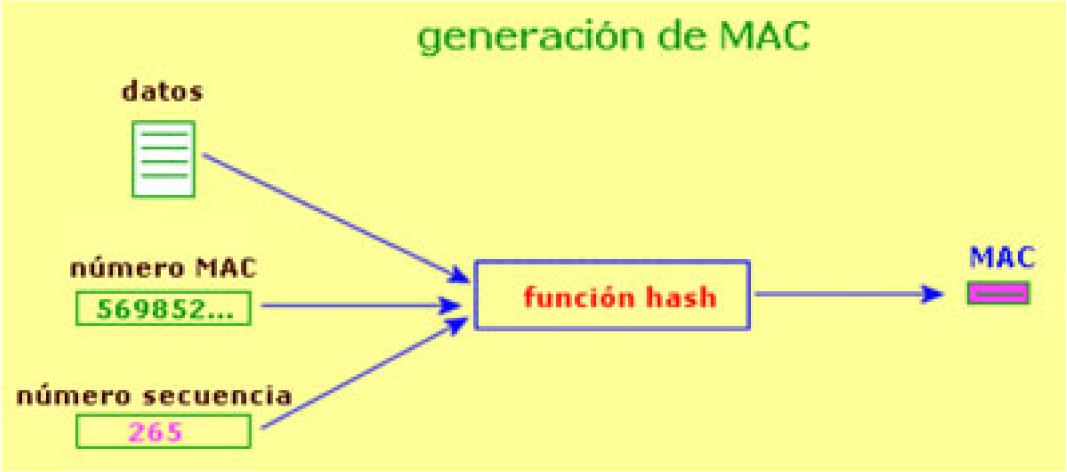
Para empezar a transmitir datos cifrados en necesario que cliente y servidor se pongan de acuerdo respecto a la forma común de encapsular los datos que se van a intercambiar, es decir, qué formato de datos se va a usar en la transmisión cifrada. Esto se realiza mediante el Protocolo SSL Record (Protocolo de Registro SSL), que establece tres componentes para la porción de datos del protocolo:

1. MAC-DATA: código de autenticación del mensaje.
2. ACTUAL-DATA: datos de aplicación a transmitir.
3. PADDING-DATA: datos requeridos para rellenar el mensaje cuando se usa un sistema de cifrado en bloque.

El Protocolo de Registro es el encargado de la seguridad en el intercambio los datos que le llegan desde las aplicaciones superiores, usando para ello los parámetros de encriptación y resumen negociados previamente mediante el protocolo SSL Handshake. Sus principales misiones son:

- La fragmentación de los mensajes mayores de 2^{14} bytes en bloques más pequeños.
- La compresión de los bloques obtenidos mediante el algoritmo de compresión negociado anteriormente.
- La autenticación y la integridad de los datos recibidos mediante el resumen de cada mensaje recibido concatenado con un número de de secuencia y un número secreto establecidos en el estado de conexión. El resultado de esta concatenación se denomina **MAC**, y se añade al mensaje. Con esta base, la autenticación se

comprueba mediante el número secreto, compartido por el cliente y el servidor, y mediante el número de secuencia, que viaja siempre encriptado. La integridad se comprueba mediante la función hash negociada.



La confidencialidad se asegura encriptando los bloques y sus resúmenes mediante el algoritmo simétrico y la clave correspondiente negociadas en la fase Handshake. Existen dos tipos posibles de encriptación:

- Cifrado en bloque: se cifran los datos en bloques de 64 bits. Si el mensaje no es múltiplo de 64 bits se le añaden los bits de relleno necesarios para obtener un número entero de bloques completos, indicándose la adición en el formato del mensaje. Este método de cifrado se conoce con el nombre de Chipher Block Chainning, CBC, y precisa un vector inicial, que habrá sido negociado previamente en la fase Handshake. Como algoritmos de cifrado se usan RC2 y DES.
- Cifrado Stream o de flujo, en el que se encriptan los datos realizando una operación lógica OR-Exclusiva entre los bytes y un generador pseudoaleatorio usando el algoritmo RC4.

Tras todos estos requisitos, el canal seguro está listo para empezar la transmisión de datos de forma segura. Cuando el cliente o el servidor desean transmitir algún mensaje al otro se genera automáticamente un resumen del mismo mediante la función has acordada, se encriptan mensaje y resumen con la clave simétrica acordada y se envían los datos. Cuando el destinatario los recibe, desencripta todo, vuelve a obtener el resumen a partir del original y lo compara con el recibido. Si coinciden hay seguridad de que la comunicación segura se ha producido satisfactoriamente, sin intromisiones externas. Si no coinciden, se pone en conocimiento del otro host, y si es preciso se suspende la conexión SSL. Cada uno de los mensajes enviados por cliente o servidor sufre este proceso de verificación.

Por último, cuando la transferencia de mensajes ha finalizado y se desea cerrar la comunicación segura, generalmente porque el cliente así lo desea, la aplicación cliente (el navegador web, p.e.) lanza una ventana de aviso de que se va a cerrar la comunicación SSL, y si es aceptada por el usuario, se sale de la misma y se regresa a

una comunicación normal, finalizando el proceso SSL.

SSL actúa computacionalmente como una máquina de estados: durante el intercambio de datos hay en todo momento un estado de escritura activo y otro pendiente y lo mismo ocurre respecto a la lectura de datos, realizándose el cambio de estados mediante un subprotocolo especial del Handshake denominado Change Cipher Spec.

SSL Handshake posee además otro subprotocolo específico, denominado Alerta, que se encarga de avisar de los problemas que ocurren durante la conexión, y que pueden llevar a la finalización brusca de la sesión.

4.1.2. IMPLEMENTACION DEL PROTOCOLO SSL

Por la parte del cliente, SSL viene implementado por defecto en los navegadores Internet Explorer y Netscape Navigator, lo que permite a cualquier usuario con uno de estos navegadores poder realizar compras por Internet de forma segura sin tener que conocer el sistema a fondo ni preocuparse de instalar programas adicionales (por lo menos autenticando al servidor web y con confidencialidad e integridad asegurada en la transacción).

La implementación en la parte servidora (la tienda o banco por lo general) es un poco más compleja. En primer lugar, es obligatoria la obtención de un Certificado Digital para el vendedor o para el servidor seguro, solicitándolo a una Autoridad Certificadora de prestigio reconocido.

Ya con el servidor certificado, el usuario podrá realizar su compra. En el momento del pago, el vendedor obtiene el PIN de la tarjeta de crédito del cliente, la fecha de caducidad y sus datos personales (si el pago se realiza por este método), por lo que deberá disponer de algún sistema que permita el envío de estos datos a una entidad financiera capaz de realizar la transferencia bancaria necesaria para completar el pago.

Existen diferentes entidades bancarias y financieras que ofrecen estos sistemas a los comerciantes, realizándose la comunicación entre comerciante y banco a través de un protocolo seguro privado en la mayoría de los casos, de forma similar a lo que ocurre cuando pagamos en una tienda "real" con nuestra tarjeta de crédito. Estos sistemas se suelen conocer con el nombre genérico de Pasarelas de Pago.

Un sistema de pasarela más avanzado es el denominadoTPV, Terminal de Punto de Venta. En el mismo se conecta una terminal especial al servidor web del vendedor, y mediante un software basado en script CGI se realiza la comunicación segura entre ellos.

Existen en la actualidad diferentes versiones del conjunto de protocolos SSL que se pueden implementar en los distintos servidores y que corren bajo los sistemas operativos más comunes (IIS en Windows NT-2000-XP, Apache en Unix, etc.).

4.1.3. 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 se complica cuando se tiene que seguir las mismas precauciones con cada una de las diferentes claves que los diferentes bancos y servidores seguros 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 las 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 de forma útil 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.

Imaginemos ahora que tras realizar nuestra compra el responsable de la tienda decide cambiar los datos del pedido, y en vez de enviarnos un televisor a $200.000 nos envía 5 a $150.000. ¿Qué podemos haces cuando nos lleguen a casa los televisores y la factura del banco?. Nada, protestar, patalear y llorar, pero nada más, 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 ningún 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 computador por ejemplo, y que cuando nos llega a casa decimos que nosotros no hemos hecho ninguna compra, devolvemos el computador 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. ¿Porqué?.

Tal vez sea porque, a pesar de sus fallos, SSL 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 especiales características.

4.2. OTROS PROTOCOLOS SEGUROS

4.2.1. PROTOCOLO TLS - TRANSPORT LAYER SECURITY

Para intentar corregir las deficiencias observadas en SSL v3 se buscó un nuevo protocolo que permitiera transacciones seguras por Internet, sobre todo teniendo en cuenta que SSL es propiedad de la empresa Netscape. El resultado de esta búsqueda fue el protocolo TLS, que permite una compatibilidad total con SSL siendo un protocolo público.

TLS busca integrar en un esquema tipo SSL al sistema operativo, a nivel de la capa TCP/IP, para que el efecto "túnel" que se implementó con SSL sea realmente transparente a las aplicaciones que se están ejecutando. Parte de las mismas bases que

SSL, pero se diferencia de él en varios aspectos fundamentales:

- En el paso CertificateRequest del protocolo Handshake los clientes sólo contestan con un mensaje si son SSL.
- Las claves de sesión se calculan de forma diferente.
- A la hora de intercambiar las claves, TLS no soporta el algoritmo simétrico Fortezza, que sí es soportado por SSL. Esto es debido a la búsqueda de un código público, ya que Fortezza es de propiedad privada.
- TLS utiliza dos campos más en el MAC que SSL, lo que lo hace más seguro.

A pesar de mejorar SSL y de ser público, TLS no está teniendo la aceptación que se esperaba (por lo menos por ahora).

4.2.2. 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 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.

4.2.3. PROTOCOLO SET

Ya hemos visto cómo SSL adolece de graves defectos a la hora de implementar las cuatro condiciones básicas de una transacción segura. Estas carencias hicieron que diferentes empresas y organismos buscaran un nuevo sistema que permitiera realizar operaciones sensibles por Internet de forma segura, con el objeto de estimular la confianza de los consumidores en el comercio electrónico.

En febrero de 1996 un grupo de empresas del sector financiero, informático y de seguridad (Visa International, MasterCard, Microsoft, Nestcape, IBM, RSA, etc.) anunciaron el desarrollo de una nueva tecnología común destinada a proteger las compras a través de redes abiertas como Internet basadas en el uso de tarjetas de crédito. Esta nueva tecnología se conoce con el nombre de Secure Electronic Transatrions (Transacciones Electrónicas Seguras), SET, y ha sido creada exclusivamente para la realización de comercio electrónico usando tarjetas de crédito.

El protocolo SET ofrece una serie de servicios que convierten las transacciones a través de Internet en un proceso seguro y fiable para todas las partes implicadas:

Autenticación: todas las partes involucradas en la transacción económica (el cliente, el comerciante y los bancos, emisor y adquiriente) pueden verificar mutuamente sus identidades 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 (web spoofing), que imitan grandes web comerciales. Por su parte, los bancos pueden asimismo comprobar la identidad del titular y del comerciante.

