UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

"COMERCIO ELECTRÓNICO SEGURO"

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:
MANUEL DELFIN CORAL ALAMO

PROMOCIÓN 1997-I
LIMA-PERÚ
2003

DEDICATORIA
A mis dos tesoros Giovanna y Silvana

COMERCIO ELECTRÓNICO SEGURO

SUMARIO

Los capítulos I, II y III del proyecto describen las tecnologías de comercio electrónico actuales, centrando su atención en los esquemas de pago electrónicos, las tecnologías de transacciones electrónicas seguras (SSL, IPSec y SET), y las expectativas del comercio electrónico en los próximos años.

Los conceptos de la Infraestructura de Clave Publica (PKI por sus siglas en Ingles), son de vital importancia en el mundo de las transacciones electrónicas seguras, es por ello que dedicamos un capitulo a la descripción de esta tecnología y los beneficios de su implementación.

Como resultado de este estudio podemos concluir que el futuro del comercio electrónico pasa por el Protocolo SET, desarrollado por Visa&MasterCard, un protocolo que permite el pago electrónico seguro por Internet utilizando tarjetas de crédito. SET es un protocolo muy complejo que incorpora las técnicas criptográficas más modernas como son la criptografía asimétrica, las firmas digitales y los certificados digitales, de modo que el presente trabajo no pretende ser una referencia detallada de estos conceptos aunque nos esforzamos por mostrarlos de manera clara y concisa.

El capitulo IV pretende explicar detalladamente el Protocolo de Transacciones Electrónicas Seguras (SET por sus siglas en Ingles), se detallan

las tecnologías criptográficas que lo soportan, los procesos de certificación así como el flujo de los mensajes de pago electrónico.

En el capitulo V se realiza una descripción de las bases legales sobre las cuales se soportan actualmente las transacciones electrónicas seguras, enfocando nuestra atención al caso Peruano así como al de los otros países de la región.

La parte final esta dedicada a los anexos, en los cuales se detallan las leyes actualmente vigentes en el Perú con relación a las Firmas y Certificados Digitales así como la Ley que contempla los delitos Informáticos.

ÍNDICE

PRÓLOGO

El desarrollo del Comercio en el Perú como factor de crecimiento económico, especialmente para las PYMEs, y como factor de competitividad de la Industria, requiere eliminar dos grandes Obstáculos. Por un lado el Estado debe garantizar que Internet y las tecnologías que lo soportan sean accesibles no solamente a las empresas sino también a los ciudadanos. Por otro lado, la ausencia de una regulación sólida se constituyen como frontera legal para una generalización de Internet y por ende los servicios de Comercio Electrónico; Habida cuenta que Internet es un espacio virtual sin fronteras y de alcance universal se hace necesario una regulación Internacional mas que nacional y regional, toda vez que esto implicaría la eliminación de una gran cantidad de obstáculos legales tanto para los prestadores de servicios como para los usuarios finales.

En los últimos años Internet ha experimentado un crecimiento exponencial en el número de usuarios y hoy en día está consolidándose como un medio de comunicación habitual en casi todos los países del mundo. El auge de Internet está permitiendo la aparición de una serie de servicios caracterizados por ofrecerse a distancia a través de la red, así podemos encontrarnos con los conceptos de Tele trabajo, Telemedicina o Telecompras entre otros. Un estudio realizado por la prestigiosa consultoría Forrester Research en el que se pronosticaba un crecimiento del comercio electrónico por Internet de los 121 millones de dólares del 1997 a los 3,800 millones en el

2002 supuso el primer aviso importante sobre las posibilidades reales de la venta por Internet. Este hecho, acompañado por el increíble éxito de la librería Amazon.com, y otras firmas no menos exitosas, han convertido al comercio electrónico en la actividad de moda en Internet y se espera que este negocio se convierta en el motor de Internet en los próximos años.

La venta directa por Internet no es más que la versión tecnológica de otros medios de venta a distancia como la venta por catálogo. Pero Internet incorpora la posibilidad de que ciertos productos puedan ser enviados directamente por la red como pueden ser: música, vídeo, documentos o cualquier otro tipo información susceptible de ser digitalizada.

El pago de estos bienes puede realizarse de varios modos: giro postal, transferencia bancaria, contra reembolso o de manera mas cómoda, por medio de las tarjetas de crédito, en este punto es importante mencionar que los pagos a través de la Internet no constituyen un método seguro ya que cualquier información que viaje por la Red puede ser fácilmente interceptada. La solución a este problema pasa por aplicar la tecnología criptográfica a las órdenes de pago electrónicas y solucionar de este modo los problemas de seguridad.

Los sistemas de pago electrónico significarán por tanto la realización práctica de muchos de los conceptos teóricos relacionados con la criptografía como: Los certificados digitales, las firmas digitales, los sobres digitales, etc. basados en la encriptación asimétrica; convirtiendo al comercio electrónico en la principal aplicación que hará uso habitual y masivo de las modernas técnicas criptográficas.

CAPITULO I
INTRODUCCIÓN A LAS TECNOLOGÍAS DE COMERCIO ELECTRÓNICO

El Comercio Electrónico es una nueva forma de entender la economía que esta llamada a ocupar un importante espacio dentro de nuestra sociedad moderna. Entender en que consiste el comercio electrónico es una tarea bastante complicada ya que se trata de un concepto que engloba una gran cantidad de conceptos.

La enorme expansión que ha tenido Internet en los últimos años ha significado un cambio importante en la forma de relacionarse de muchas personas y empresas. Internet significa un acercamiento entre compradores y fabricantes independientemente de la distancia. Esto supone un gran atractivo para las empresas que con una inversión mínima pueden acercarse a un enorme mercado potencial en crecimiento constante.

La primera aplicación al mundo de los negocios de esta tecnología fue la promoción y el marketing por la red. Actualmente Internet ya se ha consolidado como el cuarto medio de información junto a la Prensa, la Radio y la TV. Tras el éxito del marketing en la red, el siguiente paso es evidente: vender directamente por Internet, ahorrándose los intermediarios y pudiendo así rebajar los precios. Esto no es más que una extrapolación de la venta a distancia, por catálogo o por la Tele tienda de TV, donde el pago de estos bienes se realiza a contra-reembolso.

El negocio por Internet está estrechamente ligado al número de usuarios

de la propia red, que a su vez está condicionado por el precio de las conexiones a Internet. Son muchas las empresas, instituciones así como el público en general los abogan por la "tarifa plana" de conexión a Internet, esto sin duda supondría un impulso adicional a todos los negocios que se realicen por la red.

Con la utilización de tarjetas de crédito en Internet, se pueden efectuar pagos electrónicos, simplificando enormemente todo el proceso de compra. Es más, si el bien adquirido es susceptible de ser enviado digitalmente (como audio, vídeo, documentación digital o cualquier otro tipo de información digitalizada), la compra puede realizarse enteramente por Internet.

Precisamente cuando hablemos de Comercio Electrónico nos referimos concretamente al pago electrónico a través de redes de telecomunicaciones digitales como Internet; aunque, como hemos explicado anteriormente, las implicaciones económicas del Comercio Electrónico van mucho más allá.

Actualmente existe un gran interés hacia el comercio electrónico, animado por las perspectivas de negocio previstas para los próximos años. El despegue, finalmente se produjo a raíz de un estudio publicado por la consultora Forrester Research, empresa especializada en estudios sobre Internet en el que vaticinan un crecimiento del comercio electrónico (e-commerce) de los 121 millones de dólares de 1997 a los 3800 en el 2002, solo en EE.UU. Este estudio ha sido confirmado por otros similares realizados por las más prestigiosas consultorías del mundo, entre ellas podemos citar a Andersen Consulting y Price Waterhouse.

La mayoría de las iniciativas actuales de venta por Internet se pueden calificar como fracaso relativo ya que los beneficios obtenidos por esta

actividad económica esta muy lejos de ser rentable y muy por debajo de otras actividades similares como la venta por catalogo. A pesar de todo, estas iniciativas son muy importantes desde el punto de vista estratégico sobre todo para las grandes empresas que deseen posicionarse y aprovecharse de las ventajas futuras de este tipo de negocios.

Algunas empresas informáticas como Dell o Cisco han conseguido resultados notables en la venta directa por Internet pudiendo abaratar los precios aprovechando la supresión de intermediarios, y creando un referente obligado al resto de empresas del sector.

Mención aparte merece la librería Amazon.com, que ha roto todas las previsiones y en unos pocos años ha pasado a convertirse en la mayor librería del mundo, vendiendo únicamente por Internet. Su fama ha crecido hasta límites increíbles y actualmente es el ejemplo utilizando por todos los que apuestan en esta tecnología como paradigma del éxito en el comercio electrónico por Internet. Como resultado de las expectativas puestas en Amazon.com, la empresa ha experimentado un incremento del 3000 % en su cotización en bolsa en el último año.

1.1. En busca de un estándar de pago electrónico

El principal problema para la explosión definitiva del comercio electrónico es que no existe un protocolo estándar y definitivo para realizar pagos seguros por Internet. SSL ofrece una gran seguridad pero si lo comparamos con otros protocolos existentes como CyberCash, NetBill o Mondex nos damos cuenta que SSL presenta una serie de limitaciones intrínsecas que pueden comprometer la utilidad del protocolo para un uso generalizado del mismo. Analizando los criterios de seguridad y las deficiencias

de SSL respeto a estos criterios podremos hacernos una idea de cómo debería ser el protocolo ideal.

Criterios de Seguridad

Todo sistema de pago por medios no seguros, como es el caso de Internet, debe satisfacer una serie de criterios de seguridad que impidan cualquier tipo de fraude. Estos criterios son:

Confidencialidad.- Ninguna persona ajena a la transacción puede tener acceso a los datos. Más aún, las entidades implicadas en la compra no deberían conocer más datos que los imprescindibles para realizar su función. De este modo, el Vendedor no tendría porque tener acceso a los datos financieros del cliente y el banco tampoco debería conocer la lista de los artículos adquiridos.

Integridad.- Ningún dato puede ser modificado ni durante ni después de la conexión.

Autentificación.- Todas las entidades participantes en la transacción deben estar debidamente autentificadas antes de comenzar la compra. Por razones de privacidad, el cliente solo debería garantizar que es el legítimo propietario de la Tarjeta de Crédito, sin necesidad de hacer pública su identidad.

No Repudio.- Debe garantizarse que una vez finalizada la compra ninguna de las partes pueda negar haber participado en ella. Es decir, al finalizar la transacción debe quedar algo equivalente a un Recibo de compra firmado.

Tipos de Pago

Los dos sistemas clásicos por excelencia de pago no efectivo son los cheques convencionales y las tarjetas de crédito. En el sistema financiero, el dinero toma forma de entrada en los libros de los bancos y de otras instituciones financieras. Esto para el usuario se refleja en la existencia de una

cuenta depósito en la que se graba los depósitos del cliente y se realizan pagos en forma de cheques o transferencias.

Un cheque es un documento escrito por el usuario de la cuenta y autentificado por el mismo que se entrega a un comerciante, quien a su vez lo acepta antes de presentarlo en su banco. Si el banco cobrador y el del vendedor son los mismos, todo se reduce a una compensación interna de apuntes. Si por el contrario, ambos disponen de cuentas en bancos distintos, el banco cobrador deberá presentar el cheque y recoger los fondos a través de un sistema de ajuste o cámara de compensación ACH (Automatic Clearing House). Esta cámara puede pertenecer al estado, por ejemplo, al banco emisor de la moneda, o tratarse de un sistema intermediario privado, como *VisaNet ACH Service*. En el momento de la entrega del cheque, el cobrador no sabe si este se encuentra respaldado por fondos por lo que corre cierto riesgo. Pero los pagadores también asumen determinados riesgos frente a la posible existencia de cheques falsos ya que reciben los extractos de las cuentas después de pagar sin confirmación previa al pago.

Otra alternativa es la utilización de un sistema de crédito, como una tarjeta o un servicio bancario de adelantos de descubiertos. El comerciante se asegura el pago y el emisor asume la responsabilidad del cobro. El ajuste se realiza entonces cuando el comerciante envía un lote de autorizaciones a su banco entre este y el banco emisor de la tarjeta

Existen dos tipos de operaciones con tarjeta de crédito que suponen distinto balance de riesgo en función de si la tarjeta se encuentra presente o no.

En el primer caso, la tarjeta presente, todo el riesgo del crédito pasa al

comerciante. En estos casos el comerciante puede verificar la firma del titular comparando la que este imprime en el recibo con la que aparece en la tarjeta. Por ello, será responsabilidad suya si se hace uso fraudulento de la tarjeta de un tercero. La integridad de la transacción queda garantizada para el cliente mediante una copia-papel del recibo. El nombre de la cuenta se autentifica a través del número de la tarjeta y la transacción puede ser confirmada enviando los datos por medio de una red privada de la asociación.

En el segundo caso, la tarjeta no presente, el consumidor asume cierta parte (pequeña) del riesgo ante un posible fraude ya que es responsabilidad suya proteger el número de tarjeta, debido a que este es el único medio de identificación del pagador en la transacción (como mucho se podrá pedir la fecha de caducidad y dirección y comprobarlas). Este es el sistema empleado en los pedidos por teléfono o Internet (en pedidos como correo o fax, aun se cuenta con la firma del titular como medio de no repudiación, que no de autentificación). Por ello, dado que nada impide que se pueda colocar un sniffer (programa que monitoriza todos los datos que pasan por cierto ordenador) en la red, los números de tarjeta deben viajar encriptados por la red.

Hay diferencia entre el uso de cheques y de tarjetas. Un pago mediante cheques supone dinero pagado para el consumidor, que asumirá todos los inconvenientes derivados de una falla del comerciante. Sin embargo, si se paga con tarjeta se puede pedir la restitución del importe. El problema pasa a ser del banco emisor de la tarjeta, que deberá pedir cuentas al del comerciante.

1.2. Tipos de Protocolos de pago seguro

El crecimiento de Internet ha permitido crear una nueva vía de comunicación entre comerciantes y compradores potenciales, lo que ha

propiciado la aparición de diferentes sistemas de pago electrónico. El evidente riesgo de fraude condiciona totalmente estos sistemas por ello ha sido necesario aplicar las más modernas técnicas de encriptación para garantizar la seguridad.

Hoy en día el protocolo utilizado para el pago con tarjeta de crédito por Internet es el SSL (Secure Socket Layer) aunque no es el único ni el primero que se ha utilizado. Su éxito se debe a la gran seguridad que aporta y a la facilidad de implementación ya que es el único de los protocolos estandarizado. A continuación se presenta un resumen de los sistemas más conocidos creados para el pago por Internet.

1.2.1. FSTC (Financial Services Technology Consortium)

FSTC es un consorcio americano de bancos, organizaciones gubernamentales y empresas tecnológicas creado en 1995. Uno de los proyectos promovidos por este consorcio es la creación de un sistema de cobro de Cheques Electrónicos.

El pagador debe contar con un procesador seguro, que se implementa en forma de tarjeta inteligente. Este procesador es el encargado de generar los cheques que consisten, simplemente en órdenes de pago firmadas digitalmente. Los cheques se trasmiten al comerciante que los acepta firmándolos digitalmente y los envía al banco, que los hará efectivos a través de la una red ACH clásica.

1.2.2. CheckFree

Checkfree Corporation es una entidad financiera americana que lleva realizando transacciones electrónicas y cobros con tarjetas de crédito a distancia desde 1983. Sus clientes son tanto empresas como particulares que

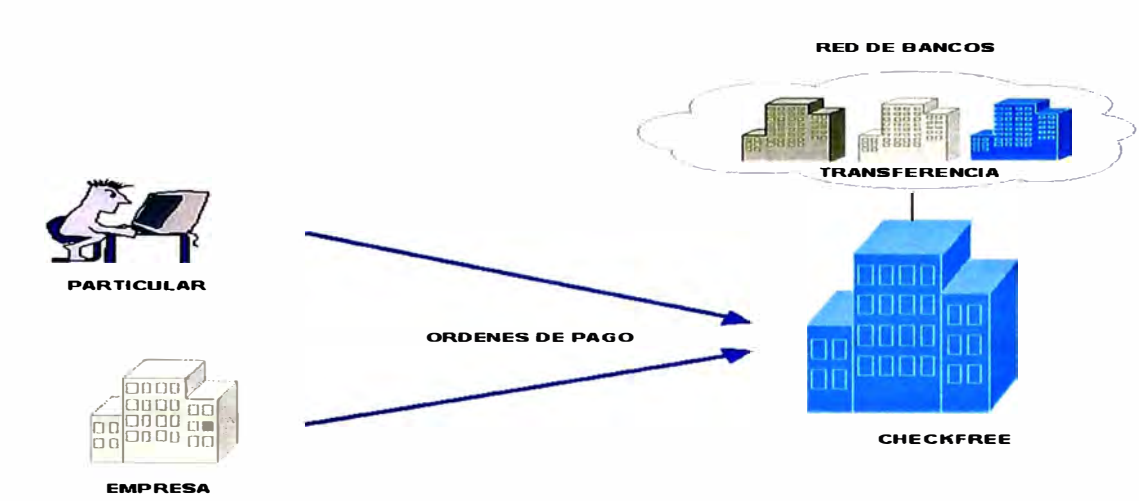


Fig. 1 CheckFree

deben poseer una cuenta en la entidad. Para realizar un pago electrónico, el usuario debe conectarse vía módem (sin pasar por Internet) a Checkfree y enviar una orden de pago. Dependiendo del tipo de pago, Checkfree utilizará la U.S. Reserva Federal o el sistema RPS de MasterCard para realizar la transferencia electrónica de fondos.

Para el pago por Internet, Checkfree ha decidido utilizar la tecnología de Cybercash de encriptación y autorización.

1.2.3. First Virtual (FV)

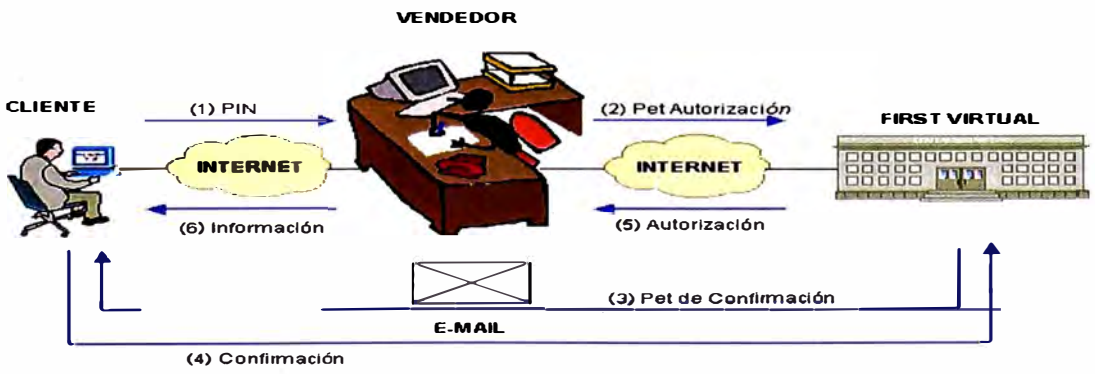


Fig. 2 First Virtual

Fue uno de los primeros en aparecer (1994) con la peculiaridad de no hacer uso de la criptografía. Un consumidor que desee hacer uso del sistema primero debe registrarse en el mismo, tras lo que obtiene un Virtual PIN, ID o identificador de First Virtual. Para ello debe de enviar un número de tarjeta de crédito, VISA o MasterCard, por medio off-line, como teléfono o fax. Una vez registrado podrá realizar compras por Internet o acceder a información restringida en un servidor que emplee el sistema FV.

Tras registrarse, se recibe un mail con una clave de doce dígitos, y un número de teléfono donde confirmarlo. Mantener un PIN cuesta 5 dólares al año aproximadamente.

Para realizar un pago bastará con presentar el Virtual PIN al comerciante. Éste se conectará a un servidor FV para comprobar si el pago es correcto, y de ser así, enviará la mercancía o dará paso libre a la información.

Para realizar un pago al comerciante, First Virtual, envía un e-mail al consumidor en el que le indica la operación y le pregunta si desea pagar o no. El consumidor deberá confirmar el pago respondiendo "yes", "no" o "fraud". Mediante este sistema el comerciante no llega nunca a saber el número de tarjeta del consumidor, ni ésta llega nunca a viajar por la red. El protocolo de validación de FV es el más lento de todos los medio de pagos electrónicos al requerir una confirmación del usuario off-line. No hace uso de la criptografía y permite el anonimato del usuario frente al comerciante.

1.2.3. NetMarket

Se trata de un sencillo sistema que permite el pago electrónico por Internet utilizando como seguridad el sistema Pretty Good Privacy (PGP) para

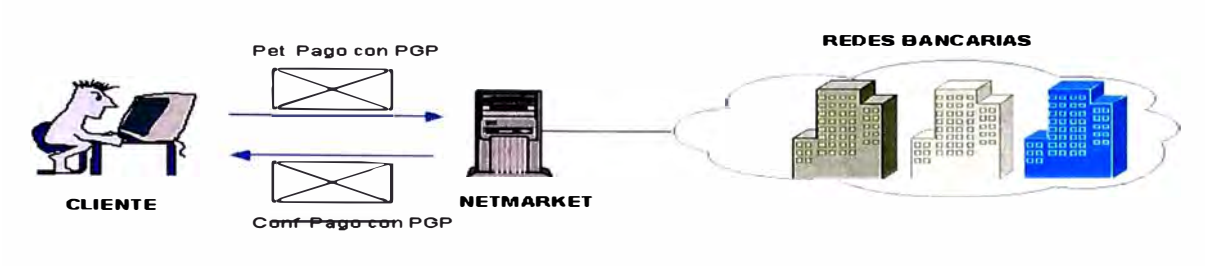


Fig. 3 NetMarket

encriptar los números de tarjetas de crédito manteniendo la confidencialidad de los datos

1.2.5. NetBill

NetBill es una alianza entre la Universidad Carnegie Mellon y Visa Internacional con el objetivo de ofrecer un sistema de pago seguro a través de Internet. NetBill se centra exclusivamente en la venta de información digital que pueda ser enviada por medios electrónicos como artículos de prensa, software, música, videos o cualquier tipo de documentación electrónica.

NetBill es un sistema prepago, es decir, todos los usuarios deben crear una cuenta antes de realizar cualquier compra. El usuario selecciona la información que desea y la recoge del servidor a cambio envía una orden de pago al Vendedor. Éste remite la orden de pago al Servidor NetBill que deberá autorizar la compra realizando una transferencia de la cuenta del comprador a la del comerciante. Tanto la orden de pago como la información adquirida se encuentran cifradas. El Vendedor desconoce los datos de la orden de pago y el Comprador no puede utilizar la información sin conocer la Clave de

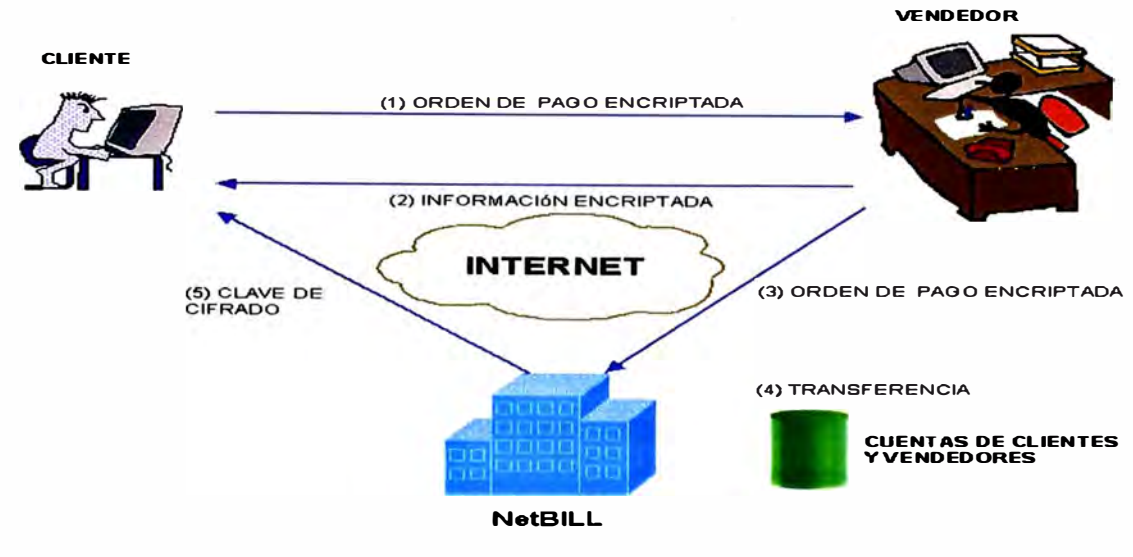


Fig. 4 NetBill

encriptación. Tras aceptar la compra, el Servidor NetBill realiza la transferencia y envía la Clave de cifrado al usuario que le permitirá descifrar los datos adquiridos.

NetBill funcionó en periodo de pruebas el verano de 1995 y permitió el acceso a diferentes servicios universitarios de la CMU.

1.2.6. NetCash y NetCheque

Sistema creado en la Universidad de Sur California (USC) en 1997. Se trata de un sistema de pago seguro por Internet que permite varias implementaciones como E-cash o como cheque digital bajo el mismo protocolo. Netcash es similar a Digicash y permite el pago con dinero electrónico de forma que mantiene el anonimato del comprador. Por su parte Netcheque sigue un esquema típico de pago con tarjeta de crédito como Cybercash. Ambos sistemas utilizan el mismo servidor para validar los pagos.

La seguridad del protocolo se basa en Kerberos, y la firma digital empleada es un ticket especial llamado Proxy. Si se desea se puede cambiar la criptografía a un modelo de clave pública, pero disminuirá el rendimiento.

Para escribir un cheque, el usuario especifica los datos, y el software cliente obtiene un ticket Kerberos para esta operación, genera un autentificador para una suma de control sobre la información del cheque, y coloca el ticket en el campo firma del cheque. El cheque se codifica entonces en Base-64 y se envía al destinatario. Al recibirlo, el software del vendedor lee la parte en claro del mismo, extrae el ticket Kerberos y lo envía a través de una conexión cifrada al servidor Netcheque que valida la operación.

1.2.7. CyberCash

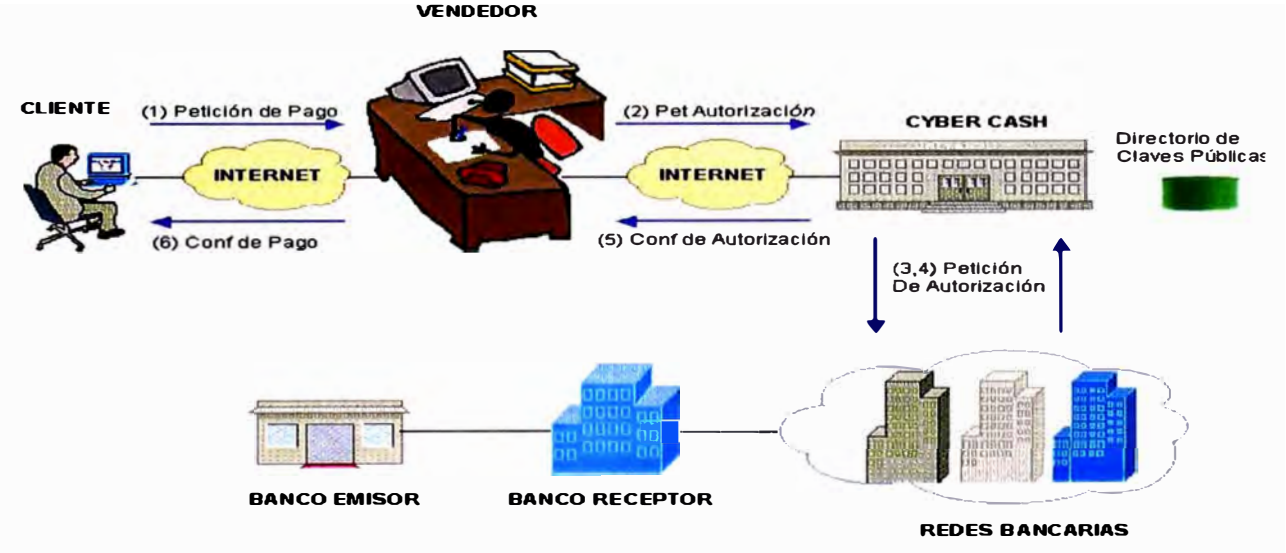


Fig. 5 CyberCash

Es uno de los medios de pago electrónicos pioneros. La empresa fue creada en 1994 y el sistema CyberCash se encuentra operativo desde abril de 1995. Se trata de un sistema integrado con el WWW que utiliza un protocolo propio manejado por un software que debe ser distribuido tanto a comerciantes como a consumidores. Constituye una pasarela entre Internet y las redes de autorización de emisores de tarjetas, contando para ello con la experiencia ganada con el sistema Verifone de autorización de tarjetas por teléfono, del cual deriva. El consumidor cuenta con un software "wallet" o monedero que

puede ligar a varias cuentas bancarias o a las tarjetas de crédito. El software encripta todos los datos, realiza un registro de todas las transacciones y se encuentra protegido mediante contraseña. En el lado del comerciante se sitúa un software similar.

Cuando un usuario baja el software de CyberCash, genera un par de claves públicas, Kp, y privada, Ks para él. El sistema empleado es RSA de 1024 bits. A continuación envía Kp al servidor de CyberCash que almacena en una base de datos. De esta forma solo CyberCash sabe las claves públicas de todos los interlocutores posibles. La comunicación entre consumidor y comerciante se lleva a cabo en claro, mientras que la comunicación de estos con CyberCash se realiza de forma protegida. Para ello se emplea una clave de sesión DES aleatoria de 56 bits que se distribuye encriptada con la llave publica del interlocutor. CyberCash tiene incrustada su propia llave publica en el software por lo que cualquiera puede comunicarse con él. Un dato importante es que la clave DES es de 56 bits cuando por las leyes de la legislación americana antes fijaban un máximo de 40 bits, y es que CyberCash consiguió un permiso especial.

La transacción se lleva a cabo de la siguiente manera:

1. El cliente selecciona un ítem a adquirir mediante WWW y elabora un pedido.
2. El software del comerciante envía "la factura pro forma" al software " wallet". La factura pro forma es texto en claro, firmado digitalmente en el que figura una descripción de la compra así como las tarjetas de crédito aceptadas. Para la realización de firmas digitales se emplean funciones hash MD5 y claves secretas RSA. A su recepción, el

software "wallet" da a elegir al usuario entre aquellas tarjetas que tiene registradas y le pide autorización para realizar el pago.

3. Previa confirmación del usuario, el software "wallet" del cliente genera un mensaje de pago y lo envía la comerciante. Este mensaje consiste en un hashing de la factura junto con las instrucciones de pago, todo ello firmado digitalmente y encriptado para CyberCash.

4. A la recepción del mensaje, el comerciante, que no puede descifrarlo simplemente añade la información al pedido (también firmada digitalmente) y lo remite a CyberCash.

CyberCash desencripta y compara los dos mensajes. Si coinciden los datos, solicita confirmación, y a través de la red financiera y trasmite la respuesta al comerciante para que este pueda cerrar la transacción con el cliente.

Todo este proceso se lleva a cabo en un periodo de tiempo inferior a un minuto. El proceso descrito es el caso más habitual, no obstante, el protocolo CyberCash es mucho más complejo y contempla la posibilidad de reintegros, anulaciones y solicitud de estado. Una versión antigua se puede encontrar en Internet en forma RFC.

Respecto a la protección del consumidor cabe destacar que, al encriptarse la orden de pago para CyberCash y no para el comerciante este no ve el número de la tarjeta de crédito lo que unido al hecho de que se comprueba la descripción de la compra, impide el abuso por parte de los comerciantes. En lo referente a la privacidad, aunque CyberCash tiene acceso a la descripción de la compra, esta no tiene porque incluir los detalles de la compra, puede constar como dato la referencia y el tipo solamente. De este

modo el comerciante no ve la tarjeta y CyberCash no ve el producto

1.2.8. DigiCash

Fundada en 1990 en Ámsterdam por el prestigioso Criptógrafo David Chaum, DigiCash ha sido una de las empresas que más han aportado al concepto de dinero digital. La diferencia con CyberCash, radica en que es un sistema de pago anticipado, donde se adquiere previamente el dinero del banco y se almacena digitalmente en el software del comprador. Este sistema permite la compra anónima ya que no requiere autentificación.

El usuario abre una cuenta en DigiCash y a cambio recibe una lista de números de 64 bits que equivalen a diferentes cantidades de dinero electrónico (E-Cash). Para pagar únicamente debe enviar uno de estos números al Vendedor. Una vez recibidos, se remitirán al Servidor DigiCash que realizará la transferencia manteniendo el anonimato del comprador. DigiCash es el equivalente electrónico a los Cheques de Viaje.

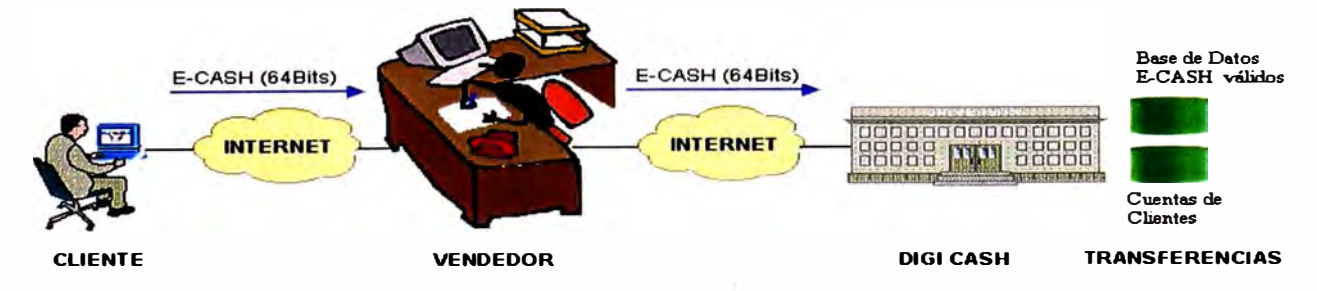


Fig. 6 DigiCash

1.2.9. Mondex International

Mondex es una asociación de bancos creada en 1995 en Gran Bretaña y destinada a promover el uso de dinero electrónico usando como soporte básico las Tarjetas Inteligentes o Tarjetas Chip. El E-Cash puede ser intercambiado por cliente y comerciantes siempre que posean los medios tecnológicos necesarios compatibles con la tecnología Mondex. Las Tarjetas pueden ser utilizadas a su vez en cajeros automáticos (ATM) o incluso en pagos a distancia por Internet.

1.2.10. Open Market

Open Market fue fundada en 1994 y es una de las empresas pioneras en el comercio electrónico por Internet. Su contribución más importante no se debe a la creación de nuevos protocolos de seguridad sino a StoreBuilder, un software destinado a la creación de Tiendas Virtuales y CyberMalls (Grandes almacenes virtuales) en Internet bajo un entorno Web. Los medios de pago han ido adaptándose a medida que han ido apareciendo nuevos medios de pago electrónicos. Primeramente Open Market funcionó permitiendo el pago con tarjeta de crédito con comunicaciones no cifradas. Más tarde se utilizó la tecnología de CyberCash y finalmente adoptó SSL.

CAPÍTULO II
INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

La Criptografía de Clave Publica es su estado actual, se ha constituido como la tecnología base sobre la cual se desarrollan otras tecnologías como E-Commerce, Intranets, Extranets, VPNs y un sin número de aplicaciones Web. La manera como el mundo hace negocios hoy en día esta cambiando, y los sistemas de seguridad que los soportan están a la vanguardia muy de la mano a estos cambios.

Hoy en día, aplicaciones tan simples como el correo electrónico ya no solamente transportan información poco relevante o simples memos sino también información tan confidencial como estados financieros de las empresas, proyecciones de negocios, etc. que requieren ser protegidos por obvias razones, la Web ya no es solamente un medio de publicidad sino también una plataforma sobre el cual se realizan transacciones de compra y venta sin limitaciones de fronteras ni lenguas ni horarios.

Asegurar los sistemas de correo electrónico, Web, E-Commerce, Intranets, VPNs, Extranets contra accesos no autorizados, suplantación de identidades, y otras formas de fraude por citar algunos, requiere de un sistema de seguridad muy robusto el cual nos provea Privacidad (Confidentiality), autenticación (authentication), control de acceso (Access Control), integridad de la información o datos (Data Integrity) y responsabilidad en la gestión (Accontability). Los Certificados y la criptografía de clave pública están

emergiendo en la actualidad como la base de un sistema de seguridad robusto, así lo indican las muchas compañías que actualmente los tienen adoptados y las muchas otras que planean adoptarlos en los próximos años como la base de los sistemas de seguridad principal.

La criptografía de clave publica ofrece muchos beneficios de seguridad cuando es apropiadamente implementado y como otras tecnologías requiere una infraestructura para poder ser desarrollado, sin embargo, la infraestructura de clave publica o mas comúnmente conocido como "PKI", no es precisamente un objeto físico o un proceso de software, sino un conjunto de servicios esenciales para la administración de los Certificados Digitales y las claves de encriptación para las personas, programas y sistemas.

El propósito de la infraestructura de clave publica (PKI), es facilitar la aplicación de la criptografía de clave publica a los negocios, la criptografía de clave publica es crucial para la tecnología de comercio electrónico, Internet, Intranets y otras aplicaciones que requieren seguridad distribuida en el cual los participantes no son parte de una misma red y no cuentan con credenciales de seguridad comunes. La criptografía de clave pública provee la forma más eficiente de implementar este tipo de seguridad en base a sus cuatro cualidades inherentes como son:

Privacidad

- Encriptando los e-mails que serán enviados a través de Internet, previendo así que estos puedan ser leídos antes de llegar a su destino.
- Encriptando el trafico de la red cuando el cliente visita un Web site, protegiendo de ese modo datos sensibles como las ordenes de compra, información de las tarjetas de crédito, etc.

- Encriptando las sesiones de video conferencia (NetMeeting), previendo de este modo que la conversación pueda ser oída.

Integridad

- Para garantizar que la información no ha sido manipulada

Autenticación

- Verificando la identidad del visitante para habilitarlo en el uso de determinadas facilidades de la red interna.
- Proveyendo al cliente la seguridad de estar visitando el su web site y no uno que maliciosamente lo reemplaza

No Repudiación

- Creando un registro, sin posibilidad de modificación de la compra de un cliente desde su web site.
- Firmando contratos electrónicos con validez legal.

La criptografía de clave pública resuelve el problema de seguridad en las redes abiertas como Internet pero a costa de una administración de claves muy compleja. Los mensajes digitales pueden por ejemplo ser firmados digitalmente haciendo uso de una clave privada, permitiendo a cualquiera que posea la correspondiente clave publica verificar al autenticidad del mensaje, pero este principio dependerá de la autenticidad de la clave publica naciendo aquí la necesidad de contar con un método para la distribución segura de las claves publicas.

La Infraestructura de Clave Publica (Public Key Infrastructure) simplifica el problema de administración y distribución de claves pero crea un nuevo problema relacionado a la administración de la cadena de confianza (Trust). PKI hace uso de toda una estructura muy bien definida para la distribución de

las claves los que a su vez son autenticados por una autoridad de certificación (Certification Authority). Un certificado básicamente consta de la firma digital de la autoridad de certificación (emisora del certificado) junto con la identidad del propietario del certificado, sin embargo, para realizar la verificación del certificado digital se requiere contar con la clave publica de la autoridad de certificación, que como se comprenderá necesita ser autenticado, generándose nuevamente el problema de autenticación mencionado en el párrafo anterior, esta vez relacionado a la veracidad de la clave publica de la autoridad de certificación. Es obvio deducir que la clave publica de una CA puede ser certificado por otra CA y así sucesivamente pero al final de la cadena, se requerirá contar con la clave publica de la CA Raíz por medios de acceso dial haciendo uso de la PSTN o cualquier otro medio de entrega seguro que se pueda imaginar.

Sin embargo, existe un problema en este diseño, que pasa si una CA emite un certificado pero sin el chequeo apropiado de la identidad del propietario, o peor, que pasa si la CA emite deliberadamente un certificado con datos falsos, además, que pasa si por error las claves pública y privada son descubiertas al dominio público. Como se comprenderá estos eventos generaran errores en cuanto a la identificación correcta de las partes involucradas en una transacción y echan a perder todo el esquema de confianza. Nos queda claro entonces que las CA deben ser consideradas de confianza absoluta, honestos a toda prueba y que hacen su trabajo de manera apropiada. La administración de la cadena de confianza (Trus Management), incluye métodos para la implementación de políticas relacionadas a la emisión y manipulación de los certificados de claves públicas y para determinar si esas

políticas son aceptadas por los CA y los usuarios, con el propósito de realizar decisiones relacionadas a las actividades on-line.

2.1. Criptografía de Clave Pública

Cuando las personas oyen las palabras encriptación o criptografía comúnmente lo asocian a la criptografía de clave compartida, en donde, las partes que interactúan en la comunicación comparten una clave única que sirve tanto para encriptar como para desencriptar la data, como se comprenderá, la perdida o descubrimiento de esta clave es de suma gravedad toda vez que irremediablemente hace que la data encriptada será vulnerable. En contraste, la criptografía de clave pública hace uso de dos claves: Una clave Publica, diseñado para ser compartido y divulgado libremente y una clave Privada que debe conservado dentro de la más absoluta privacidad. Estas dos claves son complementarias, de modo que, si la data a ser protegida es encriptada con la clave publica, esta solamente puede ser desencriptada con su respectivo par privado y viceversa.

El sistema de clave pública depende de la relación matemática entre la clave pública y la clave privada, de modo que no es posible derivar uno de ellos conociendo el otro. Hay dos operaciones fundamentales asociados con la criptografía de clave pública: La encriptación y la Firma.

El objetivo de la encriptación es lograr hacer que la data a ser protegida carezca de significado para todo receptor que no sea el destino previamente definido. En un ambiente de clave publica, si Carlos desea enviar un mensaje privado a Manuel, el hace uso de la clave publica de Manuel para encriptarlo, y luego se lo envía. Manuel, luego de recibir el mensaje encriptado hace uso de su clave secreta o privada para desencriptar la información. El concepto más

importante aquí es el hecho de que la clave publica de Manuel puede ser libremente distribuida a cualquiera para hacer posible que cualquiera en el mundo pueda enviarle información encriptada que solamente el podrá desencriptar.

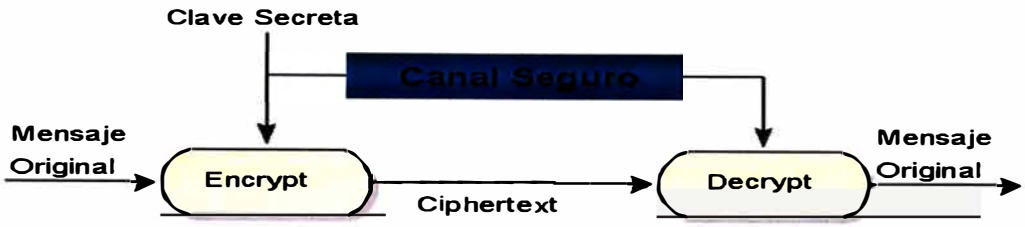


Fig. 7 Encriptación Simétrica

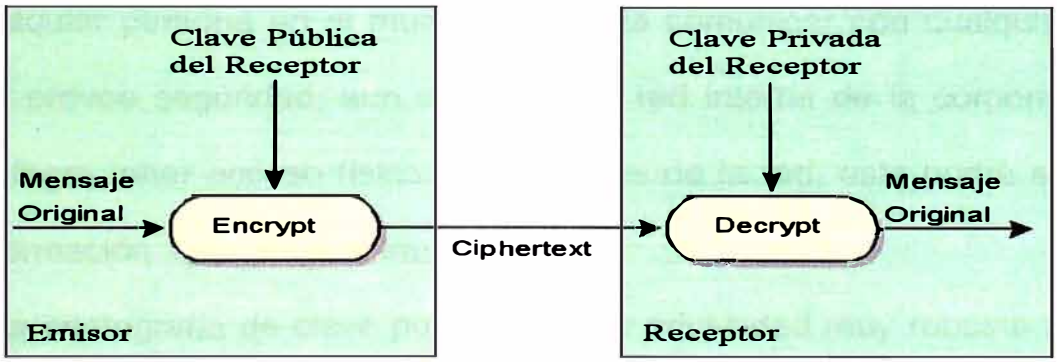


Fig. 8 Encriptación Asimétrica

La Firma, también hace uso de la encriptación, pero el objetivo en este caso es probar el origen de la data. Si Manuel desea hacer conocer al mundo que ella es el autor de un mensaje, el encriptará la información usando su clave privada para luego enviar el mensaje, como se comprenderá este

procedimiento no provee ninguna privacidad de la data toda vez que cualquiera que posea la clave publica de Manuel podrá desencriptar la información, sin embargo, el hecho de que dicho mensaje haya podido ser desencriptado haciendo uso de la clave publica de Manuel significa que este debe haber sido encriptado usando su clave privada que solamente es conocido por el, de modo que el mensaje debe provenir sin lugar a dudas de Manuel.

Estas dos operaciones pueden ser usadas para proveer cuatro capacidades muy importantes – Privacidad, Autenticación, Integridad y no repudiación – que hacen a su vez posible la seguridad distribuida y por ende el soporte de tecnologías como E-Commerce, Intranets, Extranets y otras aplicaciones de negocios basados en la web.