Confidencialidad: la información de pago se cifra para que no pueda ser espiada mientras viaja por las redes de comunicaciones. 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 o a qué dirección deben enviarse, debe recurrirse a un protocolo de nivel inferior como SSL.

Integridad: garantiza que la información intercambiada, como el número de tarjeta, no podrá ser alterada de manera accidental o maliciosa durante su transporte a través de redes telemáticas. Para lograrlo se utilizan algoritmos de firma digital, capaces de detectar el cambio de un solo bit.

Intimidad: el banco emisor de la tarjeta de crédito no puede acceder a información sobre los pedidos del titular, por lo que queda incapacitado para elaborar perfiles de hábitos de compra de sus clientes.

Verificación inmediata: proporciona al comerciante una verificación inmediata, antes de completarse la compra, de la disponibilidad de crédito y de la identidad del cliente. De esta forma, el comerciante puede consumar los pedidos sin riesgo de que posteriormente se invalide la transacción.

No repudio: la mayor ventaja de SET frente a otros sistemas seguros es la adición al estándar de certificados digitales (X.509v3), que asocian la identidad del titular y del comerciante con entidades financieras y los sistemas de pago de Visa, MasterCard, etc. Estos certificados previenen fraudes para los que otros sistemas no ofrecen protección, como el repudio de una transacción (negar que uno realizó tal transacción), proporcionando a los compradores y vendedores la misma confianza que las compras convencionales usando las actuales redes de autorización de créditos de las compañías de tarjetas de pago.

Las especificaciones formales del protocolo SET 1.0 se hicieron públicas el 31 de

mayo de 1997, y se pueden encontrar en el sitio web oficial de SETco, http://www.setco.org, organismo encargado de homologar los módulos de programación y los certificados desarrollados por empresas privadas que se usen en implementaciones del protocolo SET.

Como características principales de SET podemos destacar:

- Es un estándar abierto y multiplataforma, en el que se especifican protocolos, formatos de mensaje, certificados, etc., sin limitación alguna respecto al lenguaje de programación, sistema operativo o tipo de máquina usados.
- Su principal objetivo es la transferencia segura de números de tarjetas de crédito.
- Utiliza codificación estándar (ASN.1 y DER).
- Es independiente del medio de comunicación utilizado. Fue diseñado para su uso en Internet, pero permite la conexión a través de cualquier tipo de red siempre que se definan las interfaces adecuadas. Además, el protocolo SET se puede transportar directamente mediante TCP, mediante correo electrónico basado en SMTP o MIME y mediante HTTP en páginas web.
- Utiliza estándares criptográficos reconocidos y ampliamente usados (PKCS, Certificados X.509, etc.).
- El formato de los mensajes usados está basado en el estándar PKCS-7, al igual que SSL y S-MIME.
- Se basa en el uso de la Criptografía de Clave Pública.
- Realiza una Autenticación de todas las partes participantes en la transacción usando certificados digitales.

Vimos que en el proceso SSL sólo intervienen dos entidades: El Comprador y el Vendedor. Pues bien, en una transacción con SET se ven implicadas varias entidades:

- El titular de la tarjeta (Cardholder): posee la tarjeta emitida por el banco emisor y realiza y paga las compras.
- El comerciante (Merchand): vende productos, servicios o información y acepta el pago electrónico. La parte débil en las transacciones electrónicas es el comerciante, a quien corresponde probar que su abono está justificado (a no ser que responda el banco o entidad financiera titular de la tarjeta, todo depende del contrato que tenga con el comerciante).
- El banco emisor (Issuer): emite la tarjeta del cliente, extiende su crédito y es responsable de la facturación, recolección y servicio al consumidor.
- El banco adquiriente (Adquirer): forma relación con el comerciante, procesando las transacciones con tarjeta y las autorizaciones de pago.
- La Pasarela de Pago (Gateway Payment), que permite la comunicación directa a través de Internet entre el comerciante y las Redes Bancarias, con lo que el papel del vendedor queda limitado a un mero intermediario entre el cliente y su banco. Puede ser una entidad independiente o el mismo banco del comerciante.

Además de estas entidades principales existen otras dos relacionadas con ellas:

- La empresa propietaria de la marca de la tarjeta de crédito, como Visa, MasterCard, American Expres, etc., que avalan las tarjetas.
- Autoridades de certificación, que emiten los certificados digitales usados como medio de autenticación de las entidades que intervienen directamente en la operación. Pueden ser entidades independientes autorizadas, bancos o los mismos propietarios de la marca de la tarjeta.

4.2.3.1. PROCESO DE PAGO CON SET

El proceso de pago en una transacción electrónica usando el protocolo SET admite un gran número de opciones diferentes pero, básicamente, consta de los siguientes pasos:

- El cliente, tras seleccionar los artículos a comprar en el sitio web del vendedor, envía a éste un formulario de pedido, siendo respondido por el comerciante con el envío de su certificado digital y el de la pasarela de pago. El cliente comprueba la validez de los certificados y envía entonces al comerciante una orden de pago, que está dividida en dos secciones o documentos diferentes: la Información de pedido (OI), en la que figuran los datos de los productos comprados, su precio y las demás informaciones necesarias para la compra, y la Instrucción de compra (PI), en donde se describen sus datos bancarios y se dan instrucciones para el pago a la entidad vendedora.
- Esta orden de pago se firma digitalmente por medio de un algoritmo especial, denominado Firma Dual, que se realiza concatenando primero los resúmenes hash de los dos documentos generados y encriptando esta concatenación después con su llave privada, para seguidamente encriptar la Firma Dual mediante una clave simétrica generada por su software SET. Por último, se encriptan la clave simétrica generada y el número de la tarjeta de crédito con la llave pública de la pasarela de pago. De esta forma el vendedor no puede conocer los datos bancarios del comprador, y el banco no puede conocer la información sobre los productos comprados, a pesar de que ambos documentos están ligados por la misma firma. En ciertos casos es posible realizar la transacción sin esta firma dual, estableciéndose mediante un protocolo inicial qué método se va a usar.
- El vendedor recibe la orden de compra y la firma dual del cliente, se queda con la descripción de la compra y tras comprobar la autenticidad del comprador, utilizando para ello la firma digital de éste y su certificado, y la integridad de los datos recibidos envía los datos financieros a la Pasarela de Pago encriptados con la clave pública de la misma.
- La Pasarela de Pago comprueba la autenticidad del comprador y la integridad del PI del mismo, y con el mensaje del vendedor comprueba la relación existente entre la descripción de la compra enviada al vendedor y la usada para la firma dual recibida.
- Si todo es correcto, la Pasarela de Pago envía mediante las redes de comunicación bancarias el PI al banco del vendedor y solicita autorización para realizar el pago, mediante un documento denominado Petición de autorización de pago.

- El banco del vendedor comprueba entonces que la tarjeta de crédito es válida y permite el cargo del importe de la compra, enviando entonces un documento a la pasarela, denominado Autorización de pago, que autoriza el proceso de compra.
- Una vez informado el vendedor de la autorización procede al envío de los artículos comprados al cliente, y después de la entrega física del producto pide el importe de la venta a la Pasarela de Pagos, proceso que se conoce con el nombre de Solicitud de pago.
- Entonces la Pasarela de Pagos pide al banco del comprador la transferencia del importe de la venta al banco del vendedor, petición que recibe el nombre de Solicitud de Compensación. Entonces se le hace efectivo al vendedor el importe, con lo que se cierra el proceso total de compra.

Todos los documentos implicados en el proceso anterior deben llevar un número identificador único de transacción, conocido como **ID**.

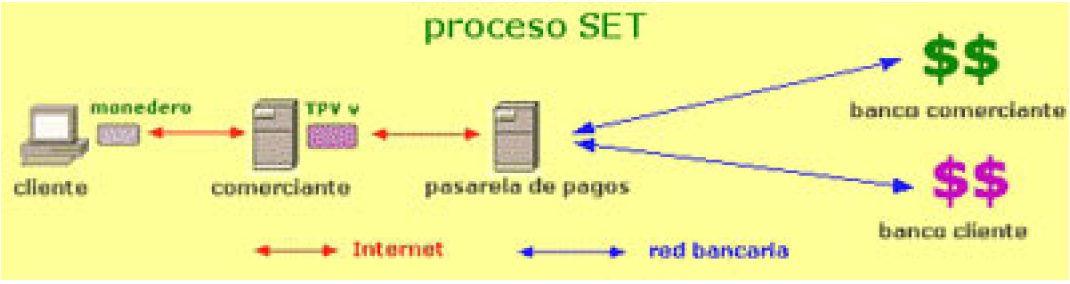


Figura. Proceso de pago mediante el protocolo SET

4.2.3.2. MONEDEROS ELECTRONICOS

Con objeto de facilitar los pagos en transacciones basadas en el protocolo SET se desarrolló una aplicación especial, denominada monedero electrónico, que simula la funcionalidad de una cartera tradicional, y que permite al usuario cliente disponer de un lugar en el que guardar los números de sus tarjetas de crédito y los resguardos de las compras realizadas.

Estos monederos o carteras, conocidos también con el nombra de Wallets, se pueden integrar en la actualidad en cualquiera de los navegadores estándar, y permiten a los usuarios realizar compras por Internet de forma cómoda y segura, usando el protocolo SET. Los datos de las tarjetas de crédito y de la compra se transmiten y se almacenan de forma segura (encriptados con un sistema simétrico), garantizando la autenticidad y la confidencialidad en el proceso de compra de forma totalmente transparente al usuario, que sólo se debe preocupar de elegir los productos que desea adquirir y decir con qué tarjeta de las contenidas en el monedero desea pagarlos.

Los monederos electrónicos poseen un sistema de administración propio que permite al usuario la cómoda gestión de sus tarjetas y de los resguardos de las compras que ha realizado. Además, son programas de poco peso, lo que permite al usuario guardarlos en un disquete y llevarlo consigo para poder operar con ellos en cualquier ordenador, sin que quede constancia luego en el mismo de ninguna de las transacciones realizadas (todo se guarda en el monedero, nada queda en fuera de él). El acceso a los datos de

monedero se encuentra protegido con una contraseña propia de cada usuario, lo que permite que una única cartera pueda tener varios usuarios distintos, cada uno con su clave de acceso, sus propias tarjetas y sus propios resguardos de compra, no pudiendo en ningún momento un usuario acceder a los datos de otro.

Las misiones principales del monedero electrónico son comunicarse automáticamente con la aplicación de venta del comerciante, guardar la información sobre las tarjetas de crédito y las compras realizadas y manejar los certificados usados en la transacción para autentificar a las partes que intervienen en la misma. También se encargan de la recuperación de transacciones perdidas, de forma que si en el proceso de compra se interrumpe la conexión a Internet, posteriormente puede continuar ésta en el punto en que se quedó.

Como utilidad adicional, los monederos permiten la personalización de su interfaz con logotipos y textos propios de cada usuario u organización que desee distribuirlos entre sus clientes.

4.2.3.3. TPVV - TERMINALES PUNTO DE VENTA VIRTUALES

En el comercio tradicional con tarjetas de crédito existe un mecanismo (una aplicación), denominada Terminal Punto de Venta, cuya misión es solicitar la autorización de pago mediante la tarjeta de crédito del cliente. Todos conocemos este sistema, consistente en una pequeña máquina, comunicada con la pasarela de pago por vía telefónica, en la que el vendedor pasa la banda magnética de nuestra tarjeta y recibe la autorización para la venta tras comprobarse la validez de la tarjeta y la disponibilidad de fondos asociados a la misma.

SET proporciona una aplicación parecida, denominada Terminal Punto de Venta Virtual, que funciona de forma transparente al usuario. Cuando éste ordena una compra, generalmente usando su monedero electrónico, en el proceso de pago que se origina el Terminal Punto de Venta Virtual almacena la información de la transacción y establece contacto con el sistema financiero usado, a través de la Pasarela de Pago usada por SET, que será la encargada de autorizar la compra.

Además, el TPV Virtual dispone de una aplicación de administración que permite llevar un control total sobre todas las transacciones que el sistema haya procesado, y mediante la cual es posible:

- Comprobar en todo momento los certificados digitales de que dispone el sistema, así como su gestión.
- Configurar las conexiones con los otros sistemas.
- Controlar en todo momento el estado de las compras.
- Almacenar ficheros logs con los eventos que se producen en el sistema, mediante los cuales el administrador puede localizar rápidamente cualquier anomalía.
- Gestionar batchs, que permiten al comerciante conocer en todo momento las compras ya liquidadas y comprobar si los datos almacenados en su sistema coinciden con los correspondientes de la entidad financiera.

- Generar informes estadísticos basados en diferentes criterios, que permiten tener un control gráfico sobre todos los datos.

4.2.3.4. PASARELAS DE PAGO

Las Pasarelas de Pago en SET son las encargadas de conectar a los comerciantes con las entidades financieras. Reciben peticiones de autorización, liquidación o reconciliación de pagos de los sistemas comerciales TPV Virtuales y las encaminan hacia los sistemas autorizadores de pago tradicionales.

El encaminamiento de peticiones financieras provenientes de SET hacia el sistema autorizador se realiza a través de un módulo dinámico, de forma que resulta posible la conexión de la aplicación con cualquier sistema autorizador existente en el mercado, independientemente del formato o protocolo de comunicaciones usado.

4.2.3.5. VENTAJAS E INCONVENIENTES DE SET

No cabe duda que el sistema SET proporciona buenas cualidades de seguridad, integridad, autenticidad y no rechazo en las transacciones comerciales por redes abiertas basadas en el pago mediante tarjetas de crédito, y que existe un gran empuje por parte de las principales empresas financieras y expendedoras de tarjetas de crédito para estandarizar su uso, pero el caso es que no se ha logrado un desarrollo e implementación masivo del mismo.

Uno de los factores que tal vez hayan influido más en ésta pasividad del mercado respecto a SET es el de la complejidad intrínseca del mismo. Con SSL el usuario no tiene que hacerse con certificado alguno (normalmente), ni tiene que andar instalando en su ordenador software adicional; tan sólo debe seleccionar los productos que desea comprar y aceptar el pago.

Otro factor a tener en cuenta es la relativa lentitud de proceso de SET, al tener que realizarse diferentes verificaciones de identidad e integridad por parte de diversas entidades a lo largo de una transacción.

Sus puntos fuertes son también su talón de Aquiles: la autentificación de todas las partes exige rígidas jerarquías de certificación, ya que tanto clientes como comerciantes deben adquirir certificados distintos para cada tipo de tarjeta de crédito, trámites que resultan engorrosos, para la mayoría de los usuarios. Se añade el problema de la revocación de certificados, la portabilidad de los mismos cuando el usuario trabaja en distintas máquinas y las cadenas de certificación. En definitiva, SET descansa sobre una infraestructura de clave pública (PKI) que en la actualidad dista mucho de ser perfecta.

SET seguirá coexistiendo con SSL durante mucho tiempo, hasta que se alcance una masa crítica de usuarios que propicien su utilización a gran escala, o caiga en el olvido superado por otra nueva iniciativa más ágil y mejor adaptada. Las opiniones de los analistas se encuentran divididas acerca de su futuro. En lo que todos coinciden es que aún le queda un largo camino por recorrer.

4.2.3.6. CERTIFICACIONES

El protocolo SET es constituye el primer proyecto de certificación a escala global que se va a realizar. Los certificados SET se estructuran siguiendo una jerarquía piramidal única, cuya cúspide la ocupa la Autoridad Certificadora Raíz (Root CA), que es la encargada de certificar a todas las demás autoridades certificadoras.

Bajo la Autoridad Certificadora Raíz se encuentran las Brand CA, o Autoridades de Certificación de Marca, propiedad de las entidades emisoras de tarjetas de crédito, entre las que destacan las pertenecientes a Visa International y MasterCard International, propulsoras del protocolo SET. Estas entidades son certificadas por la Autoridad Certificadora Raíz. Por lo tanto, cuando una Brand CA desea obtener un certificado SET debe realizar una petición a la Root CA, en un archivo de formato estándar, el PKCS#107. Si dicha solicitud es aprobada se genera otro archivo de respuesta, denominado PKCS#7, que es remitido a la CA solicitante.

Las Autoridades de Certificación de marca se encargan principalmente de emitir certificados SET a Autoridades de Certificación Geopolítica. También son responsables de la generación de los archivos BCI de certificados revocados, recopilando para ello las CRL de las CA por debajo de ellas. Una vez confeccionados estos archivos son enviados a las Geopolitical CA, que son las encargadas de su distribución.

Las Brand CA pueden autorizar a su vez a otras entidades, denominadas Geopolitical CA o Autoridades de Certificación Final, para que funcionen como autoridades certificadoras. Las Autoridades de Certificación Final se encargan de emitir los certificados SET a los usuarios finales del sistema, clientes, vendedores y pasarelas de pago.

A la hora de obtener un certificado SET se requiere un proceso de autentificación de los datos que en él van a figurar, al igual que sucede con los certificados X.509 v3. En el caso de SET la verificación de datos corresponde a unas entidades creadas al efecto, que se denominan Autoridades de Registro.

Su labor es la actuar como avaladores ante la CA de los usuarios que solicitan el certificado, encargándose también de tramitar los mismos. Las entidades destinadas a asumir el papel de Autoridades de Registro son los propios bancos, permitiendo con ello que los certificados estén asociados a cuentas bancarias y no a personas físicas, con lo que hace posible la compra anónima por Internet, al no aparecer en ningún momento el nombre del cliente que va a efectuar el pedido.

Las Autoridades de Registro actúan en nombre y por cuenta de la Autoridad de Certificación correspondiente, y deben superar un proceso de homologación antes para garantizar su fiabilidad. Sus principales misiones son validar solicitudes de certificado en base a determinados procedimientos de identificación según el tipo de certificado, solicitar luego el correspondiente certificado a la Autoridad Certificadora y entregar el mismo, una vez obtenido, al usuario final del mismo, usando para ello un disquete u otro soporte adecuado.

Toda Autoridad de Registro debe tener a disposición de los solicitantes un documento, denominado Prácticas de Registro, que especifique claramente los procedimientos operativos y de garantía de seguridad que exige y facilita.

Este sistema jerárquico y modular de las Autoridades de Certificación proporciona una gran flexibilidad a SET para adaptarse a todo tipo de necesidades, desde la pequeña empresa que tan sólo desea certificar a sus compradores hasta la gran empresa que quiere ofrecer a sus clientes una solución SET completa.

4.2.3.7. APLICACIONES DE SET

Dentro del nivel organizacional el comercio electrónico juega un papel muy importante dentro de la reingeniería de procesos de negocios, es una manera natural de automatizar los procesos entre departamentos o divisiones de una organización. Es aplicable a estrategias del Marketing Directo, a video conferencias, cursos y seminarios virtuales, y con la aparición del EDI, alcanza una magnitud insospechada, abarcando temas legales, contables, financieros, de seguros, incluso en las actividades del sector gubernamental; constituye el eje sobre el cual gira el comercio internacional y su registro en las cuentas del Estado, como Banco Central, Ministerio de Finanzas o Hacienda, de Comercio Exterior, Aduanas, etc.

4.3. SERVIDORES SEGUROS

Se entiende por Servidor Seguro un servidor de páginas web que establece una conexión cifrada con el cliente que ha solicitado la conexión, de manera que nadie, salvo el servidor y el cliente, puedan tener acceso a la información transmitida de forma útil.

El uso de servidores seguros es un elemento imprescindible en todos aquellos servicios que utilicen información confidencial, como operaciones bancarias on-line, compras por Internet, acceso a servidores de datos sensibles, etc.

Para conseguir la confidencialidad e integridad de datos perseguida los servidores seguros se basan en el uso de sistemas criptográficos mixtos, que combinan la Criptografía de clave pública con la de clave simétrica. Para garantizar al usuario su autenticidad, los servidores seguros hacen uso de los certificados digitales ya estudiados.

Cuando accedemos a un servidos seguro normalmente nos aparece una ventana indicándonos que vamos a iniciar una conexión segura, y el candado situado en la parte inferior de la ventana del navegador aparecerá cerrado cuando entremos a la página segura (Atención: la presencia del candado cerrado no garantiza una comunicación segura; hace falta comprobar el certificado del servidor). Además, si miramos en la barra de direcciones veremos que ahora estamos usando el protocolo HTTPS, que corresponde al protocolo HTTP con privacidad.

Podemos acudir al menú “Archivo” – “Propiedades” para obtener información más detallada sobre el documento seguro, entre la que destaca:

- Protocolo: HTTP Seguro (con privacidad).
- Conexiones: Protocolo Secure Socket Layer versión 3.0, algoritmo simétrico de cifrado RC4 con longitud de claves de 128 bits, algoritmo de cifrado de clave pública RSA de 1024 bits de longitud de clave.
- URL del servidor seguro.

También podemos acceder desde una página segura al certificado digital del servidor de forma rápida. Para ello basta hacer seleccionar el botón "Certificados" de la ventana anterior o hacer doble click sobre el candado cerrado.

Otro aspecto importante a considerar son los fallos a la hora de implementar los protocolos criptográficos, sobre todo en lo que respecta a la configuración propia del servidor web seguro y a los fallos de implementación que de los protocolos hacen los navegadores cliente. Uno de estos fallos es la relativa falta de seguridad de los números pseudoaleatorios generados para el proceso de creación de claves durante la fase

Handshake.

A pesar de todas estas consideraciones no hay que ser alarmista en cuanto al uso de los servidores y protocolos seguros, ya que generalmente el tiempo de duración de la conexión segura es lo suficientemente pequeño como para resultar imposible, con los medios actuales, descifrar las claves en un tiempo útil. Y a esto hay que añadir las innumerables ventajas que obtenemos de este tipo de aplicaciones, que permiten realizar transacciones seguras por Internet.