2.1.1. Privacidad

La privacidad es una necesidad para negocios de todo tipo, y es de importancia vital para aquellos que hacen uso de Internet, Internet hace posible que cualquier persona en el mundo se pueda comunicar con cualquier otro, pero no provee seguridad, aun dentro de la red interna de la corporación, si alguien logra tener acceso físico a los medios de la red, este podrá saber de toda información que viaja a través de el.

La criptografía de clave publica provee privacidad muy robusta a través de la encriptación de los datos, ya sea que estos estén compuestos por simples mensajes de e-mail, números de tarjetas de crédito enviados a través de Internet o cualquier trafico de la red, basándose en el principio de la libre distribución de las claves publicas y su fácil obtención para los procesos de encriptación y envió seguro de datos confidenciales a destinos previamente establecidos.

2.1.2. Autenticación/Integridad

Cualquier transacción involucra dos partes, ya sean estos el cliente y el servidor o un comerciante y el comprador. Para muchas transacciones, es deseable que la identidad de una o las dos partes de la transacción en curso sean autenticadas o verificadas. Por ejemplo, antes de que un cliente pueda proveer su numero de tarjeta de crédito a un site de e-commerce, deseara conocer que el sitio al cual esta accediendo no pertenece a un impostor. Una de las formas que el cliente puede usar para probar esto es haciendo que el Web site en referencia pruebe tener el Private Key correcto. Por ejemplo, un Web Browser puede encriptar la data haciendo uso de la clave publica de site real y enviarlo al web site en cuestión para que lo desencripte, probando de esta forma que el servidor en cuestión posee la clave secretea correcta y por tanto es quien dice ser.

La autenticación puede también cumplir la función de asegurar a las partes que la información que esta siendo transmitida no ha sido alterada (Integridad). La criptografía de clave pública hace posible esto por medio de las Firma Digital. Si Carlos desea firmar digitalmente su reporte anual de la compañía para ser luego enviado a su Jefe Manuel, el primeramente genera el equivalente de su huella digital haciendo uso del denominado “hash algorithm”. El hash algorithm se aplica sobre el mensaje que se pretende asegurar y esta específicamente diseñado para garantizar que aun un cambio mínimo de un simple bit en el mensaje generara un hash completamente diferente. Luego Carlos encriptará el reporte y el hash con su clave privada, de modo que Manuel o cualquier otro podrá verificar el origen y la autenticidad del reporte firmado y que solamente podrá ser desencriptado haciendo uso de la clave

pública de Carlos, luego Manuel generara su propia versión del hash algorithm y lo comparara con el hash algorithm que recibió de Carlos, si los dos coinciden probara dos cosas: 1) Que el reporte no ha sufrido manipulación alguna, es decir, que no ha sido modificado ni alterado y 2) Que el remitente del mismo es Carlos.

2.1.3. No Repudio

La no repudiación significa que los participantes de una transacción no están en la posición de negar su relación o su autoría en el envió de un mensaje. La no repudiación o el acto de garantizar la identidad del los miembros de una transacción es una de los beneficios directos de la infraestructura de clave pública (PKI). Las firmas digitales, las ordenes de compra electrónicas y otros acuerdos son legales en muchos países y su aceptación esta en franco crecimiento.

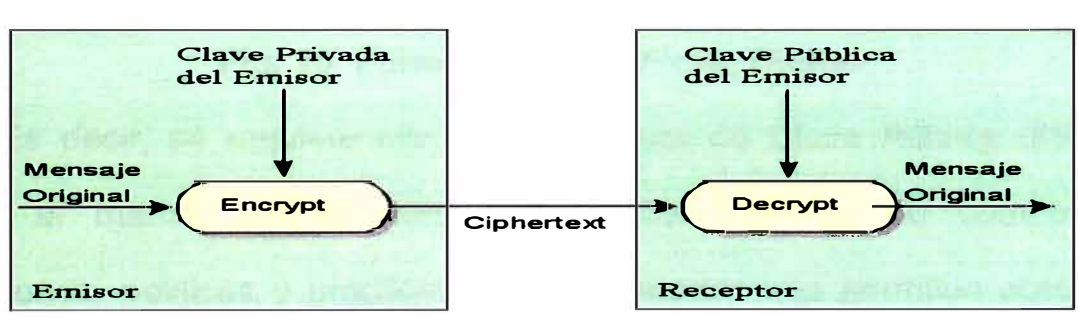


Fig. 9 Firma Digital

Sin embargo, a pesar de todas las bondades antes mencionadas, la criptografía de clave pública no es suficiente por si misma para recrear en el mundo online (comercio electrónico) las condiciones del comercio tradicional basado en el contacto directo de las partes, de modo que son necesarias además:

- Políticas de Seguridad para la definición de reglas bajo las cuales deben operar los sistemas de encriptación.

- Sistema (software/hardware) de generación, almacenamiento y administración de las claves.

- Procedimientos para la generación, distribución y uso de las claves y certificados digitales.

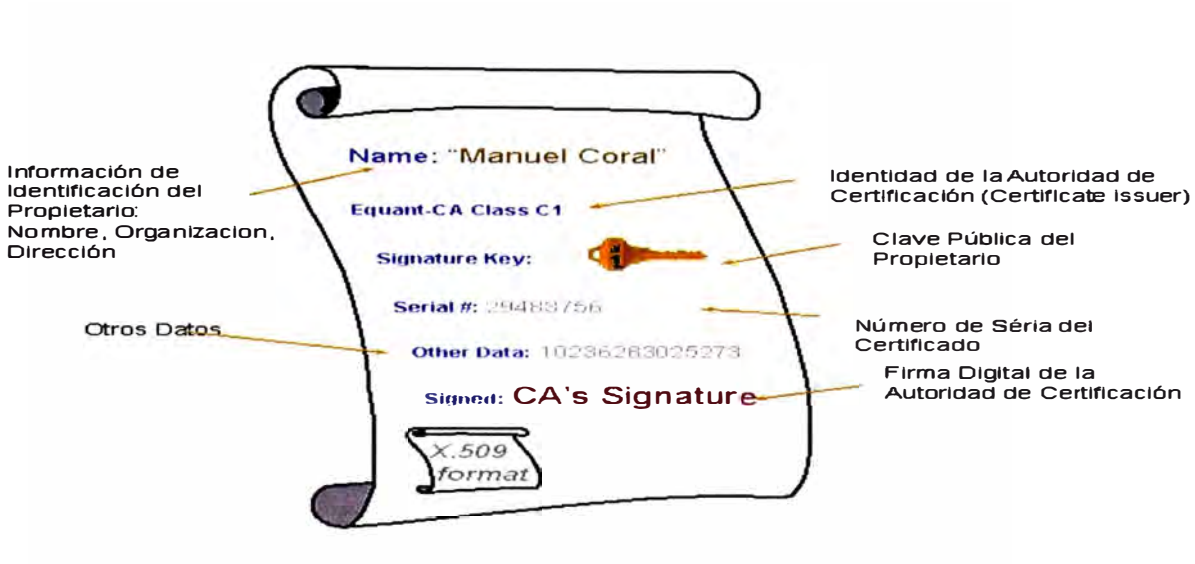


Fig. 10 Formato de una Firma Digital

Es decir, se requiere una Infraestructura de Clave Pública (PKI). PKI provee el marco general para una amplia variedad de componentes, aplicaciones, políticas y practicas que combinados nos permiten obtener las cuatro funciones de seguridad básicas necesarias para toda transacción comercial segura: Confidencialidad, Integridad, autenticación y no repudiación.

2.2. Componentes de la PKI y sus funciones

La Infraestructura de Clave Publica, es una combinación de productos de hardware y software, políticas y procedimientos que proveen la seguridad básica requerida en el mundo de los negocios online (Comercio Electrónico) de modo que los participantes de la misma, quienes no se conocen

previamente, o están localizados remotamente el uno del otro se puedan comunicar de manera segura a través de las cadenas de confianza soportadas a implementadas por la PKI.

Tabla 1: Descripción de las Funciones del PKI

Funciones	Descripción	Implementación
Registro de usuarios	Recolectar Información del usuario	Función de la CA o una RA separada
Emisión de Certificados	Creación de certificados en Respuesta a un requerimiento administrativo	Función de la CA
Anulación de Certificados	Crear y publicar el CRL (Certificate Revocation List)	Software Administrativo asociado con la CA
Almacenamiento y extracción de los Certificados y la lista de los Certificados anulados	Habilitar convenientemente los Certificados para los usuarios autorizados	La base de datos para los certificados y los CRL es usualmente segura replicada y accesible vía LDAP
Administración del ciclo de vida de las claves	Actualizar, archivar y restaurar claves	Automatizado en Software o realizado manualmente

La infraestructura de clave publica esta basado en las "Digital IDs" mas comúnmente conocidos como "Certificados Digitales", los cuales tienen la equivalencia de un pasaporte electrónico y tienen como función básica y fundamental el asociar de manera biunívoca la firma digital y la clave pública de una entidad (persona o institución). La infraestructura de clave pública (PKI) consta de los siguientes componentes:

- Política de Seguridad
- Autoridad de Certificación (CA)
- Autoridad de Registro (RA)

- sistema de Distribución de los Certificados
- Aplicaciones con soporte PKI.

2.2.1. Política de Seguridad

Una Política de Seguridad establece y define las directrices de mal alto nivel de la seguridad de la información de las compañías u organizaciones, así como los principios y procedimientos para el uso de la criptografía. Típicamente, estas políticas incluirán las pautas de cómo la organización manejara las claves e información valiosa así como también establecerá el nivel de control requerido para cumplir con los niveles de riesgos establecidos.

"Certificate Practice Statements (CPS)" - Algunos PKI son operados por autoridades de certificación comerciales (Commercial Certification Authorities : CCA) o por terceras entidades de confianza (Trusted Third Parties), y en consecuencia requieren un CPS. El CPS es un documento detallado que contiene los procedimientos operacionales de cómo las políticas de seguridad serán reforzadas y soportados en la practica, típicamente este documento incluye definiciones de cómo constituir y operar una CA, como los certificados son emitidos, aceptados y revocados y como las claves serán generadas, registradas, certificadas, almacenadas y puestas a disposición de los usuarios.

2.2.2. Autoridad de Certificación (CA)

El sistema de Autoridad de Certificación es la base de confianza de la PKI ya que este administra directamente los certificados digitales de las claves públicas en todo su ciclo de vida, de ese modo la Autoridad de Certificación tendrá potestad de:

- Emitir certificados asociando la identidad del usuario o sistema a una clave publica con una firma digital.

- Programar la fecha de expiración de los certificados.
- Asegurar que los certificados han sido revocados cuando sea necesario en base a su publicación en la lista de los certificados revocados (Certificate Revocation List: CRL).
- Cuando se implementa una PKI, una organización puede operar su propio sistema de CA, o hacer uso del servicio CA de una CA comercial o de una tercera entidad de confianza.

2.2.3. Autoridad de Registro (RA)

La función principal de una Autoridad de Registro es proveer la interfase entre el usuario y la CA. La RA tiene como tarea fundamental autenticar la identidad de los usuarios e ingresar el requerimiento de certificación a las CA. La calidad de este proceso de autenticación determina el nivel de confianza que se depositara en el certificado que finalmente será emitido por la CA.

2.2.4 Sistema de Distribución de Certificados

Los certificados pueden ser distribuidos en una variedad de maneras dependiendo de la estructura del ambiente PKI. Por ejemplo, puede ser distribuido por el mismo usuario, o a través de servicios de directorios que pueden ya existir dentro de una organización o podrán implementarse para soportar la solución PKI.

2.2.5. Aplicaciones con soporte PKI

La infraestructura de clave publica es un medio que tiene como objetivo la provisión de un marco de seguridad por medio del cual las aplicaciones con soporte PKI pueden ser desarrollados de manera confiable para la obtener los beneficios de seguridad deseados. Ejemplos de aplicaciones con soporte PKI son:

- Comunicaciones Web cliente servidor.

- E-mails.

- Intercambio electrónico de datos (EDI)

- Transacciones electrónicas a través de Internet (Comercio Electrónico)

- Redes privadas virtuales (VPNs)

2.3. Infraestructuras de Clave Pública

Como hasta ahora hemos descrito, los usuarios de Internet no pueden determinar la identidad de la entidad remota basados en los rostros o voces familiares, lo cual significa que, de primera mano cualquier información recibida de manera electrónica no puede ser confiable. De ese modo tenemos que la combinación de los certificados digitales de las claves públicas y la criptografía de clave pública son el único medio hasta hoy conocido para autenticar la identidad y el origen del mensaje.

2.3.1. Cadenas de Certificación y el estándar X.509

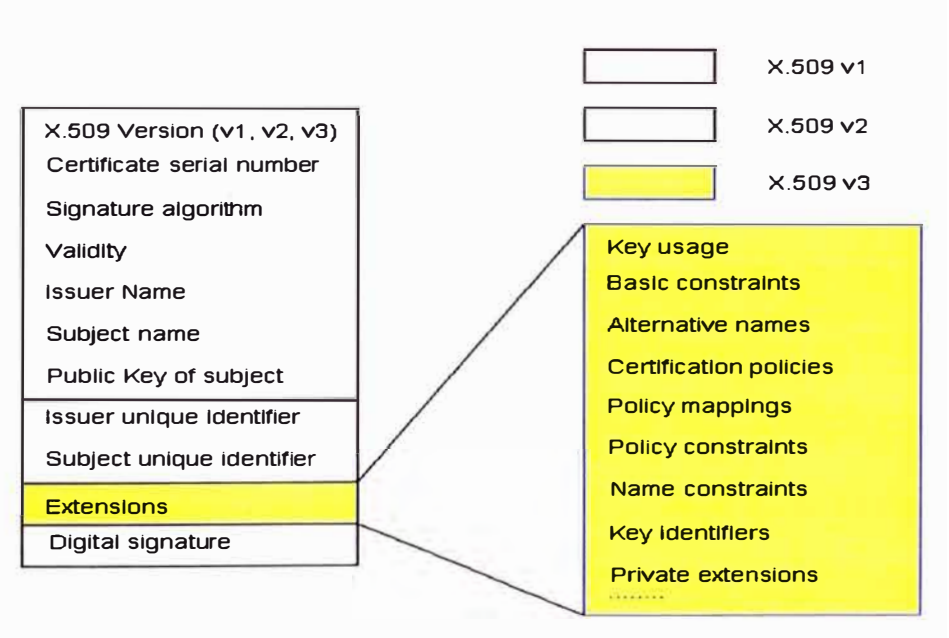


Fig. 11 Certificado X.509 y sus extensiones

Es la primera especificación estándar del Protocolo de Certificación y que fue diseñado por el CCITT/ITU y fue denominado el sistema de autenticación X.509v1, el propósito fundamental de este sistema de certificación fue proveer de seguridad al sistema de directorios X.500 y propuesto para trabajar con una jerarquía de autoridades de certificación.

Desarrollos posteriores del X.509v1 llevaron a obtener el X.509v2 y el X.509v3 los cuales añaden mejoras y resuelven algunas debilidades reportadas en la primera versión. Actualmente el estándar X.509v3 se constituye como la base de desarrollo del grupo de trabajo IETF PKIX el cual tiene como objetivo fundamental el desarrollo de una infraestructura de clave publica de propósito general para Internet. El formato de los certificados X.500 es ilustrado en la figura Nro 11

Es importante hacer notar que el sistema de directorios X.500 nunca fue adoptado por la Comunidad Internet debido a que este y su correspondiente protocolo de acceso a directorios (Directory Access Protocol: DAP) fueron catalogados como muy complejos para poder ser de utilidad para cualquier usuario común y corriente de Internet. En su lugar LDAP (Lighweight Directory Access Protocol) que es un protocolo relativamente más simple para la actualización y búsqueda de directorios sobre TCP/IP fue adoptado y ampliamente difundido.

El estándar X.509 es frecuentemente muy abierto en sus definiciones, lo cual significa que para la implementación de un sistema de manejo de certificados en el mundo real requiere la especificación de un perfil X.509 mas preciso. Debido a que el formato original del X.509 fue especificado para cumplir con las normas del X.500 en desuso hoy en día, el formato contiene un

número de campos más o menos redundantes, es así que podemos definir que los únicos campos necesarios son "Validity", "Public Key" y la "Digital Signature". "Issuer name" y "Subject name" son todavía usados, pero son interpretados como nombres generales y no como entradas en el directorio, aparte de todo lo demás que se puede encontrar en el "Extensión Part".

Para que dos usuarios puedan verificar la autenticidad de las claves publicas el uno del otro, es suficiente que exista un "certification path" entre ellos, definiendo el "certification path" como una secuencia ordenada de certificados que junto con la clave publica del certificado original en el path puede ser procesado para obtener la clave publica del ultimo certificado en el path

Las reglas de validación de los "certification paths" son realmente complejos dependiendo de cual extensión esta presente en el certificado.

2.3.2. Jerarquías de certificación

La certificación entre los nodos es dirigida por la entidad emisora de la certificación. La certificación es unidireccional cuando un agente X certifica la clave publica para otro agente Y, y es bidireccional cuando los agentes X e Y certifican sus claves publicas el uno del otro. En la jerga del PKI el termino "certificando a un usuario" significa "Certificando la Clave Publica del usuario". Las cadenas de certificación pueden formar diferentes topologías a saber.

Jerarquía estricta:

La mayoría de las implementaciones PKI son de jerarquía estricta, los mismos que normalmente consisten de uno o dos niveles. En este modelo el "certification path"va estrictamente desde el CA root, eventualmente vía CA's intermediarios y finalmente a los usuarios, en donde se asume que los usuarios

son certificados por el CA de la última rama.

En una jerarquía estricta todos los usuarios pueden ser identificados y localizados fácilmente debido precisamente a la estructura jerárquica. Un usuario deberá conocer la clave publica del CA root para poder resolver la cadena y establecer así una cadena de certificación a cualquier usuario en la jerarquía.

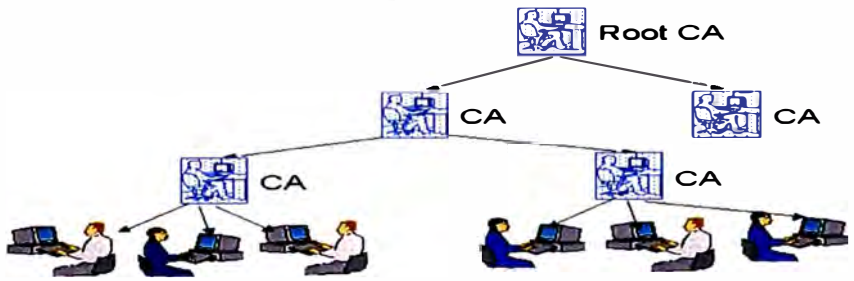


Fig. 12 Jerarquía estricta

Jerarquía General:

Una jerarquía general incluye certificaciones bidireccionales entre los CA's.

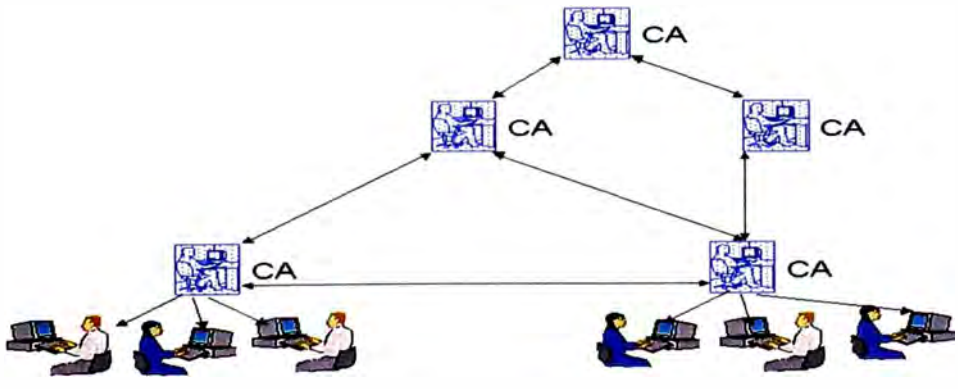


Fig. 13 Jerarquía General

Cuando la certificación se establece en ambas direcciones, cada usuario solamente requerirá obtener una copia autentica de la clave publica del CA mas cercano el cual podrá usar para obtener o establecer el "certification path" a cada usuario de la red. Es importante hacer notar que el estándar X.509 propone esta jerarquía general, pero que ninguna PKI comercial hace uso de esta topología.

PKI anárquico:

Lo opuesto a una jerarquía estructurada es una estructura anárquica en el cual cada CA (y usuario) es libre de elegir a cuales otros CA's (y usuarios) el desea certificar.

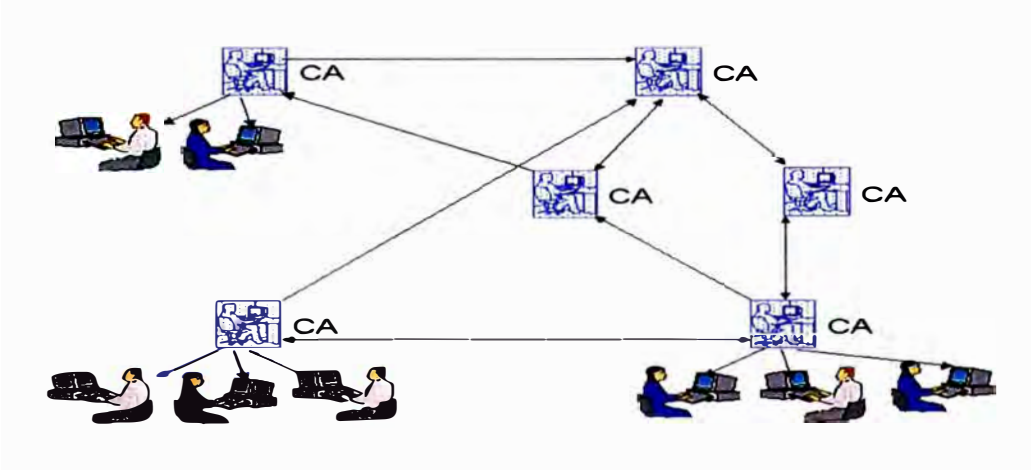


Fig. 14 PKI anárquico

La estructura anárquica corresponde al "Web of Trust" en el cual esta basado el PGP. Este consiste de certificaciones unidireccionales y bidireccionales entre agentes arbitrarios, aquí en principio no existe diferencia entre usuarios y CAs, la desventaja de una jerarquía anárquica comparada con una jerarquía estructurada es la no existencia de un algoritmo simple de identificación de los "certification path" entre los diferentes usuarios de una red anárquica, como si lo hay para el caso de las redes jerárquicas. En conclusión, bajo este esquema de jerarquía anárquica, el usuario deberá obtener tantas

claves públicas como pueda para poder de ese modo establecer cadenas de certificación a otros usuarios.