Para minimizar los riesgos posibles, a la hora de implementar o aceptar un servicio de servidor seguro podemos exigir que se cumplan una serie de condiciones, entre las que podemos destacar:

- Que el certificado de servidor seguro se corresponda con los de máximas garantías de verificación y que haya sido expedido por una Autoridad Certificadora de toda confianza.
- Que el navegador usado en la comunicación tenga implementada la última versión de SSL, es decir, el protocolo SSL 3.0. Versiones anteriores son válidas, pero no recomendadas.
- El uso de un sistema de cifrado simétrico robusto (RC4 RC5 o similar) con longitudes de clave largas (de entre 64 y 128 bits).

4.4. EDI - INTERCAMBIO ELECTRONICO DE DATOS

4.4.1. DEFINICIONES

Es un conjunto coherente de datos, estructurados conforme a normas de mensajes acordadas, para la transmisión por medios electrónicos, preparados en un formato capaz de ser leído por el computador y de ser procesado automáticamente y sin ambigüedad.

Es aquella parte de un sistema de información capaz de cooperar con otros sistemas de información mediante el intercambio de mensajes EDI.

4.4.2. ¿QUE FUNCIONALIDAD OFRECE EL EDI?

Intercambio electrónico de datos es el intercambio entre sistemas de información, por medios electrónicos, de datos estructurados de acuerdo con normas de mensajes acordadas. A través del EDI, las partes involucradas cooperan sobre la base de un entendimiento claro y predefinido acerca de un negocio común, que se lleva a cabo mediante la transmisión de datos electrónicos estructurados.

En el EDI, las interacciones entre las partes tienen lugar por medio de aplicaciones informáticas que actúan a modo de interfaz con los datos locales y pueden intercambiar

información comercial estructurada. El EDI establece cómo se estructuran, para su posterior transmisión, los datos de los documentos electrónicos y define el significado comercial de cada elemento de datos. Para transmitir la información necesita un servicio de transporte adicional (por ejemplo, un sistema de tratamiento de mensajes o de transferencia de ficheros).

Debe destacarse que el EDI respeta la autonomía de las partes involucradas, no impone restricción alguna en el procesamiento interno de la información intercambiada o en los mecanismos de transmisión.

4.4.3. PRINCIPALES CAMPOS DE APLICACION

Los típicos campos de aplicación del EDI son el intercambio de información industrial, comercial, financiera, médica, administrativa, fabril o cualquier otro tipo similar de información estructurada. Esta información, con independencia de su tipo concreto, se estructura en unos formatos que pueden ser procesados por las aplicaciones informáticas. Ejemplos de datos EDI son las facturas, órdenes de compra, declaraciones de aduanas, etc.

La automatización de las interacciones por medio del EDI minimiza las transacciones sobre papel y la intervención humana, reduciéndose las tareas relativas a la reintroducción de datos, impresión, envío de documentos vía correo o vía fax. A través del EDI, las Administraciones Públicas pueden incrementar la eficiencia de las operaciones diarias y mejorar las relaciones con agentes externos como empresas, instituciones económicas y financieras, y otras Administraciones Públicas.

El universo de clientes potenciales del servicio EDI es muy amplio, debido a que ésta dirigido a empresas que se relacionan comercialmente, en forma independiente de su tamaño.

Como ejemplo de grupos de potenciales clientes, podemos mencionar:

- Sector de la Distribución (Supermercados y Proveedores)
- Sector de las Automotrices (Terminales, Proveedores y Concesionarios)
- Sector Farmacéutico (Farmacias y Laboratorios)
- Sector de la Administración Pública
- Sector del Transporte y Turismo

4.4.4. NORMAS DE SINTAXIS

Básicamente, las normas EDI proporcionan las reglas de sintaxis que definen los documentos electrónicos estructurados (llamados mensajes EDI) y un número cada vez mayor de mensajes EDI acordados internacionalmente.

El módulo ephos sobre EDI se basa en las normas y documentos desarrollados por las Naciones Unidas y recogidos en "ISO 9735 - Intercambio Electrónico de Datos para la

Administración, Comercio y Transporte (EDIFACT) - Reglas de aplicación de la sintaxis". Si bien por razones históricas, en diferentes dominios regionales o sectoriales se utilizan otras reglas de sintaxis (no normalizadas), EDIFACT es la única sintaxis normalizada.

4.4.5. PLANIFICACION DE SISTEMAS DE INFORMACION EN LA EMPRESA

Hoy en día, el sistema informativo contable de cualquier empresa, por pequeña que sea, se encuentra informatizado, de forma que habitualmente se logran unos elevados niveles de automatización de las tareas administrativo-contables. Por ejemplo, es frecuente que se encuentren integrados los programas de contabilidad con los que gestionan la tesorería o la nómina y que estos datos se procesen muy rápidamente.

Pero suele suceder que dos empresas que mantienen una intensa relación comercial cliente-proveedor y que disponen de sendos sistemas informativos contables avanzados, realicen sus transacciones económicas introduciendo las órdenes de compra, las facturas y el resto de documentos en sobres, que posteriormente son enviados por correo. Hoy en día, también es habitual enviar estos documentos a través del fax, con lo que se agiliza la gestión. Si la empresa utiliza un fax-modem conectado al computador y gestionado por un programa informático, se evita tener que imprimir los documentos, enviándolos directamente desde su computador hasta el fax de la otra empresa.

Otra solución más sofisticada, pero menos frecuente, consiste en enviar dichos documentos a través del correo electrónico. El correo electrónico permite enviar mensajes entre diferentes computadores que estén conectados a Internet. Sin embargo, este procedimiento no está exento de inconvenientes, debido a que el correo electrónico no está normalizado y, salvo que el cliente y el proveedor acuerden previamente componer de alguna forma sus mensajes, exige que el receptor traduzca los documentos recibidos. Además, el uso de mero correo electrónico no es un medio seguro para realizar las transmisiones comerciales ni garantiza su confidencialidad.

La solución que desde hace varios años están adoptando muchas empresas se denomina EDI o Intercambio Electrónico de Datos. El EDI básicamente consiste en transmitir electrónicamente documentos comerciales y administrativos entre aplicaciones informáticas, en un formato normalizado. En este trabajo describimos qué es el EDI, qué diferentes normas EDI existen, por dónde viajan los datos, cual es la estructura de un mensaje EDI, los beneficios y los costos que para una empresa puede suponer el implantar este sistema y el impacto que puede tener sobre la contabilidad.

4.4.6. TRANSMISION DE DOCUMENTOS ENTRE EMPRESAS

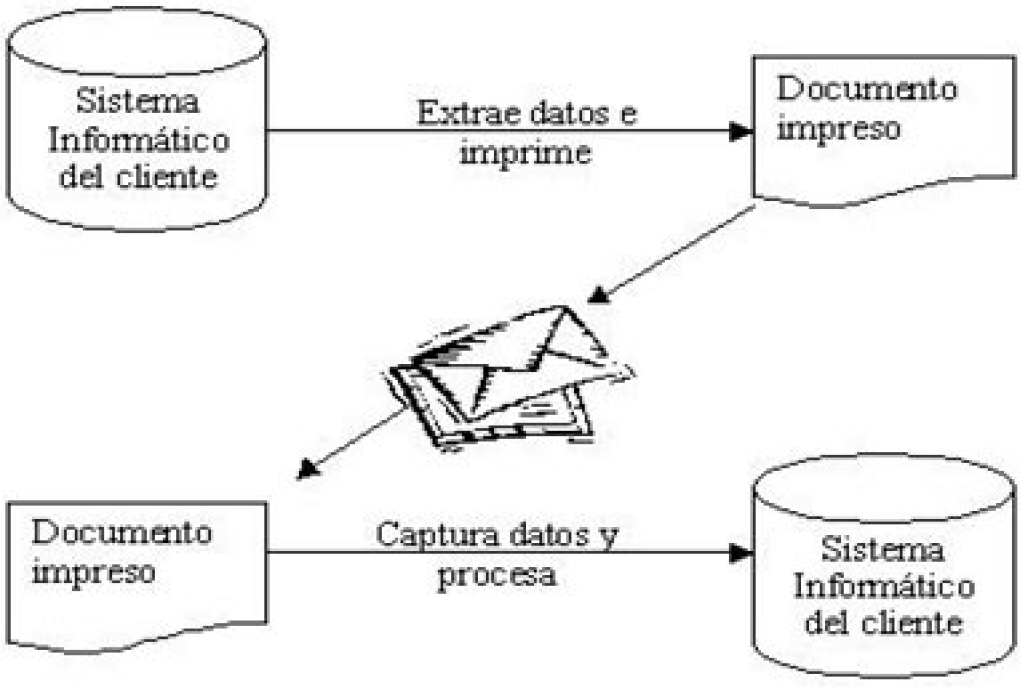
El sistema tradicional en el que se basan las transmisiones de documentos entre las empresas, al estar centrado en el uso del papel, presenta dos inconvenientes. En primer lugar, la lentitud. Documentos que se generan en computadores que procesan la información a gran velocidad, posteriormente sufren retrasos producidos al tener que procesarse de forma manual en las empresas de correos. Por este motivo, muchas

empresas han sustituido el correo como medio para enviar sus documentos por el fax, lo que ha agilizado en buena medida la gestión. Sin embargo, se mantiene otro problema: la diversidad de modelos de facturas, pedidos, cotizaciones, etc. Esta falta de normalización es causa de muchos errores administrativos y, de nuevo, de lentitud.

4.4.7. PROCEDIMIENTO CONVENCIONAL DE TRANSMISION DE DOCUMENTOS ENTRE LAS EMPRESAS

La primera empresa extrae la información necesaria de la base de datos del sistema informático contable e imprime los documentos necesarios. Estos documentos se envían por correo a la otra empresa, quien debe introducir de nuevo los datos en su sistema informático. Por lo tanto, en el procedimiento tradicional frecuentemente se producen redundancias ya que los documentos que se imprimen en una empresa son introducidos anualmente por sus empleados en el sistema informático de la otra.

La introducción del EDI consiste simplemente en incorporar un procedimiento electrónico de transmisión de información al documento administrativo-contable. La empresa puede obtener ahorro de varias formas tras implantar un sistema electrónico de intercambio de datos. En primer lugar, aparece un ahorro de tiempo, ya que la información viaja por redes de comunicación. En segundo lugar, se producen menos errores, ya que el proceso está completamente automatizado y los computadores se equivocan menos. Además puede haber un importante ahorro en dinero, dependiendo de lo que cueste enviar estos documentos.



4.4.8. SERVICIOS EDI

Como ya mencionamos anteriormente EDI es el intercambio electrónico de documentos estandarizados, a través de redes de telecomunicaciones, entre aplicaciones informáticas de empresas relacionadas comercialmente. El EDI sustituye el soporte papel de los relacionadas comercialmente. El EDI sustituye el soporte papel de los documentos comerciales más habituales (órdenes de compra, remito, factura, lista de precios, etc.) por transacciones electrónicas con formato normalizados y acordados previamente entre los usuarios del servicio.