Jerarquías aisladas:

Realmente, muchas PKI pueden coexistir en paralelo sin la necesidad de relación el uno del otro, el usuario deberá obtener la clave pública root de cada PKI para de ese modo poder verificar el certificado de los usuarios de cada jerarquía, los usuarios que pertenecen a una jerarquía con root desconocido no pueden ser identificados.

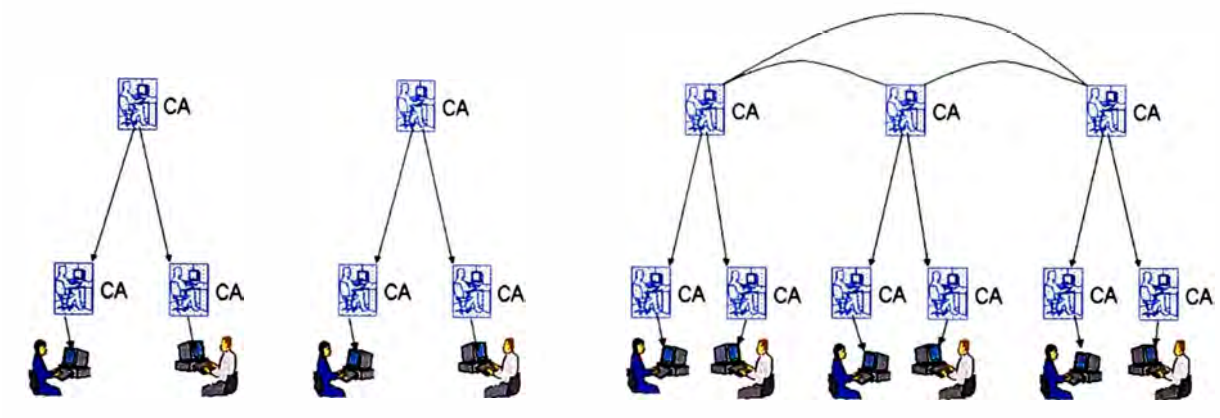
Un ejemplo clásico de este tipo de jerarquía aislada es el PKI usado para la Web, en donde las claves publicas de los Roots son almacenados codificados dentro de los Browsers, de entre ellos los más conocidos, Netscape 4.6 e IE 5.0 que ya incluyen dentro de su distribución una lista de 50 claves publicas root de los CA mas conocidos.

Jerarquías de Certificación Cruzada:

En contraste a la jerarquía anteriormente descrita, esta jerarquía no requiere que el usuario obtenga muchas claves publicas de los root CA ya que permite que exista una certificación cruzada entre ellos, de modo que será necesario que el cliente cuente con solamente la clave pública de su propio root para poder de ese modo verificar la validez de cualquier certificado aun cuando este no pertenezca directamente su jerarquía particular.

La certificación cruzada entre PKIs simplifica de manera considerable la distribución de las claves públicas de los Roots CA, haciendo que el PKI sea completamente abierto. El único inconveniente que se opone al desarrollo de estos CAs es que generalmente tiene políticas incompatibles cuando para el cross certification es necesario contar con un buen acuerdo entre ellos. En este

punto es importante hacer notar que este tema de coincidencia de políticas de los PKI esta en gran medida en manos de los Gobiernos.



(a) **(b)**

Fig. 15 Jerarquías aisladas(a), Jerarquías de Certificación Cruzada (b)

2.3.3. Administración de la PKI

Hasta ahora nos hemos avocado al aspecto criptográfico de la PKI, pero es necesario también considerar todo esa infraestructura requiere de una administración, de modo que en lo que sigue haremos una descripción de las técnicas de administración de las PKI mas conocidas.

Web PKI:

Para el caso de las "Web PKI", las Root Public Keys se encuentran codificadas en dentro del mismo Web Browser como certificados X.509v3 "self signed", es decir que la clave publica ha sido certificado por su correspondiente clave privada, el único propósito de realizar un "self certification" es para simplificar el tratamiento de los certificados. Realmente los "self certification" no añaden mayor confiabilidad a las claves públicas, y como su propio nombre lo indica el "self certification" puede ser falsificado.

Como los Root Certificates están codificados dentro del Browser no

pueden ser fácilmente actualizados, pero estas actualizaciones no necesariamente varían de distribución en distribución de estas aplicaciones, sino que también el cliente puede realizarlas. La aplicación mas popular para el establecimiento de conexiones encriptadas en el SSL, otra aplicación popular es el e-mail encriptado basado en el estándar S/MIME el cual en simples palabras realiza una encriptación digital del cuerpo del mensaje. La tercera aplicación es para la firma digital de los componentes de Software, el cual tiene mucha importancia para asegurarnos que no estamos tratando con código de software peligroso, por ello la única manera en que esta inseguridad puede ser resuelta en los Web Browsers es teniendo los componentes formados digitalmente por el fabricante del software.

Managed PKI:

En contraste al Web PKI, el managed PKI no distribuye los Root Public Keys dentro de los Browsers, pero esta basado en procedimientos de acceso out-of-band administrados por organizaciones que operan el PKI. Estas organizaciones normalmente administran las CA servers desde el cual se pueden bajar los certificados de los usuarios. Los "Managed PKI" son operados por organizaciones que tiene el control total de las estructura de confianza de la jerarquía PKI.

Las organizaciones que operan las PKIs, pueden decidir hacer, o estar obligados por alguna ley del país en cuestión a establecer cross-certificación con otros managed PKI para de ese modo crear una PKI consistente de muchas jerarquías de certificación entrelazados.

La distribución segura de las claves publicas es de importancia capital para los managed PKI, y una típica solución es equipar a cada equipo de

cliente con una tarjeta “smart card” conteniendo la clave privada del usuario adicionalmente al root public key.

2.4. Como trabajan las aplicaciones con PKI

La infraestructura de clave publica administra las claves y los certificados digitales usados para implementar la encriptación dentro de aplicaciones como e-mail y mensajería, web browsers y servidores web, Electronic Data Interchange (EDI); en aplicaciones que establecen transacciones seguras haciendo uso del web o en implementaciones VPN haciendo uso del S/MIME, SSL y IPSec; y en funciones como documentos digitalmente firmados.

E-mail y Mensajería:

Las aplicaciones de e-mail y mensajería seguros hacen uso de pares de claves para la encriptación de mensajes y files, así como para las firmas digitales. Así tenemos por ejemplo aplicaciones como Microsoft Exchage y Notes de IBM que hacen uso de la encriptación para transportar información confidencial. Lo mismo es verdadero programas de mensajería como programas groupware tales como Novell’s GroupWise. De la misma forma los sistemas EDI que soportan transacciones financieras, requieren de: Autenticación, privacidad e integridad de datos.

El protocolo de e-mail / mensajería mas conocido es el Secure Multipurpose Internet Mail Extensions (S/MIME), el cual es una extensión del protocolo MIME.

Web Access:

Los Browsers y los servidores Web hacen uso de la encriptación para autenticación y confidencialidad, y para aplicaciones como home banking y compras en línea. Típicamente haciendo uso del SSL (Secure Socket Layer),

los servidores se autentican por si mismo a los clientes. SSL también encripta trafico, la encriptación del cliente también es una opción. La gran ventaja de SSL es que no esta limitado al HyperText Transfer Protocol (http) sino que también soporta protocolos como File Transfer Protocol (FTP) y Telnet.

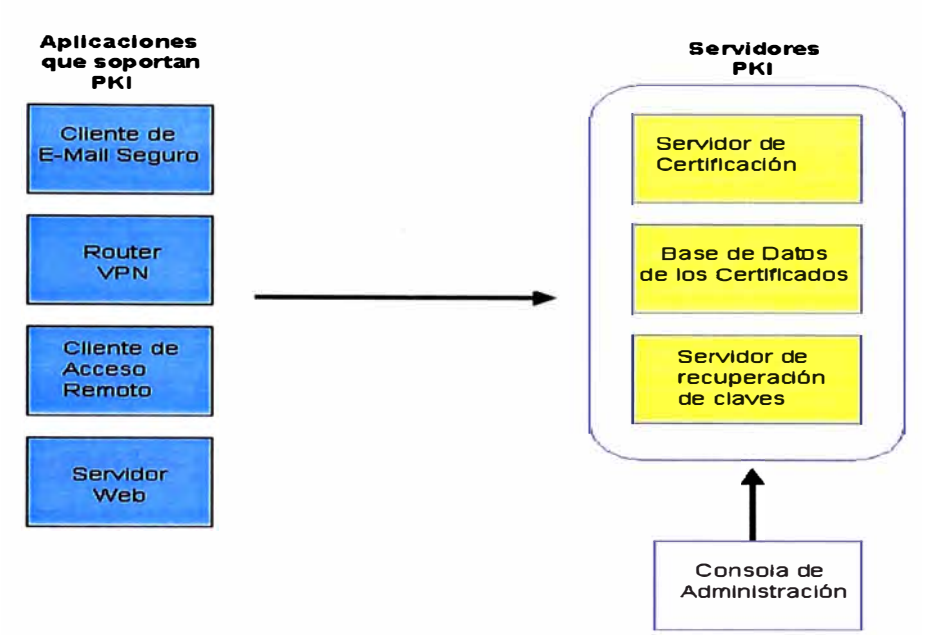


Fig. 16 Aplicaciones soportadas por PKI

VPN:

La encriptación y la autenticación son las principales tecnologías usados para convertir las link estándar de Internet en VPNs (Virtual Private Networks, usados para privacidad site-to-site (router-to-router) o para acceso remoto seguro (Client-to-Server). Estas funciones están implementadas en el contexto de los protocolos de tunneling que envuelven (o encapsulan) un protocolo dentro de otro protocolo. Por ejemplo, el protocolo encapsulado puede ser el protocolo point-to-point (PPP), mientras que el protocolo que encapsula puede ser el Protocolo Internet (IP). El estándar emergente hoy en día para el establecimiento del tunneling site-to-site es el protocolo IP Security (IPSec) del IETF.

Documentos Digitalmente Firmados:

El incremento de la necesidad de confiabilidad de los programas "bajados de Internet" ha generado preocupaciones con relación a la seguridad particularmente en el control de virus. Tecnologías como Microsoft's Authenticode hacen uso de las firmas digitales RSA™ para verificar la fuente y la integridad del contenido. Una PKI es utilizada para ampliar esta solución para un número muy amplio de usuarios y aplicaciones que requieren estos servicios.

2.5. PKI y Estándares relacionados

Los estándares en el campo la Infraestructura de Clave Publica caen dentro de dos grandes grupos: Aquellos que "definen el PKI", y los estándares de nivel de usuario que hacen uso del PKI pero no lo definen.

2.5.1. Estándares que definen el PKI

Los estándares PKI permiten que múltiples PKI puedan ínter operar, y que muchas aplicaciones puedan hacer interfaces con un único y consolidado PKI.

En particular los estándares son necesarios para:

- Procedimientos de Registro (enrollment procedures).
- Formato de los certificados.
- Formato de los CRL.
- Formatos para los mensajes de registro de certificados
- Client Requests
- Cerficate
- Server issues certificate
- Formato de las Firmas Digitales.

- Formatos de Invitación / respuesta

El principal grupo que trabaja en la interoperatibilidad del PKI es el IETF Working Group conocido como PKIX Group (PKI que hace de los certificados con formato X:509).

PKIX:

Los cuatro componentes básicos de un modelo PKIX son:

- El usuario (o entidad final).
- La Autoridad de Certificación (CA).
- La Autoridad de Registro (RA).
- La base de datos (Repository).

Componentes Estándar del PKIX:

Las especificaciones del PKIX están basadas en otros dos estándar: X:509 de la International Telecommunication Union (ITU) y los estándar de Criptografía de Clave Publica (PKCS) del RSA Security. X.509 fue diseñado para los servicios de autenticación de los servicios de directorio X.500, de hecho, la sintaxis de los certificados X.509 han sido ampliamente adoptados también fuera del ámbito X.500, sin embargo X.509 no fue diseñado para definir un sistema PKI 100% ínter operable, es por ello que vendedores, usuarios y comités de estandarización han tomado como base de su desarrollo a los estándar PKI definidos en el PKCS.

X.509: El estándar universalmente soportado por los estándares PKI es el X.509 de ITU. Cuyo propósito principal es definir el formato estándar de los certificados Digitales

PKCS: PKCS es en realidad una colección de estándares que cubren áreas de PKI como: Registro de certificados y su renovación, y la distribución del

CRL. Los tres estándares más importantes para la Interoperatividad del PKI son:

- PKCS #7: "Cryptographic Message Syntax Standard"
- PKCS #10: "Certificate Request Syntax Standard"
- PKCS #12. "Personal Information Exchange Syntax Standard"

Tabla 2: Los principales componentes del modelo PKIX

Componentes	Parte de PKI	Descripción
Usuario	NO	Usuario de certificado PKI y/o Sistema a nivel de usuario sujeto de certificación.
Autoridad de Certificación (CA)	SI	Emite, almacena y revoca certificados
Autoridad de Registro (RA)	SI	Sistema opcional al cual un CA delega ciertas funciones de administración como registro de usuarios.
Base de Datos (Repository)	SI	Sistema o conjunto de sistemas distribuidos que almacenan y permiten que entidades finales (Usuarios Finales) puedan acceder a los certificados y los CRL.

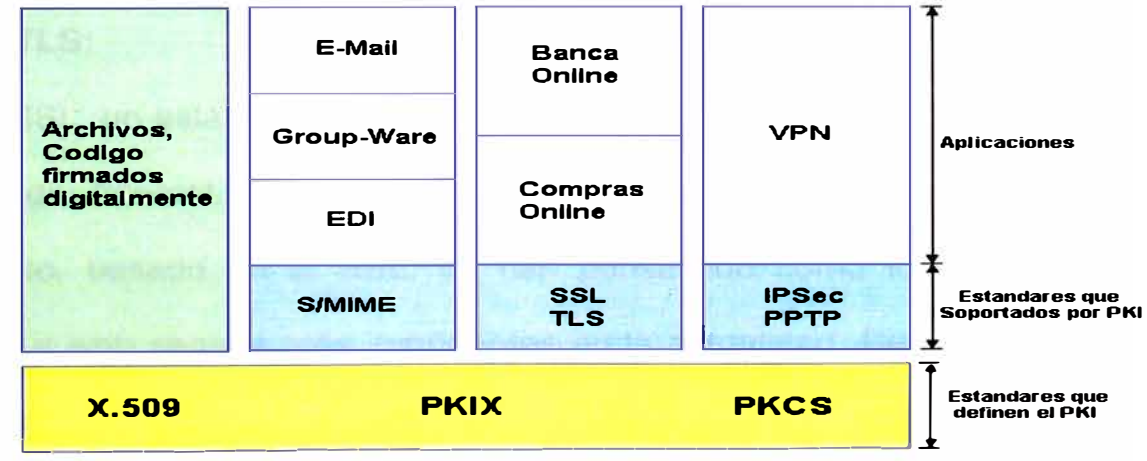


Fig. 17 Estándares PKI

2.5.2. Estándares que hacen uso de PKI

La mayoría de los estándares de seguridad actuales están diseñados para tener soporte PKI, por ejemplo, SSL (Secure Socket Layer), TLS (Transport Layer Security), Secure Multipurpose Internet Mail Extensions (S/MIME), Secure Electronic Transaction (SET) y IPSec (IP Security), todos ellos asumen, requieren o permiten el uso de PKI.

S/MIME:

Es el estándar de envió de mensajes seguros mas conocido, propuesto por el IETF, S/MIME hace uso del PKI para la firma digital de los mensajes y para soportar la encriptación de los menajes y los files añadidos. El comité S/MIME, considerando al E-mail como uno de las aplicaciones Internet mas maduras, le ha permitido la implementación y ampliaciones al estándar PKI, haciendo uso de las ventajas del PKIX y completando los vacíos de estandarización donde sea necesario. Así tenemos que los estándares más importantes desarrollados por el comité S/MIME son: Cryptographic Message Syntax, Message Specification, Certificate Handling y Certificate Request Syntax.

SSL y TLS:

SSL, un estándar IETF, que cuenta con una popularidad muy grande en el mundo Internet, lo mismo el TLS pero en menor dimensión hasta el momento, basado en el SSL, se han constituido como los estándares de acceso a web servers más importantes en la actualidad. Realmente SSL/TLS tiene una utilidad general para accesos cliente/servidor seguros en una gran variedad de aplicaciones NO Web, todos ellos basados en los certificados PKI asociados a los clientes y servidores.

SET (Secure Electronic Transaction):

SET facilita las transacciones electrónicas seguras que hacen uso de tarjetas de crédito en base al uso de claves para la autenticación, confidencialidad e integridad de los datos. PKI se constituye de este modo en una parte critica del proceso de autenticación de las dos partes que intervienen en una transacción haciendo que esta sea 100% segura.

IPSec:

El estándar IPSec (estándar IETF: Internet Protocol Security Protocol), define los protocolos para la encriptación IP, es uno de los protocolos principales usados como soporte de las VPNs, IPSec requiere de claves para la autenticación y la encriptación. Actualmente se tiene estándares completos de PKI para IPSec en desarrollo, aun cuando IPSec es algo limitado, PKI se constituye en su mejor soporte para su crecimiento futuro.

CAPÍTULO III
IPSEC & SSL

En sus primeros días, Internet fue del dominio de académicos e investigadores, de modo que su objetivo principal era maximizar las comunicaciones sobreponiéndose a todas la barreras tecnológicas de esos tiempos, pero a finales de los 80's era evidente para muchos que algunos usuarios estaban abusando de las capacidades de la red para leer, modificar transmisiones ajenas generando, eventualmente, que algunos servicios de Internet sufrieran fallas de modo que la seguridad de las transmisiones a través de Internet desde aquellos días a la fecha ha sido y sigue siendo punto de debates y muchas controversias constituyéndose en una de las áreas con mayores avances dentro del mundo On-line. Dos tipos de soluciones han emergido a la fecha para poder contrarrestar estos problemas de seguridad en Internet a saber: Soluciones Localizadas y Soluciones especialmente diseñadas para cada tipo de aplicación. Las soluciones localizadas son intentos de los administradores de la red de aislar toda o parte de su red a los accesos no autorizados y son lo que actualmente conocemos como: Screening Routers, Firewalls, Defensive Scanners y la eliminación de los huecos de seguridad en los Sistemas Operativos y programas. Las soluciones especialmente diseñadas para cada tipo de aplicación, son las aplicadas específicamente a las aplicaciones, tales como e-commerce, e-mails. Con el paso del tiempo, se hizo evidente que estas técnicas no eran generales y que la forma mas eficiente de

garantizar seguridad para el trafico Internet es hacer que los servicios de seguridad debieran estar directamente añadidos al protocolo Internet (IP), es de este modo que en 1992 la IETF inicia este proyecto denominado IPSec. Lo que diferencia a IPSec con relación a otras soluciones es que IPSec intenta hacer uso de las técnicas criptográficas pero de modo mas global para resolver los problemas de seguridad en Internet en lugar de buscar soluciones individuales para cada tipo de aplicación (como son: soluciones para sistemas de e-mail, web browsers, etc.); IPSec realmente involucra un cambio a las facilidades existentes de la estructura de redes actuales que son usadas por cada aplicación, posibilitando esto que los administradores de redes puedan proteger sus redes transparentemente a sus usuarios finales.

En términos generales IPSec puede proveer todos o parte de los siguientes tipos de protección:

Connectionless Integrity: Lo cual garantiza que el mensaje a ser recibido sea exactamente el que se envió y que ninguna modificación del mismo tuvo lugar durante su transmisión. Y por que NO Orientada a la conexión?, esto es debido a que las comunicaciones en Internet están basadas en el protocolo IP, el cual es un protocolo NO orientado a la conexión.

Data Origin Authentication: El cual garantiza que el mensaje fue realmente enviado por el que dice ser el remitente del mismo, y no por otro que se hizo pasar por el.

Replay Protection: Asegura que un mismo mensaje no sea enviado varias veces y que el mensaje no sea enviado sin orden, esta opción deberá ser implementada por el sender (remitente) y es opcional para al receptor (receiver).

Confidentiality or Privacy: Garantiza que, si aun el mensaje es "leído" por un agente externo (Hacker), el contenido no será comprensible, excepto claro esta para el receptor autorizado.

Traffic Analysis and Protection: Asegura que cualquier problema de ruptura de seguridad no rebelara el remitente ni el destinatario de la comunicación así como tampoco el volumen de tráfico que ambas entidades están intercambiando.

3.1. IPSec, Conceptos Fundamentales

IPSec es un estándar desarrollado por la IETF, diseñado para proveer interoperatividad, alta calidad, seguridad basada en técnicas criptográficas para asegurar las transmisiones de datos soportados en IP, tanto en la versión actual IPv4 así como IPv6 . Estos servicios son provistos sobre la capa IP, ofreciendo protección para el IP y/o protocolos de más alto nivel.

IPSec es valido para la versión IPv4 e IPv6. Esta comprendido por un conjunto de protocolos los cuales aseguran completamente las comunicaciones entre dos estaciones IP, asegurando:

- User Authentication
- Data Authentication
- Data Confidentiality
- Data Integrity

IPSec administra esta seguridad, paquete por paquete por medio protección no orientadas a la conexión, en contraste con los servicios L2F, L2TP y PPTP los cuales con orientados a la conexión. La encapsulación de protocolos NO-IP haciendo uso de los túneles IP permite / asegura el transporte seguro de otras aplicaciones de Internet.

IPSec, para cumplir con los objetivos antes mencionados, hace uso de dos protocolos de seguridad a saber: El Authentication Header (AH) y el Encapsulating Security Payload (ESP) así como también de otros procedimientos y protocolos de administración de las claves de encriptación.

3.2. Authentication Header(AH), Encapsulating Security Protocol(ESP)

IPSec define dos protocolos de seguridad; cada uno de los cuales tiene su propio formato de cabecera. En ambos casos la cabecera es insertada justo después de la cabecera IP.

Para el caso específico del Authentication Header(AH), este provee de: Una mixtura de Connectionless Integrity y Data Origin Authentication (estos dos servicios serán mas adelante referidos como servicios de Autenticación) y un servicio opcional de Anti-Relay.

Este protocolo de Seguridad no provee de servicio de encriptación. AH tiene una gran utilidad y de común aplicación en casos en los que la confidencialidad no es requerida.

El Encapsulating Security Payload(ESP) puede opcionalmente proveer: Autenticación, servicio Anti-Replay y Confidencialidad (a través de la encriptación). El servicio de Autenticación se aplica luego de la cabecera ESP, y no protege el Outer IP Header. Si se requiere que la autenticación se realice considerando solamente las capas superiores entonces la autenticación ESP es la elección apropiada.

A pesar de que ambos servicios, la autenticación y la encriptación son opcionales, por lo menos uno de ellos deberá ser elegido; si no se elige la opción de autenticación, se deberá elegir la opción de encriptación; si la encriptación no es elegida, se deberá elegir la opción de autenticación. Si se

elige ambas opciones, primero de realizara la encriptación y luego la autenticación; realmente AH y ESP pueden ser aplicados solos o en combinación.

3.2.1. Descripción del AH

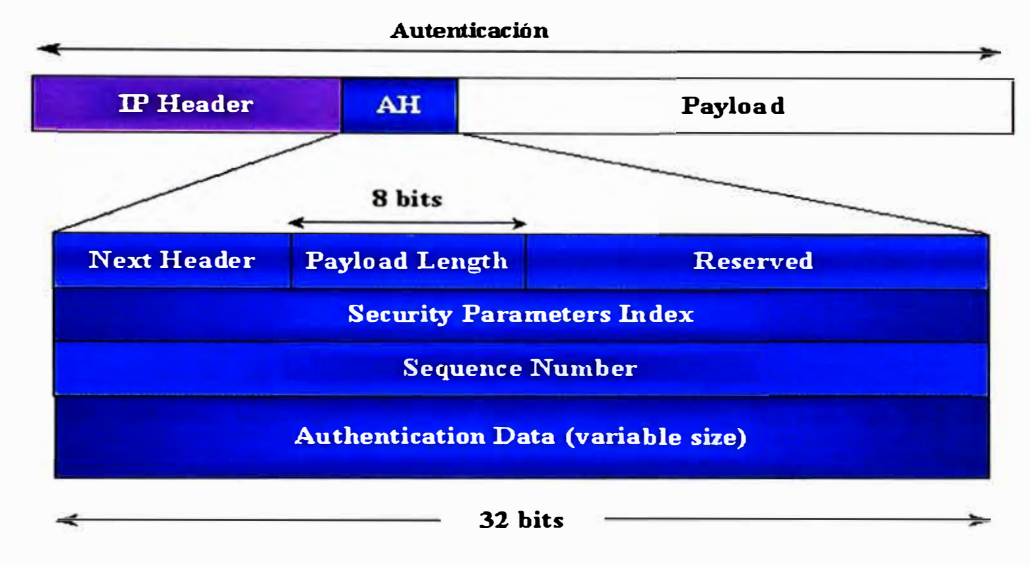


Fig. 18 Formato AH

A continuación se hará una breve descripción del Authentication Header, cualquier desarrollo minucioso de los campos que conforman el AH esta fuera del alcance de este informe.

Next Header: Campo de 8 bits que contiene información de tipo de payload luego de la cabecera AH.

Payload Length: Campo de 8 bits que contiene información acerca de la longitud de la cabecera AH.

Reserved: Reservado, para uso futuro.

Security Parameter Index (SPI): Valor arbitrario de 32 bits, que en combinación con el IP de destino y el protocolo de seguridad, identifican de

manera única al Security Association para este datagrama. El valor del SPI es elegido por sistema de destino al momento del establecimiento de SA. Los valores en el rango de 1 a 255 son reservadas por la Internet Assigned Numbers Authority (IANA) para uso futuro.

Sequence Number: Campo de 32 bits conteniendo el valor de un contador que va creciendo constantemente, este campo es principal y esta casi siempre presente aun cuando el receptor no elige habilitar el servicio Anti-Relay. El numero de secuencia es inicializado en 0 en el momento en el que se establece el SA, de ese modo, el numero de secuencia del primer paquete será 1.

Authentication Data: Campo de longitud variable conteniendo al Integrity Check Value (ICV). El algoritmo usado para computar el ICV es especificado por el Security Association. Una implementación que cumple con el protocolo AH deberá soportar los algoritmos HMAC-MD5 y HMAC-SHA-1. El ICV es computado sobre el inmutable o predecible campo del Outer IP Header (Versión, IP Header Length, Total Length, Identificación, Protocol, Source and Destination Address), los campos mutables son seteados a 0 (TOS, Flags, Fragment Offset, TTL, Header Checksum)

3.2.2. Descripción de Encapsulating Security Protocol (ESP)

Security Parameter Index (SPI): Valor arbitrario de 32 bits que en combinación con el IP address de destino (outer header) y el protocolo de seguridad (AH), identifican de manera única al security association para este datagrama. El valor del SPI es seleccionado por el sistema de destino en la etapa del establecimiento del SA. Los valores en el rango de 1 a 255 están reservados por la Internet Assigned Numbers Authority (IANA) para uso futuro.

Sequence Number: Campo de 32 bits que contiene el valor de un contador que se va incrementando, este campo es obligatorio y esta siempre presente aun cuando el receptor decide no elegir el servicio anti-replay para un SA particular. El número de secuencia es inicializado a cero cuando se establece el SA. Entonces el primer paquete tendrá el número de secuencia 1.

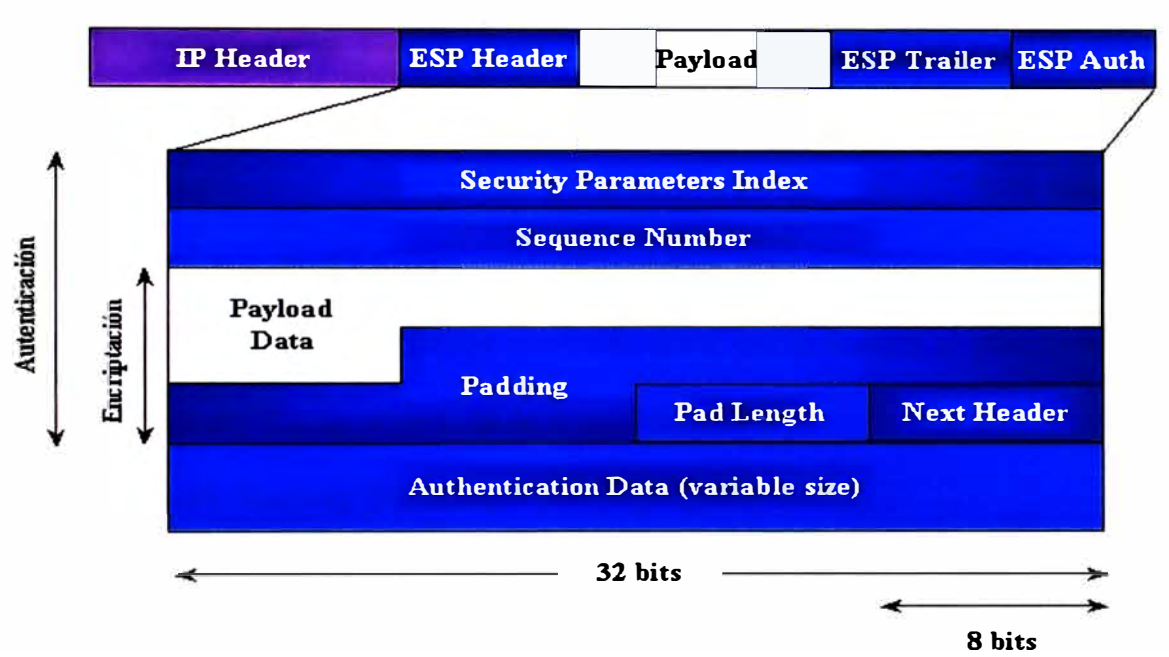


Fig. 19 Formato ESP

Payload Data: Son los datos incluidos en el paquete IP original. Se incluye un vector de inicialización al inicio del campo de payload si el servicio de encriptación ha sido seleccionado y si el algoritmo de encriptación requiere de una sincronización criptográfica.

Padding: Algunos algoritmos de encriptación requieren el plaintext para ser un número múltiplo de un tamaño de bloque. El padding es usado para llenar el plaintext hasta que se logre el tamaño apropiado. El plaintext consiste de la data de payload, el Pad Length y las cabeceras de los siguientes campos

Pad Length: Tamaño en numero de bytes del campo de Padding.

Next Header: Campo de 8 bits que contiene el tipo de data en el campo de Payload.

Authentication Data: Campo opcional de longitud variable que contiene el Integrity Check Value (ICV). Este campo esta presente solamente cuando el servicio de autenticación es especificado por el SA.

El algoritmo usado para computar el ICV es especificado por el Security Association. Una implementación compatible con ESP debe soportar los algoritmos HMAC-MD5 y HMAC-SHA-1. El ICV es computado sobre el paquete ESP menos el campo de autenticación de datos: SPI Sequence Number + Padding + Pad Length + Next Header. Si el servicio de encriptación es seleccionada, los cuatro últimos campos esta en la forma cyphertext, como la encriptación es aplicada antes de la autenticación.

3.3. IPSec Anti-Replay Service

El Anti-Replay es un servicio opcional que es ofrecido por el protocolo de seguridad ESP o AH. Este servicio puede ser elegido en la etapa de establecimiento del Security Association (SA). Por defecto este servicio esta habilitado. El servicio Anti-Replay hace uso del campo Secuence Number de la cabecera de IPSec para enumerar los paquetes. El campo de Secuence Number es de 32 bits que contiene el valor de un contador que se va incrementando y que se resetea al valor de 0 cuando se inicializa el SA. El sender incrementa el valor de contador, de ese modo el primer paquete que es enviado tiene un valor de secuence number de 1.

El sender chequea cada vez que el contador no alcance su valor máximo antes de insertar un nuevo valor en el campo del contador. Si el valor

máximo se ha alcanzado se deberá establecer una nueva negociación del SA, de modo que el servicio no deberá estar disponible si el SA es administrado manualmente. Para cada paquete entrante, el receptor chequea el sequence number para asegurar que no se duplique uno de cualquier paquete recibido durante el tiempo de vida del SA. El valor del contador siempre es registrado/llenado aun cuando el servicio anti-replay no esta habilitado. Si el servicio de anti-replay no esta activado, tanto el transmisor como el receptor no monitorean el valor del sequence number. Sin embargo este valor siempre es incrementado y receteado a cero cuando alcanza su valor máximo.

3.4. Modos de empleo del IPSec

Los protocolos de seguridad ESP y AH pueden ser empleados de dos modos:

- Transport Mode o
- Tunnel Mode.

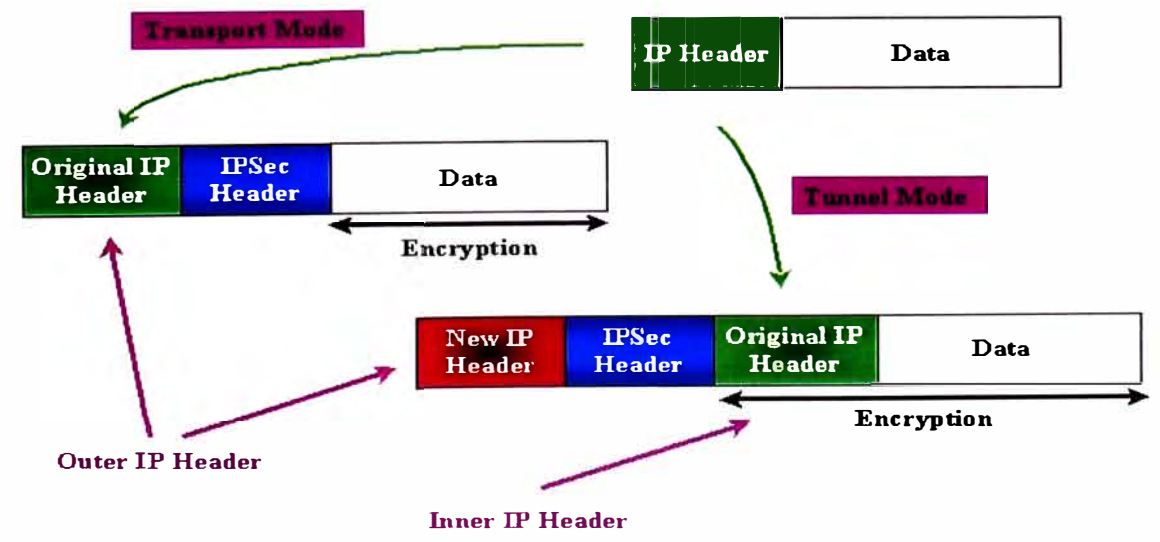


Fig. 20 Modos de empleo del IPSec

En el caso de IPSec en modo Tunnel, una nueva cabecera IP es añadida al datagrama original, de modo que el paquete original viene a convertirse en el payload del nuevo paquete. El security protocol header es insertado luego del outer IP header, y antes del inner IP header.

Las direcciones "outer IP" no necesitan ser las mismas que las direcciones "inner IP". La ventaja del modo túnel es la completa protección del datagrama encapsulado y la posibilidad de usar dos esquemas de direccionamiento:

- Uno Público (en el outer header)
- Uno Privado (en el inner header)

En el caso del IPSec en modo transporte, la cabecera original es el outer header. La cabecera del protocolo de seguridad aparece luego de la cabecera del paquete original y antes del payload.

En resumen, la ubicación de la cabecera del protocolo de seguridad, la cabecera del protocolo IPSec es insertado: después del IP header y antes de la cabecera del protocolo la capa superior (trasport mode) o antes del IP header encapsulado (tunnel mode).

3.4.1. Ejemplo de IPSec en modo de transporte

IPSec en modo de transporte es solamente aplicable a hosts y no esta disponible para gateways de seguridad. Cuando un gateway de seguridad opera en el modo transporte del IPSec esta actuando como host: El tráfico es destinado a él mismo.

En el IPSec en modo transporte, la cabecera es insertada luego de la cabecera IP y antes de las cabeceras de los protocolos de las capas superiores (por ejemplo, TCP, UDP, ICMP, etc.).

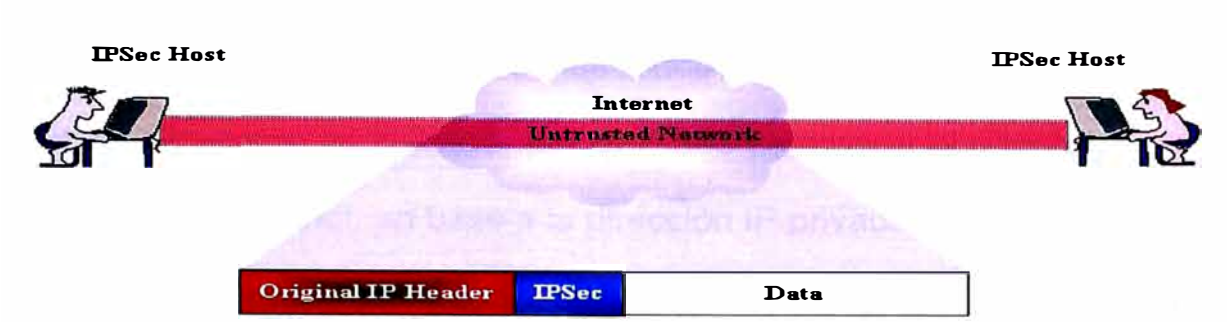


Fig. 21 IPSec modo Transporte

3.4.2. Ejemplo de IPSec en modo Túnel

IPSec en modo Túnel es aplicable a hosts y gateways de seguridad. Es importante mencionar que los gateways de seguridad soportan solamente IPSec en modo Túnel.

Las direcciones "outer IP" de origen y destino se identifican como "endpoints" del túnel. Los direcciones "inner IP" de origen y destino identifican al origen y destino originales del datagrama.

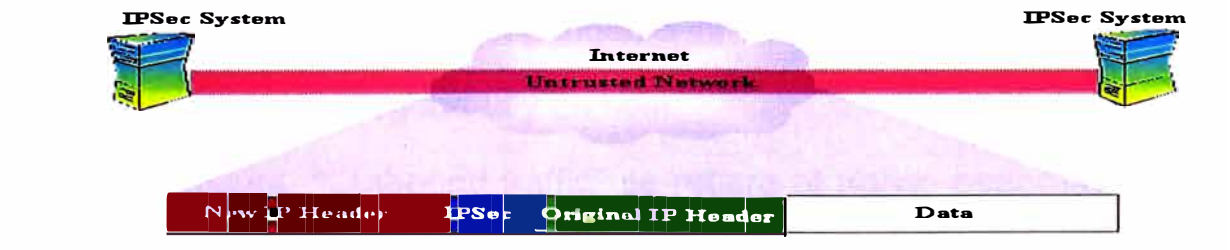


Fig. 22 IPSec modo Túnel

IPSec en modo IP tunneling permite usar direcciones IP publicas en el nueva cabecera "Outer IP", mientras se mantiene la dirección IP privada del paquete original. El nuevo paquete es enrutado dentro de la Internet de acuerdo a las políticas de ruteo de las redes IP públicas; luego la cabecera con dirección IP publico es borrada por el IPSec gateway y el paquete original es enrutado en la Intranet en base a la dirección IP privada de la cabecera.

El datagrama original no es cambiado al final del túnel excepto el campo TTL que de reducido, y el campo de checksum que es nuevamente computado debido al cambio del TTL.

3.5. IPSec systems : Host and Security Gateway

IPSec puede ser implementado en dos tipos de equipos, que de aquí en adelante denominaremos "sistemas IPSec": un host o un gateway de seguridad que es un sistema intermediario entre dos redes; un lado del gateway de seguridad es visto como no seguro, el otro lado como seguro. El gateway de seguridad implementa IPSec en la interfase "no segura" para poder de ese modo garantizar comunicaciones seguras entre hosts en la red segura y hosts en el lado de las redes no seguras.

Los servicios de seguridad pueden ser provistos:

- Entre un par de hosts.
- Entre un par de gateways de seguridad o
- Entre un gateway de seguridad y un host.

En la figura, "Outbound traffic" se refiere al trafico generado por la red segura, el cual deberá ser enviado a una red "no segura" con un protocolo de seguridad IPSec (ESP o AH). "Inbound Traffic" esta referido a trafico recibido

de la red no segura con protección IPSec, el cual a su vez deberá ser enviado a una red segura o insegura (con o sin un protocolo de seguridad).

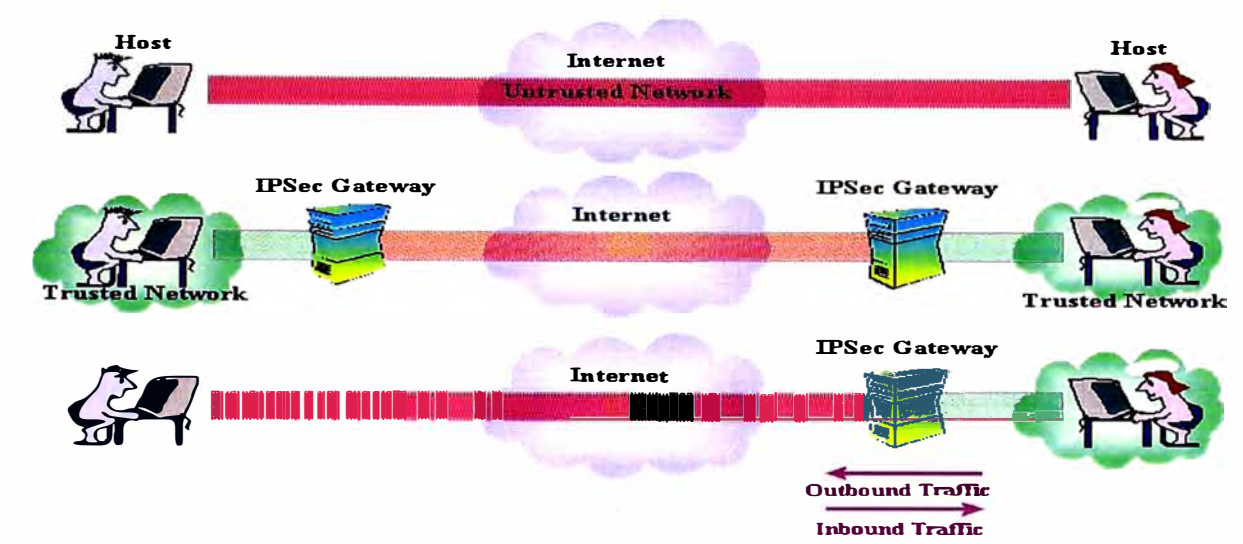


Fig. 23 IPSec, Host and Security Gateway

3.6 SSL, Conceptos Fundamentales

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL opera como una capa adicional entre Internet y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, Telnet y otras aplicaciones además de HTTP.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos. Primero se debe hacer una solicitud de seguridad. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como *SSL Handshake*. Una vez se haya establecido una comunicación segura, se deben hacer verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos. Tras finalizar la transacción se termina SSL.

Solicitud de SSL: Antes de que se establezca SSL, se debe hacer una solicitud.

Típicamente esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL. SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio. Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el *SSL Handshake*

SSL Handshake: Durante el *hanshake* se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una llave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación SSL.

Los pasos que se siguen son los siguientes:

- **Client Hello:** El "saludo de cliente" tiene por objetivo informar al servidor que algoritmos de criptografía puede utilizar y solicita una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define como cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen que métodos pueden utilizar y un algoritmo de hash de una sola vía. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.

-**Server Hello:** El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de que algoritmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.

-**Aprobación del Cliente:** El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo desencriptando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la encripta utilizando la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se le envía al servidor y en caso de que el handshake tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

-**Verificación:** En este punto ambas partes conocen la llave secreta, el cliente por que la generó y el servidor por que le fue enviada utilizando su llave pública, siendo la única forma posible de desencriptarla utilizando la llave privada del servidor. Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones encriptada con la llave secreta. Si ambas partes confirman la validez de las transacciones, el handshake se completa, de otra forma se reinicia el proceso.