Este servicio, a diferencia del correo electrónico, relaciona aplicaciones informáticas que residen en las computadoras de las distintas empresas. Por lo tanto, el intercambio de información se realiza entre aplicaciones informáticas y no entre personas.

4.4.9. PRINCIPALES BENEFICIOS

EDI sin duda nos ofrece una amplia gama de oportunidades de trabajo y beneficios para la empresa entre los que se destacan:

- Agilización de procesos comerciales
- Importante disminución de errores en los documentos
- Disminución de stocks, debido a la facilidad de aplicación de técnicas "Just-in-Time"
- Ahorro de costos de administración
- Mejora de la competitividad de la empresa que lo adopta

En el comercio exterior particularmente, se simplifican muchos procedimientos administrativos, aduaneros, bancarios, de contratación internacional, etc. La aplicación del EDI en su empresa incrementa la productividad.

4.4.10. ¿CUANDO USAR EL EDI?

Generalmente, se utiliza el EDI cuando:

- Las partes involucradas en el intercambio son autónomas y comparten un entendimiento predefinido, claro y común sobre los negocios y servicios a utilizar;
- La información a intercambiar puede mapearse sobre mensajes normalizados.

Debe destacarse que aunque no se disponga de mensajes normalizados para todas las aplicaciones, ello no debe impedir la utilización del EDI.

Un uso típico del EDI es la automatización de los intercambios entre un departamento y una organización externa (por ejemplo, una compañía suministradora) o entre dos grandes departamentos de la misma administración, cada uno de ellos dotado con su propio sistema de información y diferentes formas de representar la misma información. No obstante, dentro de un mismo departamento pueden existir unidades que tienen sus propios dominios de aplicación implementados sobre diferentes sistemas informáticos, y necesitan automatizar el intercambio de datos mediante el EDI.

La existencia de conjuntos de mensajes acordados internacionalmente es el elemento clave para la automatización de los procedimientos administrativos o comerciales. El número actual de mensajes normalizados o en fase de borrador, abarca una extensa área de aplicaciones relevantes para las Administraciones Públicas.

La introducción del EDI debería decidirse teniendo en cuenta los siguientes aspectos:

- El volumen de documentos comerciales / administrativos intercambiados.
- El actual porcentaje de error en el tratamiento de documentos sobre papel.
- El costo del tratamiento y mantenimiento de documentos sobre papel.
- El factor tiempo (si es crítico o no).
- El valor estratégico asignado al EDI en términos de beneficios a largo plazo.

Este análisis debería compararse con la evaluación del costo necesario para implementar una solución basada en el EDI. A los costos de contratación previstos deberían añadirse los costos derivados de procedimientos internos (por ejemplo, preparación del personal).

4.4.11. ¿QUE PUEDE SER INTERCAMBIADO VIA EDI?

Permite la transferencia de una gama de información como:

COMPRAS

- Ordenes de compra
- Acuse de recibo, cambios y ajustes de las órdenes de compra
- Consultas y reportes sobre el estado de las órdenes de compra

FINANZAS Y CONTABILIDAD

- Facturas
- Memos de crédito y débito
- Pagos y notificaciones
- Recibos de pagos
- Notificaciones de aceptación
- Rechazo de pagos
- Reporte de impuestos

CONTROL DE INVENTARIOS

- Ajustes de inventarios
- Planificación de producción
- Transferencia de productos y reventas
- Notificaciones del Nivel de Inventario

CAPITULO 5: “EL COMERCIO ELECTRONICO CHILENO”

5.1. ACTUALIDAD

Chile se está acercando a los niveles B2B de los países desarrollados, pues el 27% de las empresas locales participan activamente en ventas online, frente al 11% de hace un año. La tasa en los países desarrollados fluctúa entre un 30% y un 45% y no ha sufrido variación en el último año.

En el primer trimestre, Chilecompra manejó adquisiciones por US$62mn, en comparación con los US$18mn del primer trimestre del 2003.

Los grandes proveedores se llevaron la mayor parte de las ventas totales al Estado, pero dentro de la comunidad de Chilecompra existe una difusión mucho mayor: un 18% de las licitaciones se adjudicó a microempresas; un 17%, a pequeñas empresas; un 26%, a medianos proveedores; y un 39%, a grandes empresas. Sin embargo, de los 64.000 proveedores registrados de Chilecompra, un 98% corresponde a micro, pequeñas y medianas empresas. Los proveedores registrados en el sitio representan un 21% de todas las firmas chilenas.

El gasto gubernamental en el 2003 totalizó unos US$2.400mn y las licitaciones que

manejó Chilecompra dieron cuenta de US$1.310mn, es decir, la mitad del gasto estatal. El sitio debiera finalizar el 2004 con transacciones totales por US$2.200mn.

Para las licitaciones que se ofrecen a través del portal, los cálculos preliminares sugieren que el gobierno ahorró un 7% en gastos probables, en comparación con los gastos en los mismos productos y servicios antes de que el portal estuviera activo. Esto implica un ahorro de US$90mn, es decir, tres veces el ahorro que Chilecompra proyectó para el 2004 cuando anunció su plan estratégico en el 2002.

Chilecompra apunta a incorporar gobiernos municipales hacia fines de junio y como resultado prevé un crecimiento de 50% en el valor de las transacciones totales durante el segundo semestre del 2004, ya que los municipios tienen un presupuesto anual combinado de alrededor de US$450mn.

Con los municipios, el sitio prestaría servicios a aproximadamente 1.200 instituciones, duplicando las actuales 600. Además, la cantidad de licitaciones podría aumentar a 300.000 al año, en comparación con las 108.000 del 2003.

Después de los municipios, el sitio incorporará a las fuerzas armadas y cubrirá el 100% de las instituciones estatales hacia mediados del 2005, frente al 87% actual.

En febrero, el gobierno lanzó una versión actualizada del sitio, que fue modificado para permitir que todo el ciclo de compra se realizara online. En marzo, el 100% de las subastas se realizó online, en comparación con el promedio de 34% del 2003.

La actualización también preparó el sistema para el uso de facturas y cuentas digitales y se espera que Chilecompra sea un factor clave para convencer a los proveedores de que adopten la tecnología. La prensa local informó recientemente que existen 40 empresas que usan facturas digitales y se prevé que una importante cantidad de proveedores registrados de Chilecompra adoptará la tecnología en segundo semestre.

5.2. CERTIFICACION

El modelo de Certificación Electrónica en Chile define a la Subsecretaría de Economía como el órgano rector que actúa como Entidad Acreditadora. A continuación se encuentran los Prestadores de servicios de certificación, quienes darán los servicios de certificación de firmas electrónicas acreditados ante la autoridad, que dará fe sobre los datos referidos a una firma electrónica y en definitiva otorgará la llamada firma electrónica avanzada.

Las personas que quieran obtener un certificado tendrán que pagar una tarifa definida por la propia empresa certificadora, la cual le dará derecho a las tarjetas por medio de las cuales se realiza el proceso electrónico de certificación. Estas serán leídas por medio de dispositivos que ya están disponibles en el comercio. A futuro se podrán utilizar también las huellas digitales o la lectura electrónica de iris.

Los precios de los diferentes certificados en el mercado local se rigen de acuerdo a las tarifas internacionales, variando entre los US$ 30 y US$ 300, según el tipo de

certificado emitido, ya que también se pueden emitir para validar, por ejemplo, la confiabilidad de un sitio Web, en aquellos casos donde se deban realizar transacciones en línea. La duración de los certificados es, por lo general, de un año.

Actualmente, se identifican 6 modalidades de uso frecuente para certificados digitales:

- Identificación de personas para controlar los accesos a sitios web restringidos o a determinados servicios en línea. En este caso puede ser una comunidad cerrada en la cual una empresa permite a determinadas personas acceder al sitio web para manejar información restringida. Ese acceso se puede definir y asegurar a través del certificado digital.
- Transacciones electrónicas. Ejemplo de ello puede ser cuando los bancos solicitan a cada cuenta cuentacorrentista su identificación, cada vez que se genera una interacción del cliente con el sitio del banco, para efectuar movimientos en su cuenta corriente. Si el cliente tiene certificado digital y el sitio del banco también está certificado, la transacción se produce en un ambiente absolutamente seguro.
- Trámites fiscales. En la Operación Renta, los contribuyentes pueden hacer su declaración de impuestos vía Internet autentificándose frente al sitio del Servicio de Impuestos Internos con certificados digitales. De este modo, se genera un entorno seguro para la transmisión de la información.
- Intercambio de correo o e-mail seguro. Una de las actividades masivas que actualmente ocurren en la comunicación de personas y empresas es el uso del e-mail. En este canal, susceptible a intrusiones, el uso de certificado digital permite firmar el correo, identificando a quien emite y a quien se dirige la comunicación, y también encriptar el contenido, haciéndolo extraordinariamente difícil de "hackear".
- La firma digital en documentos electrónicos, permite signar electrónicamente un Contrato, Orden de Compra u otro documento. A la luz de la Ley de Firma Digital, dichos actos celebrados por personas naturales o jurídicas, públicas o privadas, serán válidos y producirán los mismos efectos que los celebrados por escrito y en soporte de papel.
- La Seguridad en Servidores Web permite a quien contacte un sitio certificado, tener la certeza de que se trata de ese sitio y no una suplantación, permitiendo realizar transacciones en forma segura.

5.2.1. EMPRESAS DE CERTIFICACION

Se trata de entidades que serán acreditadas por el Ministerio de Economía, de las cuales es posible mencionar a E-Cert y Acepta.com, aprobadas por el SII como empresas prestadoras de Servicios de Certificación en el ámbito tributario.

5.2.1.1. ACEPTA.COM

Empresa cuya misión es proveer de las herramientas necesarias para que personas y

empresas puedan utilizar la red con confianza en la era digital. Acepta.com en una empresa dedicada a fortalecer los mecanismos de prevención de fraudes en la red, lo que permite minimizar las necesidades de represión.

Acepta.com es a su vez acreditada mediante auditorías externas, como es la acreditación obtenida con el Servicio de Impuestos Internos para emitir certificados reconocidos en el ámbito tributario.

5.2.1.1.1. TIPOS DE CERTIFICACION

CERTIFICADO DE FIRMA

Con un certificado de firma electrónica se puede enviar documentos electrónicos firmados y recibir información de manera confidencial. Además, permite acreditar identidad ante cualquier otra persona o sitio Web en Internet. Esto permite dejar atrás el viejo, incómodo e inseguro método del Rut y contraseña logrando mayor seguridad, tranquilidad y confianza.

CERTIFICADO SITIO WEB

Con los certificados digitales de Sitio Web se puede realizar transacciones comerciales con plena confianza, puesto que tanto la empresa como los clientes estarán seguros de efectuar transacciones con la persona o empresa con quien realmente desean interactuar y no con un impostor.

TOKEN USB

Refuerza la seguridad que brindan los certificados de firma electrónica incrementando su facilidad de uso y traslado. Con el token USB se puede elevar aún más el nivel de confianza y seguridad, ya sea en transacciones de comercio electrónico o autenticación segura en sitios Web entre otros beneficios.