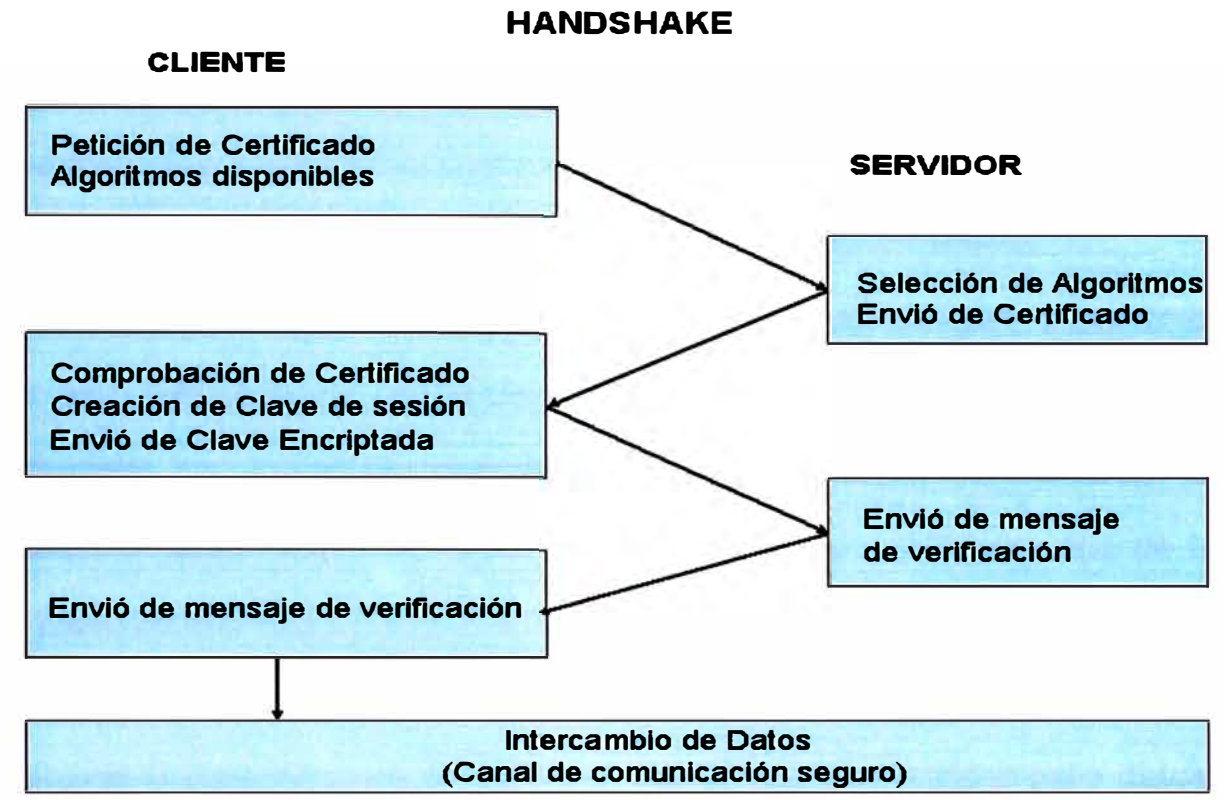


Fig. 24 SSL HandShake

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión. El handshake se realiza solo una vez y se utiliza una llave secreta por sesión.

Intercambio de datos: Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash de una vía acordado durante el handshake), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

Terminación de una sesión SSL: Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

3.6.1. Deficiencias del Protocolo SSL

SSL fue creado como un protocolo de comunicaciones seguro de uso genérico. Como no fue pensado explícitamente para el comercio electrónico presenta usa serie de deficiencias que deben tenerse en cuenta.

- **Confidencialidad:** SSL garantiza la confidencialidad extremo a extremo pero una vez finalizada la conexión, el Vendedor posee todos los datos del comprador, así como su número de tarjeta de crédito. El Vendedor podría almacenar esos datos y el Cliente estaría expuesto a cualquier tipo de fraude por parte de toda persona que tuviera acceso a dicha información.
- **Integridad:** SSL no garantiza la integridad de la información una vez finalizada la conexión, por lo que el vendedor podría modificar esos datos, por ejemplo, cobrando de más al cliente.
- **Autentificación:** El cliente no necesita autentificarse, una persona con acceso a números de tarjeta de crédito robados podría realizar cualquier tipo de compra por Internet. Este es precisamente el tipo de fraude más común y que causa mayores perdidas a las compañías de crédito.
- **No repudio:** Una vez finalizada la compra no existe ningún tipo de comprobante de compra por lo que cualquier protesta posterior carecerá de medios para su confirmación. Tampoco existe ningún documento firmado por lo que tanto el Cliente como el Vendedor o el Banco podrían negar su participación en la compra sin que existiera la posibilidad de probar lo contrario.

Con SSL, toda la seguridad recae en la confianza que el Cliente tenga del Vendedor, ya que potencialmente el Vendedor puede realizar cualquier tipo de fraude con total impunidad. Solo las empresas con muy buena reputación podrían, a priori, contar con esta confianza del consumidor.

El más que posible fraude con números de tarjetas robados hace que las Entidades de Crédito añadan una comisión en las compras bastante elevada (un 5% +/-) para compensar este tipo de fraude. Esto hace que el precio de la compra se incremente considerablemente, lo que anula el atractivo inicial de comprar por Internet: los precios bajos.

Estandarizar la comunicación con el banco es una de los puntos importantes que hay que solucionar para conseguir una mayor transparencia y poder abrirse a la competencia.

SSL utiliza Certificados digitales siguiendo el estándar X.509, es decir, certificados de propósito general. Seria más interesante que existieran Autoridades Certificadoras creadas especialmente para emitir certificados de este tipo y que dichas Autoridades estuvieran avaladas por la banca de tal modo que los certificados digitales expedidos tuvieran conexión con cuentas de bancarias concretas.

3.6.2. Solución Final: Protocolo SET

Las empresas de crédito son las principales interesadas en que el uso de las Tarjetas de Crédito se generalice en todos los ámbitos de la vida, incluyendo evidentemente a Internet. No es de extrañar por tanto que las dos empresas más importantes de este sector, Visa y Mastercard uniesen esfuerzos y potenciaran la creación de un nuevo protocolo que permita los pagos por Internet de un modo totalmente seguro, sin las limitaciones que plantea SSL.

La idea básica consistía en crear un protocolo especialmente diseñado para garantizar la seguridad en el pago mediante Tarjetas de Crédito a través de medios de comunicación inseguros como es el caso de Internet y que este

protocolo se convirtiese en un estándar abierto para la industria que sirviese de base a la expansión del Comercio Electrónico por Internet.

Para ello debían contar con el apoyo de las principales compañías informáticas, así que al proyecto se le unieron empresas de la talla de Microsoft, Netscape, IBM, Verifone-HP, GTE y contaron como desarrolladores a RSA Data Security, Verisign, Terisa-Spyrus y SAIC.

El 31 de Mayo de 1997 se hicieron públicas las especificaciones formales del protocolo SET versión 1.0, estas especificaciones se pueden encontrar el web oficial de SET, <www.setco.org>. Los documentos oficiales son:

1. Book 1: Descripción de negocio
2. Book 2: Guía para Programadores
3. Book 3: Descripción formal del protocolo

A estos documentos hay que añadir un cuarto:

4. Guía de interfase externo

En este documento se dan las normas para la conexión por Internet, ya que SET internamente no especifica el tipo de protocolo de comunicación que debe utilizarse ni las características de las interfases.

Características principales de SET

Las especificaciones de SET parten de una serie de criterios de diseño que permitan la mayor difusión y seguridad del protocolo. Estas características generales son:

- Estándar abierto
- Objetivo específico: Transferencia de números de tarjetas de créditos
- Utiliza codificación estándar (ASN.1 y DER)

- Independiente del medio de comunicación utilizado
- Utiliza estándares criptográficos ampliamente manejados (PKCS, X.509)
- Utiliza Criptografía de Clave Pública
- Autentificación basada en la certificación digital de todas las entidades participantes en la transferencia

Entorno:

A diferencia de SSL, en SET se definen tres entidades independientes: Cliente (Cardholder), Vendedor (Merchant) y la Pasarela de Pago (Gateway Payment) que se interconectan directamente por Internet, haciendo el Vendedor de puente entre el Cliente y la Pasarela de Pago. Previamente a cualquier comunicación entre ellos, todas las entidades deben haber obtenido un certificado digital valido a través de la Autoridad de Certificación adecuada. La Pasarela de Pago permite la conexión desde Internet con las Redes Bancarias como VisaNet, dentro de estas Redes distinguimos otras dos entidades. El Issuer o entidad emisora de la tarjeta de crédito y el Adquirer o banco receptor de la transacción electrónica.

SET se diseñó pensando en su utilización en Internet pero no de un modo exclusivo como SSL, sino que permite la conexión a través de cualquier tipo de red siempre que se definan los interfaces adecuados.

Jerarquía de Certificación:

SET es el primer proyecto de certificación a escala global que se va ha realizar en el mundo. Los certificados SET se estructuran siguiendo una jerarquía piramidal única que culmina en una Autoridad Certificadora Raíz (Root CA) que es la encargada de certificar a todas las demás autoridades certificadoras. Bajo la Root CA se encuentran las Brand CA o CA propiedad de

las Entidades emisoras de Tarjetas de Crédito. Obviamente las primeras Brand CA's pertenecen a Visa Internacional y MasterCard Internacional. Las Brand CA's pueden a su vez certificar a otras CA's para que actúen en un ámbito político determinado, estas CA's reciben el nombre de Brand Geopolitical CA.

Autoridades de Registro:

SET establece un protocolo para la obtención de certificados electrónicos. En la práctica la obtención de un certificado implica que la CA necesita estar segura de que el destinatario del certificado digital es realmente quien dice ser. Esta labor la llevaran a cabo las llamadas Autoridades de Registro, que actuarán de avaladores ante la CA de los usuarios y se encargarán de tramitar los certificados liberando al usuario final de gran parte de esta labor. Las Autoridades de Registro serán precisamente los bancos, esto permitirá que los certificados estén asociados a números de cuentas bancarias y no a personas físicas; permitiendo las compras anónimas, por lo menos desde el punto de vista del Vendedor.

Pago electrónico:

El esquema de pago electrónico SET es muy similar al de CyberCash y, al igual que este, admite una gran variedad de opciones. En un pago normal SET, todo se inicia con una orden de pago que el cliente envía al vendedor. Esta orden de pago esta dividida en dos: la descripción de la compra (OD) y los datos financieros del cliente (PIN). Estos datos se firman y se relacionan entre sí por medio de un algoritmo llamado Firma Dual. Los datos financieros van, a su vez, encriptados con la clave de la pasarela de pago por lo que no pueden ser consultados por el vendedor.

El vendedor envía estos datos encriptados a la Pasarela de Pago que

autoriza la transacción. Una vez autorizada, el Vendedor envía una respuesta al comprador firmado que sirve de comprobante de venta. Finalmente el vendedor realiza la captura del importe, es decir envía la orden al banco de que se efectúe la transacción.

SET

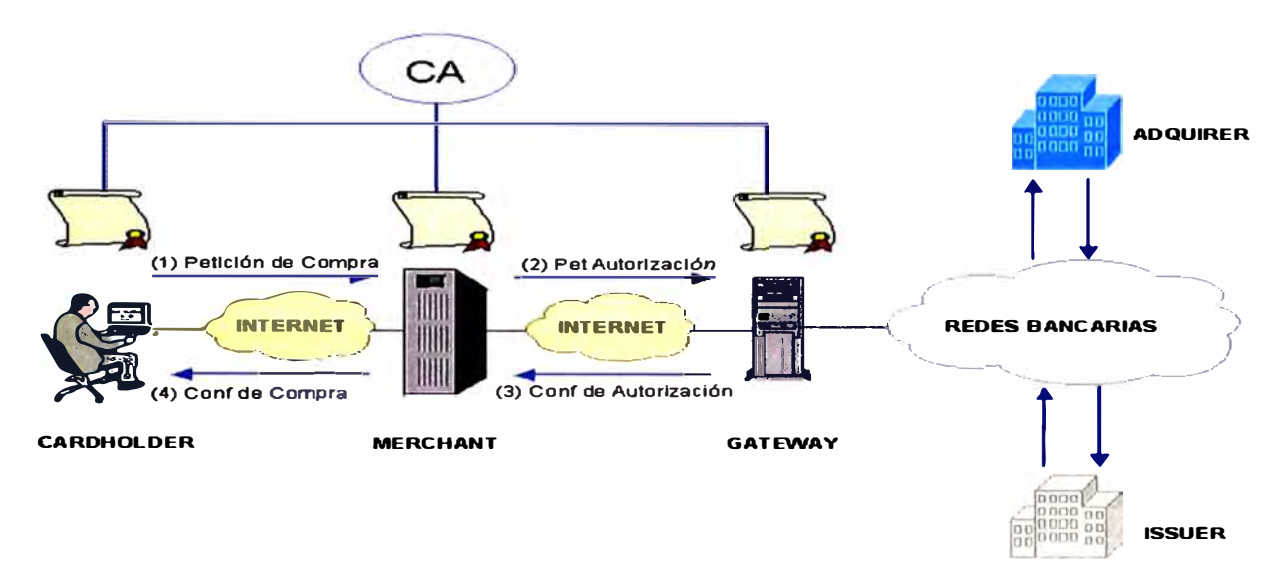


Fig. 25 Secure Electronic Transaction (SET)

Ventajas de SET sobre SSL

SET ofrece una serie de mejoras sobre el sistema basado en SSL. Concretamente en lo referente a los servicios de seguridad podemos comentar lo siguiente:

1. Confidencialidad: Al separar los datos financieros de la descripción de la compra aumentamos la confidencialidad ya que ni el vendedor ni el banco tienen acceso a datos que no le son imprescindibles
2. Integridad: Todos los mensajes van firmados digitalmente de modo que se garantiza la integridad de todos los datos incluso tras finalizar la conexión.

3. Autentificación: Todos los participantes están certificados por una Autoridad Certificadora única, lo que imposibilita cualquier tipo de usurpación de identidad así como la utilización de números de tarjeta de crédito robados
4. No repudio: Los mensajes firmados pueden servir como Recibo de compra, sirviendo de prueba inalterable de que la transacción se produjo de un modo concreto.

Defectos de SET 1.0

La versión 1.0 presenta una serie de defectos y debilidades que intimidan enormemente a la industria y que puede ser uno de los factores que están retrasando la implantación definitiva de este sistema a nivel mundial.

La primera deficiencia importante es la dependencia de algoritmos de encriptación concretos. Esto implica que si se encuentra una vulnerabilidad en alguno de estos protocolos, la seguridad de SET se vería seriamente amenazada. Y precisamente esto es lo que ha sucedido recientemente.

La EFF (Electronic Frontier Foundation) construyó en Noviembre de 1998 una maquina llamada DEScracker capaz de desencriptar el protocolo DES en tan solo 4 días. El objetivo de la EFF no era otro que demostrar lo que se venía diciendo desde hacia tiempo: El algoritmo DES está desfasado y es susceptible de ataques.

Pero el gran defecto de SET 1.0 es su sistema de certificados que presenta numerosas debilidades a la hora de implementarlo en la práctica. Concretamente sus puntos débiles son:

1. Distribución: El modo de conseguir un certificado Digital es tremendamente complicado, especialmente teniendo en cuenta que estos certificados irían destinados al público en general.

2. Almacenamiento: El talón de Aquiles de SET 1.0, todo el sistema se basa en mantener en secreto la clave privada del cliente. Por lo que esta clave se convertiría en objetivo prioritario de robos, ataques de hackers y virus informáticos. Con la agravante de que lo más probable es que el cliente no fuera consciente de que es lo que debía proteger.
3. Movilidad: El certificado quedaría almacenado localmente en el ordenador personal del cliente lo que impediría el uso de un terminal diferente para realizar la compra. Este es un defecto estructural de gran importancia por sí solo.
4. Revocación: El método utilizado para controlar los certificados revocados no acaba de convencer a los expertos que están estudiando otras alternativas. Esto, hasta cierto punto es comprensible ya que nunca antes se ha probado una jerarquía de certificación a nivel global de estas características.

SET 2.0

Como respuesta a todas estas deficiencias se ha creado un equipo de investigación que esta trabajando en la nueva versión de SET que acabara con todos estos problemas. Se permitirá que el protocolo pueda seleccionar entre varios algoritmos de cifrado como SSL y se perfeccionara el sistema de revocación de certificados. Pero el punto básico de la versión 2.0 será la unión de SET con otro tipo de tecnología muy de moda en la actualidad: Las tarjetas Inteligentes o Tarjetas Chip.

Las tarjetas inteligentes son unas tarjetas del tamaño de las tarjetas de crédito convencionales que en lugar de almacenar la información en una cinta magnética lo hacen en un circuito integrado que llevan acoplado a la propia

tarjeta. Este chip es un pequeño Microprocesador con capacidad para almacenar y generar claves criptográficas y realizar algunos algoritmos de cifrado.

Con la utilización de estos dispositivos se solucionarían las deficiencias más importantes. Las Tarjetas Chip servirían de sistemas de almacenamiento de claves, evitado el almacenamiento de las claves en el propio ordenador y permitiendo la movilidad a otros ordenadores. Además el proceso de certificación se vería muy simplificado desde el punto de vista del cliente final: el usuario iría al banco y obtendría su tarjeta chip debidamente certificada, siendo el propio banco el encargo de realizar los procedimientos necesarios para la certificación.

CAPITULO IV
SECURE ELECTRONIC TRANSACTION (SET)

El objetivo principal del protocolo SET es el de poder realizar pagos seguros con tarjetas de crédito a través de una red insegura como Internet. Se pretende que SET sea un protocolo abierto a la industria de tal manera que cualquier empresa interesada en el comercio electrónico pueda crear sus propias herramientas compatibles con este protocolo.

El proyecto SET (Transacciones Electrónicas Seguras) es una iniciativa de Visa y Mastercard y cuenta con la colaboración de IBM, Microsoft, Netscape, GTE, SAIC, Terisa, RSA Data Security y Verisign. Otras Entidades de Crédito como American Express y Diners Club apoyan totalmente esta iniciativa. Muy posiblemente se convierta en un estándar del comercio electrónico en poco tiempo.

Con más de 40 millones de usuarios y con una previsión de crecimiento de 60 millones más en dos años, Internet se está convirtiendo en una nueva forma de hacer negocio. El contacto entre el cliente y el vendedor es mucho más directo gracias a las potentes herramientas interactivas que ofrece Internet, como la Web. Esta situación favorece el que los clientes puedan acceder a la información sobre productos y precios directamente desde sus casas. El siguiente paso lógico en esta situación es que los fabricantes y vendedores ofrezcan sus productos directamente a los consumidores por Internet. Unos de los problemas que surgen en esta situación es el pago a

distancia de los productos. La solución natural a este problema debería ser la utilización de tarjetas de crédito.

SET surge precisamente para dotar de seguridad a este tipo de transacciones electrónicas. De este modo se definen una serie de agentes que intervienen en la transacción:

Cardholder (Cliente):

Cualquier persona que posea una tarjeta de crédito y que desee realizar una compra a través de Internet.

Merchant (Vendedor): Servidor que ofrece la posibilidad de comprar productos a través de Internet. Para permitir transacciones con tarjetas de crédito debe haber llegado a un acuerdo previamente con un banco que le acepte estas transacciones (Adquirer).

Gateway Payment (Pasarela de Pago):

Servidor que sirve de puente entre la red abierta en la que se encuentran el Cliente y el Vendedor (generalmente Internet) y las Redes Bancarias. Este servidor realiza las tareas de paso del protocolo SET al protocolo EFT (Transferencia Electrónica de Fondos).

Adquirer: Banco receptor de la transferencia, previamente el Vendedor debe haber creado una cuenta a su nombre. Generalmente el Adquirer tendrá a su cargo una Pasarela de Pago por lo que se suele tratar a ambas entidades como una sola.

Issuer:

El Banco o Entidad Financiera responsable del pago efectuado con una tarjeta de crédito por parte del Cardholder.

Autoridad Certificadora (CA):

Entidad encargada de emitir certificados a las entidades participantes en una transacción SET.

4.1. Formato general de los mensajes

Siempre que ha sido posible se ha optado por la utilización de estándares para facilitar el trabajo a los desarrolladores y asegurar la interoperatividad entre las diversas implementaciones del protocolo. Para garantizar esta interoperatividad y para permitir nuevas revisiones del protocolo, SET usa los estándares de Criptografía de Clave Publica (PKCS) para representar los parámetros criptográficos y encapsular mensajes.

Los mensajes SET están definidos usando el estándar ISO/IEC 8824 Abstract Syntax Notation (ASN.1) y codificados utilizando el Distinguished Encoding Rules (DER). Esto permite una codificación sin ningún tipo de ambigüedades utilizando un estándar muy bien estudiado y ampliamente utilizado.

En las especificaciones no se define como se transmiten los mensajes SET entre las distintas entidades. Potencialmente puede ser utilizado en cualquier red de datos aunque la principal aplicación actualmente será Internet, y más concretamente la World Wide Web.

Message Wrapper:

El MessageWrapper es el nivel superior de la estructura de datos ASN.1/DER del protocolo SET. En este mensaje se incluyen una serie de datos no encriptados que permiten una rápida detección de mensajes erróneos o duplicados.

Todo mensaje estará compuesto por una cabecera y el cuerpo del mensaje. En la cabecera se incluyen varios datos no encriptados entre ellos: Versión y Revisión del protocolo (1.0 por el momento); Fecha y Hora: en formato UTC; identificador del software, y varios códigos identificadores del mensaje.

El cuerpo del mensaje estará compuesto por uno de los posibles mensajes definidos por el protocolo como PinitReq, AuthReq, CapRes, etc.
La estructura formal del Message Wrapper es la siguiente:

Tabla 3: Formato General SET

Campo	Descripción
Message-Wrapper	{Cabecera, Mensaje, [Extensiones]}
Cabecera	{Version, Revision, Fecha, [MessageIDs], [RRPID], SWIdent}
Versión	*Versión del estándar SET utilizado.*
Revisión	*Revisión del estándar SET utilizado.*
Fecha	*Fecha y Hora del mensaje generado.*
MessageIDs	*{[LID-C], [LID-M], [XID]}*
RRPID	*Identificador del ciclo de Petición/Respuesta.*
SWIdent	*Identificación del software (Vendedor y Versión) utilizado. El formato de este campo es una secuencia de caracteres.*
Mensaje	<PInitReq, PInitRes, PReq, PRes, InqReq, InqRes, AuthReq, AuthRes, AuthRevReq, AuthRevRes, CapReq, CapRes, CapRevReq, CapRevRes,

	CredReq, CredRes, CredRevReq, CredRevRes, PCertReq, PcertRes, BatchAdminReq, BatchAdminRes, CardCInitReq, CardCInitRes, Me-AqCInitReq, Me-AqCInitRes, RegFormReq, RegFormRes, CertReq, CertRes, CertInqReq, CertInqRes, Error>
LID-C	*Código identificador del Comprador.*
LID-M	*Código identificador del Vendedor.*
XID	*Código identificador de la transacción.*
Extensiones	*Opcionalmente, un mensaje puede contener varias extensiones no encriptadas, en las que se incluirán datos no confidenciales de la transacción.*

4.2. Criptografía

La seguridad en SET está garantizada por la utilización de la moderna criptografía de clave pública. La versión 1.0 de SET hace uso del algoritmo RSA tanto para firma como para encriptación de datos. Adicionalmente se utilizan el algoritmo DES para encriptación simétrica y SHA-1 para la creación de Hash. El formato de los mensajes encriptados cumple con las especificaciones PKCS#7.

4.2.1. Confidencialidad

La información confidencial intercambiada entre los agentes que forman parte de una transacción SET se encripta utilizando un sistema conocido como

Sobre Digital, que consiste en encriptar el mensaje con DES y posteriormente encriptar la clave DES utilizando el algoritmo RSA. Metafóricamente es como si introdujéramos la clave de sesión en un sobre.

El estándar PKCS#7 especifica un formato llamado EnvelopedData que es utilizado en SET para este fin.