ValID

Acepta.ValID es un sistema para sitios Web, que permite extraer fácilmente el Run de los usuarios que se autentifican en el sitio con certificados de firma electrónica. Además, valida la vigencia del certificado, consultando automáticamente a la autoridad certificadora correspondiente, y permite resguardar la información de vigencia de manera segura.

SECURINTEGRATOR

SecurIntegrator es un servicio de evaluación de vulnerabilidades para sitios Web. Entrega un completo informe sobre las vulnerabilidades encontradas, junto con las recomendaciones a seguir para solucionarlas. Esto le permite a cualquier empresa brindar servicios en Internet de una manera segura y confiable.

CARPETA WEB

La misma carpeta en la casa y oficina, con esto ya no se necesita enviar los archivos por e-mail. Con el certificado de firma electrónica, se puede acceder a los documentos desde cualquier computador a través de Internet, de una manera completamente segura. Se puede almacenar y administrar remotamente los documentos en una "carpeta web",

de igual forma como si fuera una carpeta más de un disco duro.

5.2.1.2. E-CERT CHILE

La Empresa Nacional de Certificación Electrónica, e-certchile, fue creada por la Cámara de Comercio de Santiago (CCS) con el apoyo de la Asociación Chilena de Empresas de Tecnologías de la Información (ACTI) y CORFO.

El objetivo de e-certchile es otorgar la seguridad indispensable para la realización de negocios por vía electrónica, a través de la emisión de Certificados Digitales, que pueden considerarse el equivalente a la cédula de identidad. De este modo, personas y empresas pueden comprobar su identidad en Internet.

La Misión de e-certchile es posibilitar que personas, empresas y entidades gubernamentales puedan realizar transacciones electrónicas en forma segura y confiable a través de Internet.

E-certchile registra y garantiza la identidad de las partes que negocian sin conocerse vía Internet, la integridad de los contenidos de sus envíos, así como también la aceptación de los compromisos adquiridos en un ambiente de confidencialidad. De esta forma, se elimina el temor de personas y empresas a que su información o medios de pago sean interceptados o mal utilizados.

E-certchile cumple dos roles fundamentales: ser una Autoridad de Certificación, emitiendo y administrando certificados digitales; y ser una Entidad de Registro, validando las solicitudes de certificados.

5.2.1.2.1. TIPOS DE CERTIFICACION

CERTIFICADO PARA FIRMA DIGITAL AVANZADA

El certificado de Firma Digital Avanzada es el equivalente electrónico de la cédula de identidad y permite firmar documentos con validez legal.

Este certificado provee alta seguridad por la obligatoriedad de presentar los antecedentes de identificación personalmente ante la Entidad de Registro.

SERVIDOR SEGURO

E-certchile ofrece certificados para Servidor Seguro de máxima seguridad (128 bit SSL). Los certificados de Servidor Seguro e-certchile, permiten confirmar que la dirección URL pertenece a una determinada entidad comercial, como también permiten entablar comunicaciones seguras con clientes y proveedores, utilizando la tecnología SSL (Secure Sockets Layer), el estándar para las comunicaciones seguras en la Web.

Opcionalmente, el certificado digital para Servidor Seguro, permite controlar el acceso a un segmento privado del sitio Web.

E-MAIL SEGURO

El certificado e-mail seguro de e-certchile, sirve como un sustituto a una carta certificada o a la firma, cuando se envía mensajes a través de Internet. Por el sólo hecho de firmar digitalmente y encriptar los e-mail, se asegura que los mensajes confidenciales

y adjuntos estarán protegidos de posibles delitos de espionaje, alteraciones del contenido y suplantación de identidad.

RUT DIGITAL

El certificado de Rut Digital es el equivalente electrónico de la cédula de identidad y permite autentificarse en Internet.

Este certificado contiene información que identifica y permite:

- Firmar digitalmente documentos, de modo que el destinatario sabe de quien proviene el archivo.
- Encriptar (cifrar) el mensaje usando la llave pública del destinatario (la que se puede obtener en el directorio de la entidad certificadora)
- Adicionalmente, permite identificarse ante sitios Web que implementan control de acceso.

Este certificado provee alta seguridad por la obligatoriedad de presentar los antecedentes de identificación personalmente ante la Entidad de Registro.

CONTROL DE ACCESO

Este certificado permite la autenticación del propietario. Está pensado para entidades con necesidad de controlar los accesos de clientes a los diferentes servicios en línea.

DISPOSITIVOS PORTABLES SEGUROS

Para mayor seguridad el Certificado Digital puede residir en un Dispositivo Portable Seguro, ya sea en E-Token el cual se conecta directo a cualquier puerto USB o una tarjeta inteligente (Smart Card). Para esta opción se necesita disponer de un dispositivo periférico llamado Lectograbador el cual se conecta al computador, permitiendo detectar y leer el certificado contenido en el chip de la tarjeta. Se puede adquirir estos productos para certificados de Firma Digital Avanzada.

E-TOKEN

E-Token puede generar y guardar las credenciales personales de los usuarios, como claves privadas, contraseñas y certificados digitales, dentro del propio chip (como el de las tarjetas inteligentes). Las claves privadas de los usuarios nunca salen del eToken.

- Diseño USB portátil: no necesita ningún lector especial.
- Anti-rechazo mediante la tecnología avanzada de firma digital PKI: los datos se firman en la tarjeta inteligente alojada dentro del eToken, lejos del entorno inseguro del PC.
- Autenticación de dos factores: requiere el eToken físicamente, junto con la contraseña del eToken.
- Interfase USB estándar. Compatible en SO. Windows 98 o superior.

CONCLUSION

Como conclusión de este trabajo podemos decir que debido a la creciente incorporación de Internet en nuestra vida cotidiana, el comercio electrónico será un importante protagonista de la economía en los siguientes años.

En sus comienzos, el comercio electrónico tuvo muchas falencias que no le permitían otorgar un servicio seguro, cuestionándose su operabilidad. Pero con el transcurso del tiempo se ha convertido en un componente más de la economía mundial debido a sus grandes ventajas respecto del comercio tradicional, que han sido enumeradas en este trabajo.

La seguridad en las transacciones es un aspecto al que se le ha dado gran importancia debido a que es la principal preocupación de los potenciales clientes en Internet, se han asignado muchos recursos a combatir los fraudes electrónicos, la suplantación de identidad, la intercepción de mensajes confidenciales, el mal uso de datos personales, entre otros. En este trabajo quisimos mostrar el resultado de ese esfuerzo, explicando cada uno de los componentes que han hecho del comercio electrónico una actividad que cada día tiene más adherentes.

Por esto, hoy podemos decir que el aumento en el uso de este nuevo medio de compra ya no debería estar limitado por la falta de seguridad, sino que por la falta de un cambio en la mentalidad de la mayoría de los usuarios de la red, que aún siguen viendo con desconfianza cualquier transacción electrónica.

Si bien, la red pública es un medio que no ofrece medidas estrictas de seguridad, lo

que es el motivo principal de la falta de confianza de los usuarios, de aplicarse todos los elementos que se mencionaron en este trabajo para realizar transacciones seguras, el comercio electrónico podrá desarrollarse en un medio totalmente seguro.

GLOSARIO

Algoritmos: Conjunto de instrucciones que especifican la secuencia de operaciones a realizar, en orden, para resolver un sistema especifico o clase de problema. Suelen expresarse a través de letras, cifras y símbolos, que forman un algoritmo determinado.

Autentificación: Proceso mediante el cual un usuario comunica sus datos a un sistema a efectos de que este lo reconozca y le permita interactuar con él. En Internet en función del grado de confidencialidad de los datos que se manejan la autentificación puede ser más o menos sencilla. Desde el login y la contraseña, hasta el uso de palabras claves pasando por el valor aleatorio de una tarjeta de códigos de la que se dispone offline.

Autoridades de certificación: Son las encargadas de autentificar la identidad a los participantes de una transacción. Existen diferentes niveles de certificación según las necesidades de cada tipo de transacción, desde las más básicas hasta las más exhaustivas, las de “clase 3” que son las utilizadas para el comercio electrónico.

Banca electrónica: Es la conexión electrónica entre una empresa y sus bancos. La banca electrónica es la respuesta a la búsqueda de una mayor eficacia en las relaciones financieras. Su objetivo es llegar a sustituir al papel en pro de un sistema totalmente automático y electrónico.

Base de datos: Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de

aplicaciones de productividad personal más extendidos. Entre las más conocidas pueden citarse dBase, Paradox, Access y Aproach, para entornos PC, y Oracle, ADABAS, DB/2, Informix o Ingres, para sistemas medios y grandes.

Biometría: Conjunto de métodos automatizados de identificación y verificación de la identidad de una persona viva, basados en una característica fisiológica. Analiza y mide ciertos rasgos unívocos de un individuo para crear un identificador biométrico. Este identificador puede ser almacenado en una base de datos y recuperado para su comprobación posterior.

Bit: Cantidad de información más pequeña que puede transmitirse. Una combinación de bits puede indicar un carácter alfabético, un dígito, una señal, un modificador u otras funciones.

Carrito de compras: Zona virtual de un sitio Web de compra electrónica donde el usuario va guardando los objetos o servicios a medida que los va comprando, de la misma manera que haría en un supermercado. Al final el usuario decide cuáles de ellos compra efectivamente o no

Centro comercial virtual (eMall): Agrupa bajo el mismo dominio y sitio web a un cierto número de cibertiendas, organizadas por calles. Algunos Cybermalls funcionan como una réplica de los centros comerciales offline, es decir, alquilan un espacio en el cual las cibertiendas, ceñidas a unas condiciones tecnológicas determinadas, pueden exponer sus productos y realizar ventas online.

Certificado digital: Es un documento digital que contiene información sobre a identidad de la autoridad que lo ha emitido y sobre el firmante de la transacción. Cada certificado está enlazado a la firma del agente al que certifica.

ChileCompra: Es el Sistema de Compras y Contratación del Sector Público, cuyo objetivo es garantizar elevados niveles de transparencia, eficiencia y uso de tecnologías en el mercado de las compras públicas, beneficiando así a empresas, Organismos Públicos y ciudadanía.

Ciberespacio: Es un término acuñado por el autor de ciencia-ficción William Gibson para describir todos los recursos de información disponibles en las redes informáticas.

Cliente: En Internet, usuario final o representante de una empresa u organización que adquiere los productos o servicios que se le ofertan a través de las diferentes plataformas. El modo más habitual de realizar el consumo es a través de páginas Web. Por otra parte, un cliente es además un tipo de programa que se necesita para poder conectar desde cualquier ordenador de un usuario con otro ordenador que ejerce de servidor.

Comercio electrónico: Compraventa de bienes y servicios mediante Internet y la telefonía móvil sin que exista ningún tipo de contacto físico o presencial entre comprador y vendedor. Quien vende puede hacerlo por correo electrónico, anuncio en grupo de noticias, en una lista de distribución, en una página Web, o por medio de un mensaje de texto al teléfono móvil. Quien compra puede pagar aceptando el ingreso en cuenta, contra reembolso, dando el número de VISA vía formulario, o anotando el de cualquier otra tarjeta, en una TPVV o a través de mensajes desde su teléfono móvil.

Comunicaciones: Transferencia electrónica de información de un lugar a otro. Las comunicaciones de datos se refieren a las transmisiones digitales, y las telecomunicaciones, a transmisión análoga y digital, incluyendo voz y video.

Conectividad: Estado que permite la transferencia de datos entre dos computadoras.

Confidencialidad: Garantiza que la información que se entrega a través de la red está protegida por un sistema de seguridad a fin de que terceros no autorizados no puedan tener acceso a ella.

Consumidor – Administración (C2A): Formas de relación entre los ciudadanos y las Administraciones Públicas realizadas mediante tecnologías de la información y de las comunicaciones.

Consumidor – Consumidor (C2C): Relaciones de intercambio entre dos consumidores a través de la Red.

Criptografía: Ciencia que estudia la manera de cifrar y descifrar los mensajes para que resulte imposible conocer su contenido a los que no dispongan de unas claves determinadas. En informática el uso de la criptografía es muy habitual, utilizándose en comunicaciones y en el almacenamiento de archivos. En comunicaciones, se altera mediante una clave secreta la información a transmitir, que circula cifrada hasta que llega al punto de destino, donde un sistema que conoce la clave de cifrado es capaz de descifrar la información y volverla inteligible.

CSP (Commerce Service Provider): Proveedor de servicios de comercio electrónico. Empresa que ofrece soluciones, como catálogos electrónicos, tiendas virtuales, etc.

Data Encryption Standard (DES): Algoritmo de cifrado de datos el cual utiliza bloques de datos de 64 bits y una clave de 56 bits. Ha sido estandarizado por la administración de EE.UU.

Dinero electrónico: También se denomina E-cash (contracción de los términos electronic y cash) y Digital cash. Del mismo modo que el dinero físico, el electrónico es anónimo y de valor inmediato. Este tipo de mecanismo de pago se creó con la intención de resolver los problemas de seguridad relacionados con el uso del número de tarjeta de crédito por Internet.

Documento electrónico: Representación material, destinada e idónea para reproducir una cierta manifestación de voluntad, materializada a través de las tecnologías de la información sobre soportes magnéticos, como un disquete, un CD-ROM, una tarjeta inteligente u otro, y que consisten en mensajes digitalizados que requieren de máquinas traductoras para ser percibidos y comprendidos por el hombre.

E-administración: Formas de relación entre los ciudadanos y las Administraciones Públicas, y entre estas últimas, realizadas mediante tecnologías de la información y de las telecomunicaciones. Ejemplos: la declaración de impuestos a través de Internet, o los servicios de información y tramitación ofrecidos a través de los sitios web de las Administraciones Públicas.

E-business: Cualquier tipo de actividad empresarial realizada a través de las Tecnologías de la Información y las Comunicaciones.

EDI (Electronic Data Interchange): Es un conjunto de procedimientos y normas que permiten la comercialización, control y registro de las actividades (transacciones) electrónicas. Es el intercambio electrónico de datos y documentos de computador a computador, en un formato estándar universalmente aceptado, que se realiza entre una empresa y sus asociados comerciales.

E-economy: Término se aplica al hecho de que la economía mundial forma hoy una red interconectada en la que todo lo que sucede en un punto afecta en mayor o menor medida a todos los demás. También se aplica a la actividad empresarial surgida en torno a Internet en todo tipo de sectores, no solamente en empresas que tienen como actividad principal la Informática y las Telecomunicaciones.

E-mail (electronic mail o correo electrónico): Se refiere a los mensajes transportados electrónicamente de un computador a otro.

Empresa – Administración (B2A): Corresponde a todas las transacciones entre las empresas y las organizaciones gubernamentales, se piensa que a través de ella se podrá promover la calidad, la seriedad y el crecimiento del comercio electrónico.

Empresa – Consumidor (B2C): Modalidad de comercio electrónico en el que las operaciones comerciales se realizan entre una empresa y sus usuarios finales.

Empresa – Empresa (B2B): Consiste en el comercio electrónico entre empresas a través de Internet. Esto incluye la presentación de propuestas, negociación de precios, cierre de ventas, despacho de pedidos y otras transacciones. Con este método se agiliza notablemente el tiempo empleado para esta contratación, ya que los pedidos a través de Internet se tramitan en tiempo real. También abarata los costos del pedido, se pueden comunicar con otras empresas de lugares distantes, e incluso de otros países.

Encriptación: Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor. Se usa para evitar el robo de información sensible, como números de tarjetas de crédito.

Firewalls o corta fuegos: Mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala. Estos sistemas suelen incorporar elementos que garantizan la privacidad, autentificación, etc., con lo que se impide el acceso no autorizado desde Internet.

Firma electrónica y/o digital: Es un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el signatario utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

Función hash: Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado resumen de los datos originales, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a

los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico.

Globalización: Fenómeno de repercusión automática, instantánea y de alcance mundial que se da en el ámbito de las actividades sociales, económicas y financieras, y que es causado principalmente por la acción combinada de las tecnologías de la información y de las comunicaciones, y de los medios de comunicación de masas.

Hackers: Este término describe a aquella persona, con altos conocimientos de sistemas, capaz de vulnerar diversas barreras de seguridad con objeto de detectar y alertar acerca de las deficiencias que vaya encontrando en su camino. Un buen hacker actúa sin ánimo de lucro o protagonismo y jamás destroza nada ni hace mal uso de la información a la que pueda tener acceso. Los que se dedican a romper los códigos de las licencias de registro del software; o robar claves de acceso de cualquier sistema o servicio, o destrozar algo son crackers, es decir, "rompedores".

Hardware: Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman un ordenador, incluidos sus periféricos.

Hipernexo: Nexo que relaciona un elemento (palabra, icono, imagen) al interior de un documento web con otro documento existente en el espacio WWW.

Hipertexto: Texto que incorpora nexos o relaciones a otros documentos.

Home-banking: Es un servicio para los usuarios de tarjetas de débito, por medio del cual se pueden efectuar las mismas operaciones que realizan en los Cajeros Automáticos, a excepción de extracciones o depósitos. Se puede ingresar desde cualquier computadora conectada a Internet.

HTML: Formato utilizado en los documentos en WWW.

HTTP: Protocolo que permite la comunicación y transporte de información en WWW.

HTTPS: Versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

Informática: Ciencia que estudia el tratamiento automático y racional de la información, a través de los ordenadores. Este término se refiere a lo mismo que computación, solo que informática tiene origen francés y computación origen inglés.

Infraestructura de Clave Pública (PKI): Procedimiento criptográfico que utiliza dos claves, una pública y otra privada; la primera para cifrar y la segunda para descifrar. Se utiliza en Internet, que es una red pública no segura, para proteger aquellas comunicaciones cuya confidencialidad se desea garantizar.

Infraestructura Global de la Información: Es el nombre que se le da a la infopista o autopista de datos que cubrirá todo el planeta.

Integridad: Se refiere a las medidas de salvaguarda que se incluyen en un sistema de información para evitar la pérdida accidental de los datos.

Interfaces: Conexión e interacción entre hardware, software y el usuario. El diseño y construcción de interfaces constituye una parte principal del trabajo de los ingenieros, programadores y consultores. Los usuarios "conversan" con el software. El software "conversa" con el hardware y otro software. El hardware "conversa" con otro hardware. Todo este "diálogo" no es más que el uso de interfaces. Las interfaces deben diseñarse, desarrollarse, probarse y rediseñarse; y con cada encarnación nace una nueva especificación que puede convertirse en un estándar más, de hecho o regulado.

Internet: Red de computadores establecida a nivel mundial y que nació con fines de defensa y académicos en la década del '50. Permite la conexión de cualquier computador que cuente con un módem y reciba el permiso de acceso de un proveedor del servicio. Integra información de variado tipo y se estima que millones de personas se conectan en la red.

Interoperatividad: Capacidad de los programas de ordenador para intercambiar información y utilizar mutuamente la información así intercambiada.

ISP (Internet Service Provider): Proveedor de servicios de Internet.

Kit de Conexión a Comercios (KCC): Es la interfaz que se une a la tienda virtual del Comercio, que se encarga de producir un enlace con el Servidor de Pagos de Transbank.

Logística: Conjunto de técnicas y medios destinados a lograr una gestión eficaz de los flujos de información acerca de los productos y servicios entre el productor, el distribuidor y el cliente final. La logística, que es una de las piezas claves del comercio electrónico, incluye también la gestión y el control de los inventarios y, por supuesto, la preparación y expedición de los pedidos.

Medio digital: Representación electrónica de cualquier elemento de uso corriente. Por ejemplo, vídeo digital es la representación binaria de un vídeo analógico. O un documento electrónico es la representación binaria de un documento de papel. Así sucede con el sonido, las imágenes, el correo, los fax, etc. En un futuro podríamos llegar a la representación electrónica de la persona misma.

Mercado electrónico: Ámbito donde se realizan las ventas y subastas en la Red. Es el mercado virtual donde productores, intermediarios, consumidores, empleados, usuarios domésticos e industriales, en definitiva, quienquiera sea, interactúa electrónicamente o digitalmente de alguna manera.

Microchip: Circuito electrónico de pequeñísimo tamaño. Es una de las tecnologías fundamentales en la base de todo el desarrollo actual de la informática.

Módem: Dispositivo que convierte las señales digitales en analógicas, y viceversa, y que permite la comunicación entre dos ordenadores a través de una línea telefónica normal o una línea de cable.

Monedero electrónico: Es un sistema de prepago que opera con una tarjeta inteligente que tiene un microchip, éste, al hacer contacto con los lectores de los dispositivos que, para tal fin, tienen instalados los establecimientos comerciales, realiza las transferencias del dinero contenido en la tarjeta.

Multimedia: Término que hace referencia a los diferentes tipos de datos que pueden ser procesados y mostrados por los ordenadores en forma de texto, gráficos, animaciones o vídeo. La plataforma Web esta considerada como la parte multimedia de Internet.

No-repudio: Situación en la cual el receptor de un mensaje de correo electrónico no puede negar haberlo recibido. Este concepto jurídico, en el ámbito del marketing e Internet, también se aplica al caso en el que el responsable del contenido de una Web no pueda negar que ha sido el quien la ha publicado en la Red.

On line: En red, en línea. Se está en red cuando se efectúa la conexión entre dos ordenadores en tiempo real, sin embargo, la expresión se refiere, en la mayoría de los casos, a cuando estos ordenadores se conectan vía Internet. Se está también on line a través de los mensajes que se reciben entre teléfonos móviles y entre un móvil e Internet y a la inversa.

P2P (Peer to Peer): Comunicación bilateral exclusiva entre dos personas a través de Internet para el intercambio de información en general y de archivos en particular.

Página Web: Es un documento creado en formato HTML (Hypertext Markup Language) que es parte de un grupo de documentos hipertexto o recursos disponibles en el World Wide Web. Una serie de páginas Web componen lo que se llama un sitio Web.