En el formato PKCS#7 **EnvelodepData** se diferencian claramente dos campos: el *RecipientInfo* en que se haya la Clave de Sesión encriptada con RSA y el *EncryptedContentInfo* en el que se encuentra el mensaje encriptado con DES mediante la clave de sesión.

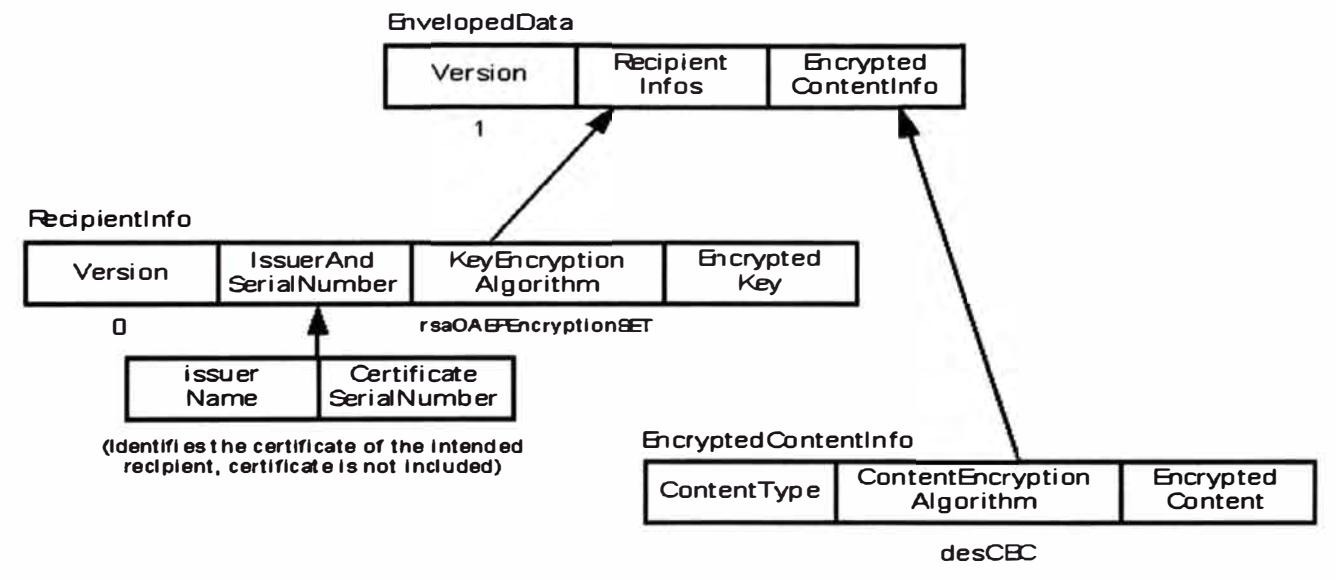


Fig. 26 Formato PKCS # 7

PCKS#7 es un tipo de formato de encriptación de mensajes que no está condicionado por algoritmos concretos, en su lugar aparece el campo "Algoritmo" en el que se debe especificar uno de los algoritmos de cifrado reconocido por los estándares PKCS.

El campo de datos a encriptar con RSA debe tener una longitud concreta

de 1024. Para garantizar que este campo tenga el formato correcto aumentado a la vez la fortaleza del algoritmo, se ha optado por la utilización de OAEP (Optimal Asymmetric Encryption Padding) que define el formato que debe tener este campo.

El propósito de OAEP es el de asegurar que las partes individuales del mensaje no puedan ser extraídas de un bloque PCKS#7. Hay técnicas criptoanalíticas que hacen que algunos bits del mensaje sean más fáciles de determinar que otros. OAEP distribuye aleatoriamente los bits de un bloque PCKS#7 garantizando que la dificultad en la extracción de un bit determinado sea igual para cada uno de ellos.

La versatilidad del OAEP permite la verificación del mensaje desencriptado así como compaginar varios datos para ser cifrados conjuntamente y la utilización de fresh (números aleatorios recién creados) para dificultar la desencriptación del mensaje.

Para formar un bloque OAEP primeramente se crea el ADB que no es más que concatenar los datos que deben ser encriptados. Estos datos son el DEK (Clave de sesión que posteriormente será utilizada para cifrar el mensaje con DES) y el resto de datos que forman parte del mensaje a encriptar. En SET se aprovecha este formato para incluir los datos financieros más importantes (el PAN) en la encriptación RSA aumentando así la confidencialidad del sistema en lo referente a los datos más críticos de la transacción.

Al ADB se le añaden otros datos (BT, BC y V) que servirán para verificar la integridad del mensaje en el proceso de desencriptación, formando así el bloque DB. A este bloque se le añade un valor aleatorio llamado E-Salt y se le aplican dos funciones Hash que dan como resultado el valor PBD. El objetivo

de este proceso es distribuir la información aleatoriamente entre todos los bits del mensaje a encriptar. Finalmente se le añaden una serie de valores que completan el formato creando un valor de 128 bytes que será cifrado mediante el algoritmo RSA.

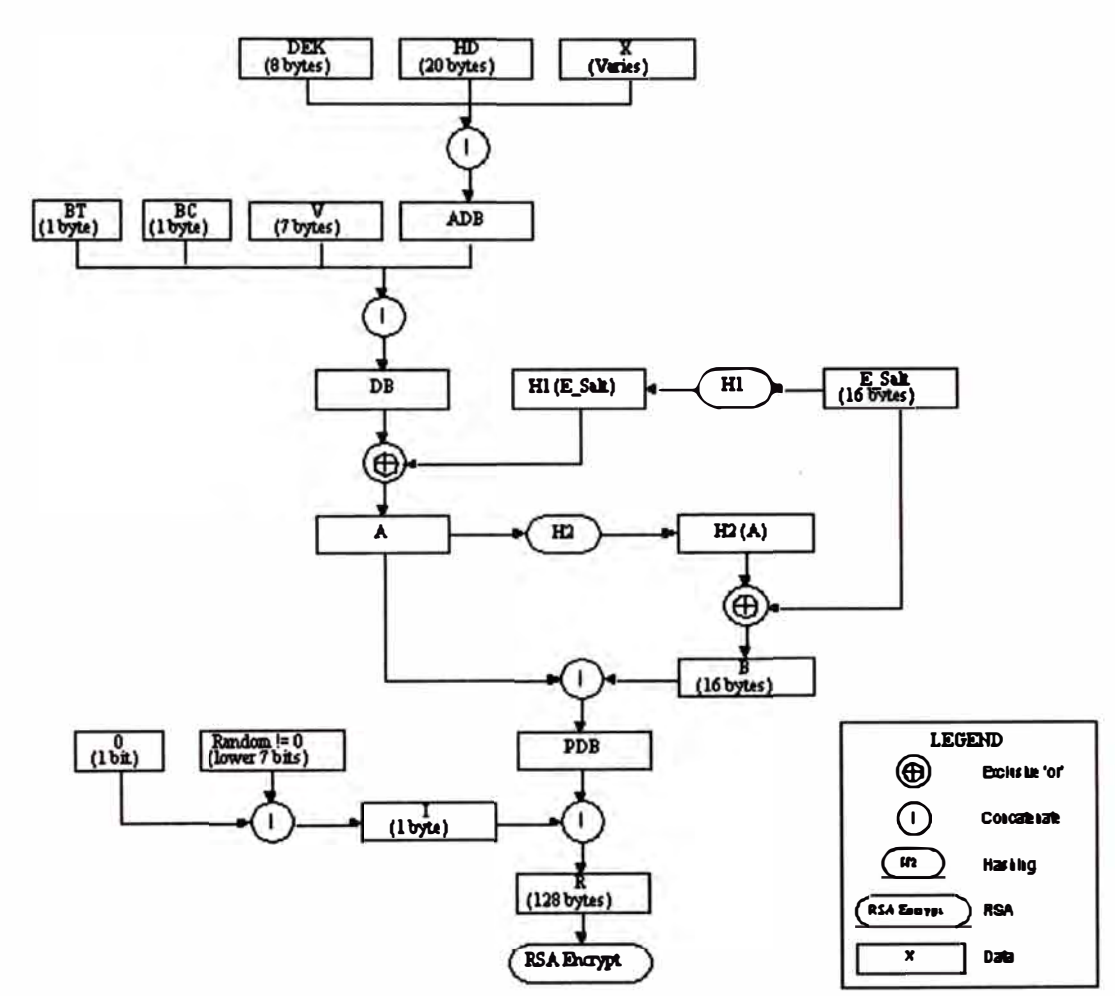


Fig. 27 Formato OAEP

4.2.2. Integridad y No Repudio

La integridad de los mensajes queda garantiza mediante la utilización de Firmas Digitales, estas firmas se realizan usado nuevamente el algoritmo RSA y el formato PCKS#7 SignedData.

Para realizar la Firma digital se crea un Hash del mensaje mediante la función SHA-1, este hash se encripta con la clave privada del firmante

mediante el algoritmo RSA creando un digest encriptado que sirve de firma. En el formato PCKS#7 se especifican los campos necesarios para indicar los algoritmos utilizados, el texto original, el hash y el hash firmado, así como todos los certificados y listas de revocación (CRLs) necesarias para comprobar la validez de la firma.

SET incorpora un algoritmo propio llamado Firma Dual que permite unir dos datos mediante una firma digital de tal manera que la firma pueda ser comprobada sin necesidad de conocer el contenido de todos los datos firmados. La Firma Dual es necesaria en SET ya que se pretende que el Vendedor no tenga acceso a los datos financieros del cliente y que el Banco no tenga acceso a los datos de la compra.

La Firma Dual se obtiene aplicando la firma digital a la unión de los hash de los campos que deben ser firmados, en este caso: El hash de la descripción de compra (OI) y el hash de los datos financieros (PI). Así,

Firma Dual = Firma { H(OI) + H(PI) }

Para comprobar la firma únicamente necesitamos conocer los hash y no el valor real del campo. Tanto la PI como la OI quedan unidas de tal forma que si hubiese una reclamación posterior sería posible reconstruir la firma de forma unívoca demostrando que la orden de pago corresponde a una compra concreta. De este modo garantizamos tanto la privacidad de los datos como la integridad y el no repudio de los mismos.

TrainStain

Además de la comprobación de identidad mediante la utilización de certificados digitales, SET incorpora una medida adicional de autentificación llamada TrainStain. El Trainstain se obtiene de aplicar la función HMAC al

identificador de la transacción XID y a un número secreto llamado CardSecret que se crea en el proceso de certificación y que es compartido por el Cliente, la CA y el Banco emisor.

El algoritmo HMAC, también conocido como mecanismo de hash cifrado, da como resultado un hash de 160 bits a partir de un valor t, una clave k y la utilización del algoritmo SHA-1.

$HMAC(t,k) = H((k \oplus opad) \mid H((k \oplus ipad) \mid t))$

Donde, ipad es el byte 0x36 repetido 64 veces; opad es el byte 0x5C repetido otras 64 veces; y $\oplus$ es la función XOR.

En el caso concreto del TrainStain, t = XID (el identificador de la transacción) y k =CardSecret, un valor secreto que comparten el Cardholder y el Issuer.

4.3. Certificación

La principal mejora en seguridad que ofrece SET con respecto a otros sistemas utilizados para el pago con tarjeta de crédito en Internet es la Autentificación de todas las partes implicadas en una transacción utilizando certificados digitales.

Un Certificados Digital es un documento digital que certifica que una Clave pública pertenece realmente a un usuario determinado. En cualquier certificado aparecen varios campos típicos, entre ellos: El nombre del propietario del certificado, fecha de caducidad y la clave pública del usuario. Este documento esta firmado digitalmente por un organismo conocido como Autoridad Certificadora (CA). En SET se ha establecido una jerarquía de certificación de tal manera que las CA's están certificadas a su vez por otras Autoridades Certificadoras de mayor nivel.

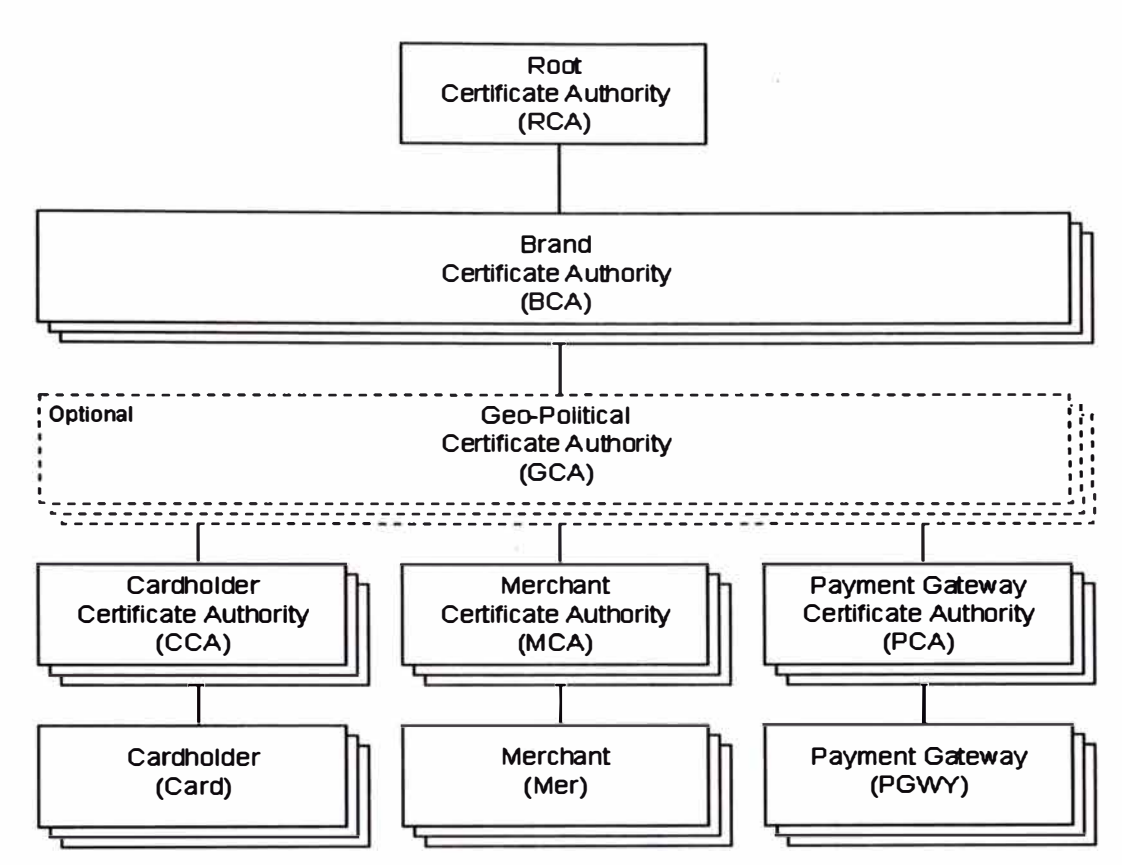


Fig. 28 Jerarquía de certificación

El proceso de certificación se lleva a cabo a partir de una Autoridad Certificadora Raíz (Root CA) la cual emitirá certificados para otras Autoridades Certificadoras de primer nivel llamadas Brand CA. Estas CA's serán las encargadas de certificar al resto de las CA's. Opcionalmente las Brand CA pueden dividirse en Geo-political Brand CA por motivos geográficos o políticos. El proceso de certificación debe ser anterior a cualquier transacción e independiente de esta. Los protocolos de certificación SET están definidos aunque pueden no implementarse y optarse por otro tipo de medio para certificar a una entidad SET. Dada la importancia de este proceso lo lógico es que se utilicen sistemas off-line para entregar los certificados.

El Cliente debe poseer únicamente un certificado de firma, mientras que tanto el Vendedor como la Pasarela de Pago deben contar con dos certificados

cada uno: uno de firma y otro de encriptación.

Los certificados SET cumplen con el formato X.509 que especifica una serie de campos obligatorios. El versión 3 de X.509 (la versión utilizada en SET) establece un método genérico para incluir información adicional en el certificado en forma de extensiones. Las extensiones son campos opcionales que se añaden al final del certificado X.509. SET establece una serie de extensiones obligatorias lo que hace incompatible el uso de otro tipo de certificados en el protocolo SET aunque cumplan con el estándar X.509v3, como los certificados SSL.

El formato genérico de un certificado X.509 es el siguiente:

Tabla 4: Formato genérico de un certificado X.509

Nombre	Tipo de Valor	Descripción
Versión	nteger	ndica la versión del certificado. En este caso el valor debe ser 3.
Número de Serie	nteger	Número de Serie único asignado por a CA emisora del certificado.
Signature .AlgorithmIdentifier	DID and type	Define el algoritmo usado para firmar el certificado.
Emisor	Nombre	Contiene el Distinguished Name (DN) de la CA emisora.
Validity .notBefore	UTC Time	Fecha a partir de la cual el certificado es válido.
Validity .notAfter	UTC Time	Fecha de expiración del certificado. Si se trata de un certificado de cliente, esta fecha queda subordinada a la fecha de validez de a tarjeta de crédito.

Propietario	Nombre	Contiene el Distinguished Name de la entidad propietaria de la Clave.
SubjectPublicKeyInfo .algorithm .AlgorithmIdentifier	OID and type	Especifica los algoritmos que pueden ser utilizados con esta clave.
SubjectPublicKeyInfo .subjectPublicKey	Bit string	Contiene la Clave Pública
IssuerUniqueID		No usado en SET.
SubjectUniqueID		No usado en SET.
Extensions .extnId	OID format	Contiene el identificador OID de la extensión, definido por X.509 o por SET.
Extensions .critical	Boolean; 0 falso (Defecto) , 1 cierto	Este campo indica si una extensión es crítica o no.
Extensions .extnValue		Extensiones.

4.3.1. Validación del canal de certificación

Para validar una Clave Pública de firmado es necesario comprobar toda la cadena de certificación hasta llegar al Certificado de Root, que vendrá preinstalado en toda aplicación SET. El proceso de distribución de un nuevo Certificado Root (En caso de caducidad de la clave pública) está especificado aunque dada la peculiaridad del caso, no se tratará en este documento.

Cada Certificado se encuentra enlazado con el certificado de la entidad emisora siguiendo una Jerarquía de Confianza, tal como se muestra en la figura Nro 34

Para asegurar la validez de los certificados, la aplicación realizará las siguientes comprobaciones:

. Las fecha actual debe estar entre el rango de fechas validas del certificado.

- La Firma Digital debe ser correcta

- Comprobar la existencia de una cadena de certificados que permita validar la jerarquía de Confianza hasta llegar a la Root CA.

- Comprobar igualmente la validez de los certificados de cada Autoridad Certificadora implicada en la jerarquía.

- Averiguar que si alguno de los certificados a sido revocado por una autoridad superior

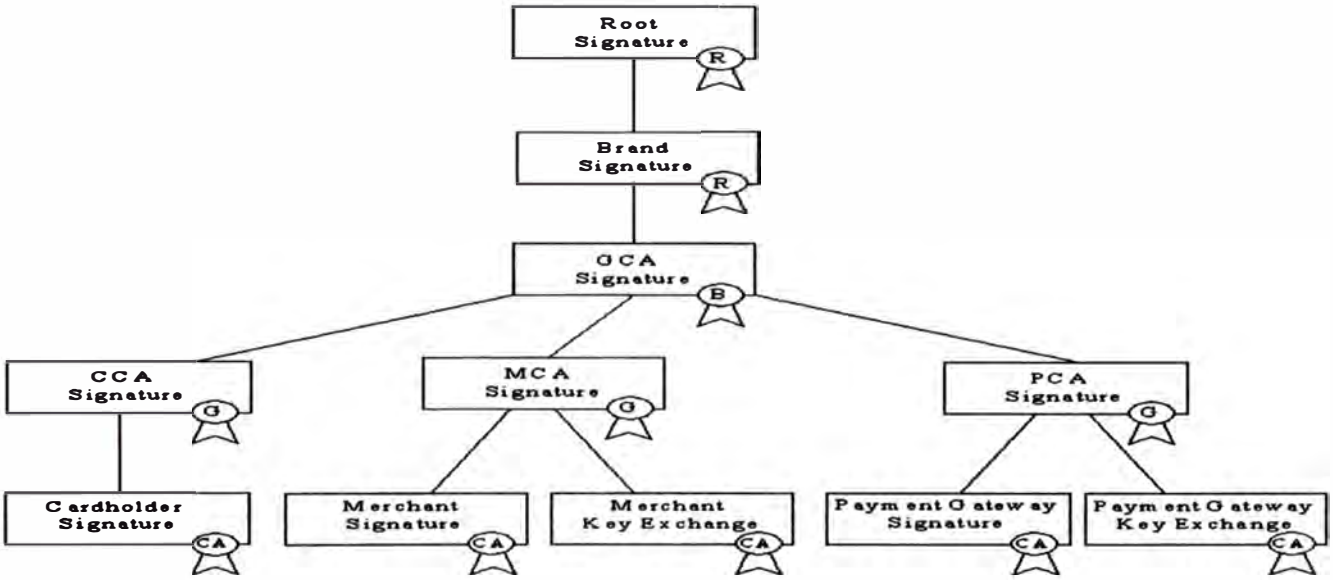


Fig. 29 Jerarquía de confianza de los CA

4.3.2. Revocación de Certificados

Si se tiene la sospecha que una clave privada ha sido violada será necesario comunicar a todos los usuarios de SET esta situación. El proceso de revocación es extremadamente complicado ya que al tratarse de un sistema centralizado de certificación, el conjunto de usuarios afectados puede ser de varios millones en un futuro cercano.

El envío de este tipo de mensajes podría producir una cantidad de información de control excesiva (overhead) y provocar un funcionamiento deficiente del sistema. Para evitar esta situación se ha optado por aprovechar todos los recursos existentes y evitar el envío de información innecesaria.

Un Cliente no necesita tener información sobre la validez de los certificados de otros clientes, ni el Vendedor necesita tener información sobre los certificados de otros vendedores.

El certificado de un Cliente está unido a un número de tarjeta de crédito. Si por alguna razón se revoca dicho certificado, se cancelará también la cuenta asociada a la tarjeta.

El Vendedor no debe preocuparse por la validez del certificado del cliente ya que en caso de estar revocado, el banco impediría la transferencia y devolvería un mensaje de error indicando el motivo

El cliente tampoco necesita tampoco saber si el certificado del Vendedor ha sido revocado, ya que en este caso la Pasarela de Pago impediría la transferencia. Tampoco debe preocuparse por sus datos bancarios, ya que se envían encriptados de tal manera que el Vendedor no tiene acceso a esos datos.

Teniendo en cuenta estas premisas podemos concluir que el Cliente y el Vendedor únicamente necesitan disponer de la información sobre revocación de certificados de Pasarelas de Pago y de Autoridades Certificadoras. Teniendo en cuenta que existirán muy pocas instituciones que realicen estas funciones y la enorme seguridad que emplearán en la protección de sus claves, es de suponer que los mensajes de este tipo serán muy infrecuentes.