Passwords: Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado. Es frecuente su uso en redes.

Plan de Marketing: Documento donde ser plasma de un modo sistemático el conjunto de acciones que se va a seguir para lograr unos determinados objetivos en un plazo de tiempo concreto, basándose en las condiciones de un escenario dado y en función de un presupuesto asignado a tal efecto. La acción puede ser, por ejemplo, el modo de posicionar un nuevo sitio Web en el mercado. El objetivo: hacer comercio electrónico a través de él. Y todo lo anterior con el menor tiempo y dinero posibles. Por supuesto en el Plan de Marketing se deben incluir detallados análisis de la competencia, del producto o servicio, de la capacidad de respuesta, así cómo un seguimiento riguroso del grado de ejecución del proyecto adaptado a un cronograma.

Plan de negocios: Informe donde se expone los argumentos por lo que se crea una empresa, la viabilidad de la misma en un plazo de tiempo determinado y las principales iniciativas que se van a llevar a cabo para lograr su posicionamiento en el mercado. Si la idea de ese plan de negocio es presentarlo a un posible inversor, cabe añadir, que el contenido debe ser completo pero evitando la información superflua. Ese contenido debe hablar del mercado en que se va a operar, del producto o servicio que se ofrecerá, y del modelo organizativo que se va a seguir. Además el plan debe presentarse de modo ordenado y siguiendo una estructura sencilla y cómoda de entender.

Portal: Es un sitio Web que ofrece varios servicios. Por ejemplo: noticias, correo electrónico vía Web, foros de discusión, buscadores, información financiera, etc.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede

describir detalles de bajo nivel de las interfaces máquina-a-máquina o intercambios de alto nivel entre programas de asignación de recursos.

Protocolo SET (Secure Electronic Transaction): Protocolo de seguridad para compras en Internet. Es un conjunto de normas o especificaciones de seguridad, encriptadas, que constituye una forma estándar para la realización de transacciones de pago a través de Internet. Desarrollado por Visa, Mastercard y otras empresas.

Protocolo SSL (Secure Sockets Layer): Un protocolo de bajo nivel que permite establecer comunicaciones seguras entre un servidor Web y FrontPage o un explorador de Web.

Proveedores de Capital: Gran parte de las nuevas empresas de comercio electrónico han sido financiadas por fondos especializados, inversionistas de riesgo (venture capital) y capitalistas populares que han suscrito las primeras emisiones bursátiles.

Proveedores de Contenido: Incluye a todos los proveedores de información, entretención y servicios interactivos en línea, incluyendo buscadores y portales temáticos, tiendas virtuales e e-tailers (minoristas que venden a través de Internet).

Proveedores de hardware: Se relacionan al soporte físico de Internet, a nivel de los puntos de origen y destino de la red: fabricantes y ensambladores de PCs, módems, routers, proveedores de hosting (hospedaje) y hardware informático en general.

Proveedores de red: básicamente un negocio vinculado a las telecomunicaciones, compuesto por proveedores de conectividad, transporte y distribución de contenidos y acceso final (ISP, Internet Service Providers).

Proveedores de servicios complementarios. Comprende todos los servicios de gestión necesarios para el comercio propiamente tal, como pagos electrónicos, certificación/autentificación de firmas de clientes y proveedores, almacenaje y distribución de productos, etc.

Proveedores de software y diseño: relacionados con todo el espectro de programas orientados a la navegación (browsers), compresión y/o encriptación de datos y el diseño de páginas web (HTML, XML, Java) o paquetes de comercio electrónico como Ariba, Intelsys y Commerce One.

Red: Sistema de elementos interrelacionados que se conectan mediante un vínculo dedicado o conmutado para proporcionar una comunicación local o remota.

Redes informáticas privadas: Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.

Repository o registros: Son la base de datos a la que el público puede acceder on-line para conocer la validez de los certificados digitales, su vigencia o cualquier otra circunstancia que se relacione con los mismos.

Secure Server: Servidor seguro. Tipo especial de servidor diseñado para dificultar en la mayor medida posible el acceso de personas no autorizadas a la información en él contenida. Un tipo de servidor seguro especialmente protegido es el que se utiliza en

transacciones de comercio electrónico.

Seguridad: Mecanismos de control que evitan el uso no autorizado de recursos.

Servidor: Computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos. Internet es en último término un conjunto de servidores que proporcionan servicios de transferencia de ficheros, correo electrónico o páginas WEB, entre otros.

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.

Servidor de pagos (o pasarela de pagos): Una de las soluciones tecnológicas entregadas por Transbank que permite al Comercio operar con Tarjetas de Crédito, a través de la autorización de transacciones en línea vía Internet.

Sistemas de pagos electrónicos: Es el mecanismo mediante el cual se ejecuta la contraprestación de una obligación asumida a través de Internet, es decir, mediante la contratación electrónica.

Sitio Web: Conjuntos de servicios de red, ante todo documentos HTML, que están enlazados juntos y que existen en el Web en un servidor específico.

Software: Conjunto de programas, documentos, procedimientos y rutinas asociados con la operación de un computador. Es la parte intangible del computador. Dentro del software destaca el sistema operativo, las aplicaciones y los documentos..

Subasta virtual (e-Auction): Oferta, durante un periodo de tiempo determinado, de productos o servicios a quien mejor lo pague. En Estados Unidos es el negocio de Internet que más dinero ha dado, desde el primer día, hasta el momento. La empresa líder del sector es Ebay. En España y resto de países europeos esta iniciándose el sistema con propuestas como las de Mercado Libre, Ibazar, o Aucland.

Suministro puntual (spot sourcing): Forma de adquirir inputs que se necesitan para satisfacer una demanda puntual. Para esto las empresas buscan soluciones entre proveedores que no necesariamente conocen, porque, normalmente, lo que prima es un suministro rápido al menor coste posible.

Suministro sistemático: Forma de adquirir inputs que se precisan de manera regular (por ejemplo, un fabricante de automóviles precisa siempre de determinados componentes). Para esto las empresas tienden a utilizar proveedores a los que les une una relación estable, negociada en unas determinadas condiciones.

Tarjeta inteligente: Tarjeta que dispone de un chip capaz de procesar datos (personales o no), almacenarlos y encriptarlos. Una aplicación muy extendida de esta tecnología son las tarjetas que funcionan con los teléfonos móviles del sistema GSM.

Tarjetas de crédito: Cualquier tarjeta u otro documento que permita a su titular disponer de un crédito otorgado por su emisor, y es utilizado por su titular o usuario en la

adquisición de bienes o en pago de servicios, vendidos o prestados por establecimientos afiliados al sistema; sin perjuicio de prestaciones adicionales.

Tarjetas de débito: Cualquier tarjeta u otro documento que identifica al titular de una cuenta corriente o de una cuenta a la vista o de una cuenta de ahorro a la vista, contratada con el Emisor y que sea utilizada como instrumento de pago en la red de establecimientos afiliados al sistema, que cuenten con dispositivos electrónicos que operen con captura en línea de las transacciones y en que los montos correspondientes sean debitados inmediatamente en la cuenta del titular y acreditados en la cuenta del beneficiario, sólo si dichas transacciones son autorizadas y existen fondos suficientes.

Tecnología: Es el conjunto ordenado de conocimientos y los correspondientes procesos que tienen como objetivo la producción de bienes y servicios, teniendo en cuenta la técnica, la ciencia y los aspectos económicos, sociales y culturales involucrados.

Teleadministración: Es la posibilidad de que los ciudadanos accedan a los servicios administrativos de manera electrónica, 24 horas al día 7 días a la semana para la obtención de información.

Telecomunicación: Técnica de transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. Por tanto, el término *telecomunicación* cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de ordenadores.

Telemática: Es la transmisión de datos a distancia entre y por medio de ordenadores. Si sustituimos el vocablo transmisión por el concepto de comunicación, comprendemos la palabra datos en un sentido amplísimo y sobreentendemos que tras los equipos informáticos hay personas, el concepto adquiere otro significado: la comunicación entre personas utilizando el ordenador como medio.

Teletrabajo: Es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador en la empresa durante una parte importante de su horario laboral. Engloba una amplia gama de actividades y puede realizarse a tiempo completo o parcial.

TIC (Tecnologías de Información y Comunicaciones): Conjunto de herramientas, habitualmente de naturaleza electrónica, utilizadas para la recogida, almacenamiento, tratamiento, difusión y transmisión de la información.

Tienda virtual (e-Shop): Página Web donde se pueden realizar compras electrónicas en la cual le solicitará una serie de datos al usuario en orden de ejecutar la transacción.

Transacciones digitales: En informática, se llama transacción a la operación que modifica el estado de una base de datos, sin que los datos en sí mismos pierdan consistencia alguna.

Videoconferencias: Sistema de comunicación mediante el cual dos o más personas situadas físicamente en distintos lugares pueden conversar y verse en vídeo a través de la Red.

Webpay: Servicio integral que ofrece Transbank a los Comercios en Internet, para que reciban pagos con Tarjetas Bancarias a través de distintas soluciones tecnológicas. Una de ellas es el Servidor de Pagos.

World Wide Web: Red mundial amplia, conocido también como: W3 ó el Web. Sistema de arquitectura cliente / servidor creada por el CERN y permite la distribución y obtención de información en Internet basado en hipertexto e hipermedia. Ha sido una de las piezas fundamentales para la comercialización y masificación de Internet.

BIBLIOGRAFIA

BULL, R.; CASANOVA, C. (2001) Firma electrónica y certificación digital v1.4. Documento Centro de Tecnologías de Información de Intec-CTI.

ESCOBAR, P. (2002) Tecnologías y normativa de firma electrónica. Documento Centro de Tecnologías de Información Intec-CTI.

FED. STEERING PKI COMITTEE. (2000) The Evolving Federal Public Key Infrastructure.

GARIBOLDI, G. (1999) Comercio electrónico: conceptos y reglamentaciones básicas. Documento de divulgación 4, BID - INTAL.

MELNICK, S.; BARRAZA, J. M. (2002) E-Business, sí o sí. Centro de Estudio de la Economía Digital de la Cámara de Comercio de Santiago.

http://derecho.udp.cl

http://www.acepta.cl

http://www.b2u.cl

http://www.baquia.com

http://www.ccs.cl

http://www.chilecompras.cl

http://www.cisco.com/

http://www.claveempresarial.com/

http://www.cnc-once.cl
http://www.contador.cl
http://www.diariopyme.cl/
http://www.ebcenter.org/
http://www.e-certchile.cl
http://www.eclac.cl
http://www.economia.cl
http://www.educom.cl
http://www.elcomercioperu.com.pe/
http://www.emprendedores.cl
http://www.entelchile.net
http://www.improven-consultores.com/
http://www.infonomics.net
http://www.laempresa.net/
http://www.lasegunda.com
http://www.onnet.es
http://www.paisdigital.org
http://www.publimark.cl
http://www.revistanegocios.net
http://www.santandersantiago.cl
http://www.uvirtual.cl
http://www.verisign.cl