SET utiliza el estándar CRL (certificate revocate list) para controlar los certificados revocados. CRL es una extensión del estándar X.509 pensado especialmente para crear listas de certificados revocados. El formato de una CRL es muy parecido al formato de X.509 concretamente:

Tabla 5: Formato CRL

Nombre	Formato y Valores	Descripción
CRL .versión	Integer; V2	ndica la versión del CRL. En este caso 2.
CRL .signature .algorithmIdentifier	OID and type	Define el algoritmo utilizado para firmar el CRL.
CRL .Issuer	Nombre	DN de la CA emisora del CRL. Deberá coincidir con el DN que aparece en el campo Subject Name del certificado de la CA.
CRL .thisUpdate	UTC Time	Fecha a partir de la cual el CRL es válido.
CRL .NextUpdate	UTC Time	Fecha de expiración del CRL..
CRL .revokedCertificates .certSerialNumber	nteger	Número de serie del certificado revocado.
CRL .revokedCertificates .revocationDate	UTC Time	Fecha de revocación del certificado revocado.
CRL .revokedCertificates .extensions	Extensiones	No usado en SET.

CRL .extensions	Extensiones	Se permite dos tipos de extensiones: CRLNumber y AuthorityKeyIdentifier.

Cada Autoridad Certificadora puede crear una lista de revocación CRL que deberá ir manteniendo y actualizando. Así mismo cada CA se responsabilizará de la distribución de la Lista. El CRL debe ser lo más reducido posible por eso no se incluyen los certificados revocados que hayan expedido de fecha ya que no serían válidos de ninguna forma.

4.4. Flujo de Mensajes de Pago

A continuación vemos un esquema de los diferente mensajes que se producirían en una transacción SET típica. Existen muchos otros mensajes posibles que permitirían mayores opciones e implementaciones diferentes. En todo caso, el flujo de mensajes entre las diferentes entidades seguirá el siguiente esquema:

La transacción comienza con una Petición de Inicio de Compra (PinitRes) que envía el cliente al vendedor. La respuesta de esta petición (PinitReq) servirá para obtener toda la información necesaria para realizar la transacción. Esto es, los certificados digitales, las claves públicas de Merchant y Gateway, la lista de certificados revocados, etc. Esta primera fase es opcional en los casos en que el cliente ya posea previamente toda la información necesaria.

La transacción comienza realmente al enviarse la Petición de Compra (PReq), en este mensaje se envían todos los datos financieros básicos para realizar la transacción: el PAN (número de la tarjeta de crédito), el importe de la

compra y la firma del cliente que ratifica la transacción. El Vendedor recibe este mensaje y remite los datos financieros a la Pasarela de Pago quien será la encargada de autorizar o no la transacción. El Vendedor no tiene acceso a estos datos ya que se encuentran cifrados, el Merchant actúa en este caso como un simple intermediario.

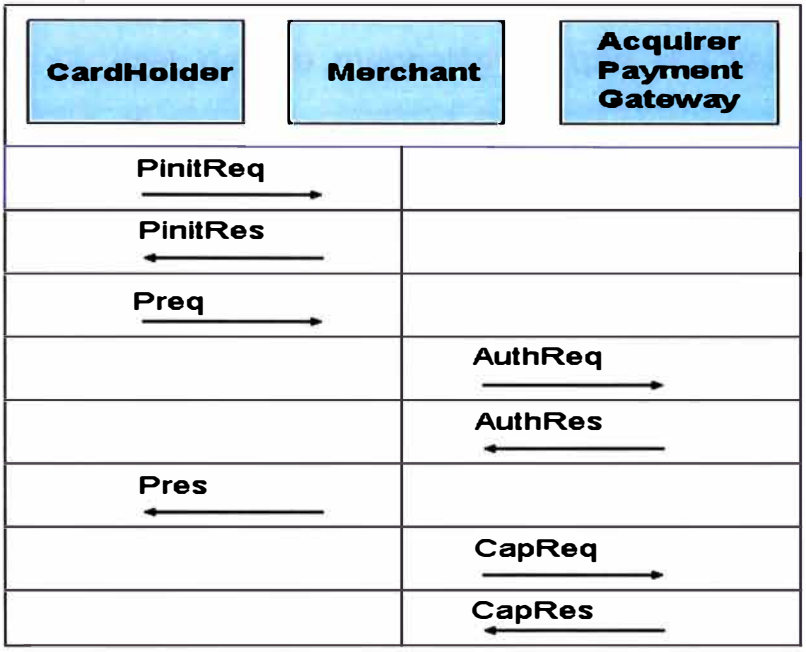


Fig. 30 Flujo de los mensajes de Pago

Tras recibir la PReq, el Merchant envía una Petición de Autorización para la transacción (AuthReq) remitiendo los datos de la orden de pago recibidos del cliente al Gateway. El Gateway se comunica con el banco emisor (Issuer) y con el banco receptor (Adquirer) y determina si se debe autorizar el pago. La Pasarela de Pago responde al Vendedor con un AuthRes (Respuesta de Autorización). Finalmente el Vendedor remite la respuesta al Cliente finalizando así la transacción SET.

La Autorización del pago no implica que la transacción se realice instantáneamente, sino que generalmente se esperará al final de la jornada

para realizar la Captura efectiva de la transacción. Esta Captura se realizará mediante los mensajes CapReq y CapRes.

Explicaremos a continuación estos mensajes en detalle utilizando únicamente los campos necesarios, ignorando las múltiples opciones que pueden añadirse a cada tipo de mensaje.

4.4.1 Petición de Inicio de Compra

El propósito de este par de mensajes es que el Cliente obtenga los certificados y CRL necesarios para realizar la transacción. Estos mensajes irán precedidos generalmente por la fase de compra y por un proceso de inicio SET en el cual comprador y vendedor decidirán el producto y el precio de compra. Estas fases no están contempladas implícitamente en el protocolo SET aunque son condiciones necesarias para poder realizar la transacción.

El mensaje de Petición PinitReq identifica el tipo de tarjeta que va ha ser utilizada, proporciona un identificador local para el Cardholder y se envía un resumen de los CRL y Certificados válidos que dispone el cliente.

El par de mensajes PinitRes/PinitReq no utilizan ningún tipo de encriptación ya que la información enviada no es confidencial.

PinitReq = {RRPID, Lenguaje, LID-C, Chall-C, BrandID, BIN, Thumbs}

RRPID: Es un número aleatorio de 20 bytes que sirve para identificar la pareja Res/Req. Este número se encuentra también en la cabecera del Message Wrapper lo que permite una identificación rápida de los mensajes.

Lenguaje: Identificador del lenguaje utilizado en la transacción.

LID-C: Es un número aleatorio de 20 bytes que identifica al cliente en una transacción. Al igual que el RRPID su utilidad radica en que permite una identificación rápida de los mensajes.

Chall-C: Es un número aleatorio de 20 bytes, creado para impedir ataques de play-black. De este modo se garantiza que las respuestas a este mensaje son recientes y no copias de transacciones anteriores. A este tipo de datos se les conoce como Fresh.

BrandID: Identificador de la entidad emisora de la tarjeta de crédito que se desea utilizar (Visa, MasterCard, etc.)

BIN: Las 6 primeras cifras del número de tarjeta de crédito, que indican el banco emisor de la tarjeta (Issuer)

Thumbs: Hash de los certificados y CRL que posee el cliente

4.4.2. Respuesta de Inicio de Compra

En función de la tarjeta de crédito que vaya a utilizarse, el vendedor decide la Pasarela de Pago que va a utilizar y envía el Certificado Digital con la Clave Pública de esta al cliente. Este mensaje está firmado por el Vendedor.

PinitRes={TransID, RRPID, Chall-C, Chall-M, PEThumb, [Extensiones]}

TransID: El Vendedor genera un identificador personal (LID-M) y un identificador de la transacción (XID) que junto con el identificador del cliente (LID-C) formarán el TransID.

RRPID: Copia del RRPID recibido en el mensaje Req

Chall-C: Copia del número aleatorio (Fresh) creado por el Cliente

Chall-M: Nuevo Fresh creado por el Vendedor

PEThumb: Hash de la Clave pública de encriptación de la Pasarela de Pago seleccionada por el vendedor para realizar la transacción.

Comparando el Thumb recibido, el Merchant conoce la situación del Cardholder en cuanto a Certificados y CRL. Si el Merchant posee datos más actualizados los enviará al Cliente en forma de extensiones del mensaje.

4.4.3. Petición de Compra

Es la parte más importante del protocolo, el objetivo es entregar los números secretos de la tarjeta de crédito a la Pasarela de Pago pasando por el Vendedor.

El Protocolo SET admite la posibilidad de pagos no firmados por el cliente en el caso de que este no disponga de certificado. En este caso el formato del mensaje PReq variaría bastante. Es de suponer que en la práctica habitual se inutilice esta opción ya que de lo contrario se perdería uno de los pilares básicos de SET: la Autentificación del Cliente.

PReq es el mensaje más complejo del protocolo. Consiste de dos partes: una Instrucción de Orden (OI) para el Merchant y una Instrucción de Pago (PI) para el Gateway Payment que utilizará el Merchant como puente para la comunicación. La PI irá cifrada con la clave del Gateway por lo que el Merchant no tendrá acceso esos datos. A su vez estos dos mensajes están firmados y relacionados entre sí por una técnica conocida como Firma Dual. Resumiendo tenemos que,

$$PReq = \{PI, OI\}$$

El proceso previo al pago SET, se debe haber establecido dos datos muy importantes:

La descripción de la compra (OD) y el importe de la misma (PurchAmt). A estos dos datos se le añade un valor aleatorio llamado ODSalt y se calcula el Hash de los tres Datos (HOD). Se añade el ODSalt para impedir ataques de diccionario al Hash HOD. El HOD permitirá identificar la compra realizada sin necesidad de conocer el contenido exacto de la misma.

Firma Dual

En las especificaciones se incluye la firma dual como parte del PI. Es más adecuado considerarla como una parte independiente del mensaje ya que es utilizada tanto por el Merchant como por la Pasarela de Pago para comprobar la Firma Dual.

La firma dual consiste en que el Cardholder firma digitalmente un mensaje compuesto por los Hash del PI y del OI. De esta manera se consigue que ambos datos queden firmados y relacionados entre sí, sin que se haga ninguna referencia a los valores reales de estos datos.

Firma Dual = Firma { Hash(PIData) + Hash(OIData)}

Orden Instrucción (OI)

La OI contiene datos de la compra para el Merchant. Esta parte del mensaje no se encripta ya que no incluye ningún dato confidencial. Esta formado por:

OI = {OIData} + Hash{PIData}

Siendo:

OIData ={ PIDs, BranlD, BIN, HOD, ODSalt}

PIData = {PIHead, PANData}

OIData contiene todos los datos necesarios para identificar la compra. Está compuesto por los PIDs, es decir, los identificadores la transacción (XID, LID-C, LID-M, RRPID, Chall-C y Chall-M), por los datos financieros no confidenciales BrandID y BIN, y por el hash de los datos de compra HOD y ODSalt.

Como el Merchant conoce el Hash de PIData solo tiene que hacer un Hash del OIData y compararlo con la firma digital para comprobar la validez de

la firma dual, sin necesidad de conocer los datos financieros del Cardholder.

Payment Instruction (PI)

La PI se encripta con la clave de encriptación del Gateway Payment por lo que el Merchant no puede tener acceso a estos datos. Los datos financieros más importantes componen el PAN Data.

PANData = {PAN, CardExpiry, PANSecret, Fresh)

PANData está compuesto por el PAN (número de la tarjeta de crédito), la fecha de caducidad, un Fresh y el PANSecret que es un número secreto que comparte el Cardholder, la CA y el Issuer.

El punto fuerte de este mensaje es el Sobre Digital que permitirá encriptar el PANData con la clave pública del Gateway. El mensaje cifrado de PI estará compuesto, análogamente al OI, por:

PI = {PIHead} + Hash {OIData}

Siendo,

PIHead ={TransID, HOD, PurchAmt, MerchantID, TransStain, SwID)

PIHead contiene todos los datos no críticos necesarios para realizar la transacción. Estos son los identificadores de la transacción (TransID), el hash de la Descripción de la compra y su importe(PurchAmt), el Identificador del Merchant (extraído del certificado digital correspondiente), el Identificador del Software del cliente y el TransStain.

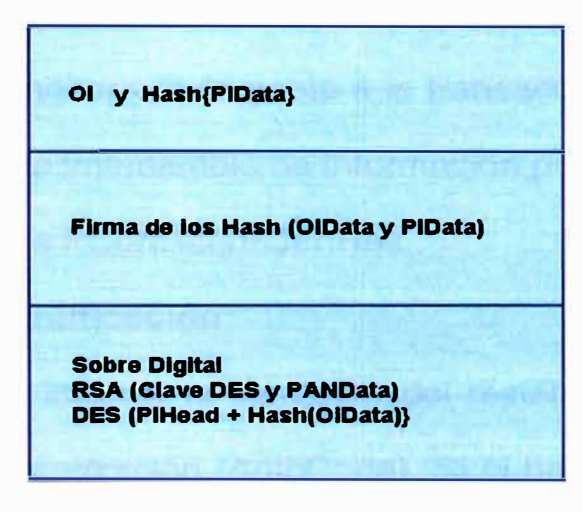
El TransStain es una información secreta que se debe enviar al Issuer y que unido al PANSecret sirve de comprobante de la compra adicional. Su valor es:

TransStain = HMAC(XID, CardSecret)

El Sobre Digital se crea empleando el algoritmo de clave pública RSA en el formato PKCS#7 EnvelopedData. El PANData y la Clave de sesión DES se encriptan mediante RSA utilizando el algoritmo OAEP. Con esto se consiguen varias cosas. Por un lado, la información crítica (PAN) queda encriptada con un algoritmo de clave pública lo que ofrece una seguridad adicional al sistema. La elección del algoritmo OAEP impide que se realicen ataques a RSA basados en suposiciones sobre el texto en claro, además de ofrecer varias formas de verificar posteriormente la desencriptación del mensaje. Con la Clave de sesión DES se encripta el resto del mensaje PI.

En definitiva la estructura del mensaje PRes es la siguiente:

Tabla 6: Formato Pres



4.4.4. Respuesta de Compra

El Vendedor comunica al Comprador el resultado de la operación de pago enviando un código indicando el resultado de la transacción. La respuesta se envía firmada por el Vendedor por lo que sirve de Comprobante de compra

PRes={TransID, RRPID, Chall-C, Código}

4.4.5. Petición de Autentificación

Tras recibir la PReq, el Merchant realiza un Petición de Autorización al banco remitiendo la PI del Cardholder al Gateway Payment mediante el mensaje AuthReq. Este mensaje permite una cantidad enorme de opciones que no serán tratadas en este documento. El mensaje AuthReq está compuesto por el PI y una serie de datos adicionales, todo ello firmado por el Merchant y encriptado con la clave pública del gateway.

AuthReq={PI, TransID, RRPID, MerTermIDs, Fecha, PurchAmt, CaptureNow}

CaptureNow es un booleano que permite realizar la captura y la autorización a la vez. MerTermIDs son una serie de identificadores del Merchant que indica entre otras cosas la cuenta en la que debe depositarse el importe de la transacción.

El Merchant debe conocer previamente a la transacción la Clave pública de la Pasarela de Pago. Este intercambio de información puede llevarse a cabo utilizando el par de mensajes PCertReq/PCertRes.

4.4.6. Respuesta de Autentificación

La pasarela de pago informa al vendedor del resultado de la operación enviándole un código de Autorización (AuthCode). Si el booleano CaptureNow fue activado en el mensaje AuthReq se envía también un código de Captura de la transacción (CapCode). En caso contrario se envía un mensaje encriptado son toda la información sobre el pago llamado PANToken. Con el PANToken el Merchant podrá crear un mensaje para capturar la transacción al final de la jornada. SET implementa una serie de opciones que permiten al Merchant realizar todas las capturas a la vez en forma de lotes, simplificando el número de mensajes a procesar.

La respuesta de la autorización se envía encriptada con la clave pública del Merchant y firmada por la Pasarela de Pago.

AuthRes = {TransID, RRPID, AuthCode, PurchAmt, CapCode o PANToken}

4.4.7. Captura de la Transacción

El par de mensajes CapRes y CapReq realizan la función de validar las transacciones, efectuándose la transacción real en ese momento. El Merchant envía el PANToken o una serie de PANTokens en forma de lote y el Gateway se encarga de realizar las transferencias electrónicas a la cuenta del Merchant. Una vez finalizado el proceso, la Pasarela de Pago devuelve un código de Captura donde explica el resultado de las transacciones.

CapReq = {CapRRTags, CapItem+, CapToken+}

CapRRTags incluye los identificadores de la transacción y la fecha.

A continuación, el Merchant envía uno o más PANToken. La información se divide entre el CapToken que contiene el mensaje que el Gateway le había dejado al Merchant como testigo de la autentificación; y el Capitel que contiene información relacionada con el CapToken (Fecha, Hora, Importe, etc..). El mensaje se firma y se encripta con la clave del Gateway.

4.4.8. Respuesta de la Captura

El Gateway realiza las transacciones y envía un mensaje con un código en el que se explica el resultado de dichas operaciones. El mensaje se firma y se encripta con la clave del Merchant.

CapRes = { CapRRTags, CapResItem+}

Siendo el CapRRTags el conjunto de identificadores y CapResItem+ una serie de datos de respuesta a los CapTokens enviados por el Merchant. Cada

CapResItem está compuesto por el Código de Captura, por el Importe del mismo y por varios identificadores de la transacción

CapResItem = {TransIDs, AuthRRPID, CapCode, CapAmt}

Los diseñadores de SET decidieron optar por un protocolo optimizado al máximo con el fin de disminuir el tiempo de proceso de desencriptación de los datos a costa de la simplicidad del protocolo formal. Este echo, unido a la multitud de opciones que incorpora, hace de SET un protocolo excesivamente complicado de entender.

Esta decisión es fruto de la experiencia adquirida con el sistema CyberCash, del cual SET es heredero. La utilización de criptografía de clave pública RSA convierte el tiempo de proceso en un factor crítico pero aumenta enormemente la seguridad frente a todo tipo de ataques.

Por estos motivos hay que contemplar la explicación anterior de los diferentes mensajes que intervienen en una transacción SET como una simple aproximación a los mismos.

4.5. Implementación de SET en el Perú

En Perú, la implementación de SET está siendo liderada por VISANET. A continuación se detalla el estado actual y las próximas novedades.

Visanet:

Es una empresa creada por Visa International (www.visa.com), Banco Continental, Banco de Crédito (www.bcp.com.pe) Interbank (www.interbank.com.pe) y Unibanca. Cuyo objetivo es uniformizar los servicios y productos que brindan a sus clientes (Comercios).

El proyecto de Visanet:

Para la implementación de SET en Perú Visanet ha desarrollando un proyecto el cual permite probar la tecnología SET en un ambiente controlado, por decirlo de alguna manera. En este proyecto participan seis Entidades Financieras:

Banco de Crédito

Banco Continental

Interbank

Banco Santander

Citybank

Banco Sudamericano y cuatro Comercios:

E. Wong (www.ewong.com)

Cosapi Data(www.peruplaza.com/cosapidata)

Diario El Comercio(ec-store.elcomercioperu.com.pe)

Telefónica Servicios

Internet(tienda.telefonica.com.pe/telefonica)

Para probar el funcionamiento de SET, los bancos participantes han certificado a algunos de sus tarjeta habientes (invitados con anterioridad y que aceptaron voluntariamente) para que puedan realizar compras en los cuatro Comercios participantes. Por su parte Visanet es la Autoridad Certificadora de Comercios.

El proyecto ha permitido probar la tecnología SET, así como el ciclo completo de venta (calidad del servicio). Dicho proyecto ya está en su etapa final y próximamente se lanzará SET como forma segura de pago al mercado peruano. A partir de esa apertura los Comercios interesados podrán disponer

de un medio seguro para realizar transacciones en línea. Los bancos podrán certificarse con Visa para emitir certificados digitales a sus clientes que deseen comprar a través de Internet con la garantía SET.

Cadena de Confianza en el Perú:

Para que un Comercio pueda vender en Internet con la seguridad SET requiere: un certificado digital, una página Web en un servidor seguro (Con el Software SET).

El certificado digital se obtiene a través de Visanet. Los certificados tienen validez por un año.

La página web puede ser alojada en un servidor seguro propio del Comercio o en un servidor seguro rentado. Dicho servidor debe contar con el Software SET. Actualmente son dos los proveedores de software aprobado por SETCO IBM y Trintec. La inversión es muy variable, depende de la plataforma escogida, del volumen que se espera manejar.

4.5.1. Obtención de certificados SET en el Perú

Los términos y condiciones para obtener un certificado SET para toda entidad afiliada a Visanet pasan por necesariamente firmar un addendum al contrato de afiliación, el mismo que acuerda limitarse a los siguientes términos y condiciones para el uso del certificado SET:

1.- Este certificado digital SET emitido por Visanet, podrá ser utilizado únicamente para realizar transacciones electrónicas seguras, tal como lo define el addendum de comercio electrónico al contrato de afiliación que su establecimiento ha firmado y ha sido aceptado por Visanet.

2.- Por el presente el establecimiento acepta la divulgación de la información emitida en su solicitud para la obtención de su certificado digital SET a todas

las partes que requieran dicha información para procesar su solicitud.

3.- El establecimiento podrá utilizar únicamente su certificado digital SET para realizar transacciones con tarjeta Visa, no puede utilizar su certificado digital SET, aplicables o informaciones relacionadas a estos (criptografía, por ejemplo) para cualquier otro fin que no se relacione con transacciones con tarjetas Visa.

4.- El tiempo de duración de un certificado digital SET es de 01 año calendario a partir de la fecha de emisión del mismo, revocable a petición de parte.

5.- El establecimiento deberá tener el máximo cuidado en la creación, resguardo, manipulación y mantenimiento de su certificado digital SET. El establecimiento deberá utilizar una contraseña secreta, de su exclusivo conocimiento, para cuando necesite obtener acceso a su certificado digital SET, y/o firmar digitalmente cualquier información relacionada al certificado digital SET. El establecimiento escogerá una contraseña que no sea obvia, que contenga letras y números. En caso no se mantenga el secreto o se altere esta contraseña y se haga posible el uso indebido del certificado digital SET, eL establecimiento debe notificar inmediatamente a Visanet.

6.- El establecimiento usará su certificado digital SET solamente con programas compatibles con el mismo. Tales programas siempre estarán identificados con la marca SET.

7.- Visanet puede con absoluta discreción, aprobar o rechazar su solicitud para obtener su certificado digital SET o para reemplazar dicho certificado. Visanet emitirá una factura al establecimiento, conteniendo el costo de la emisión del certificado digital SET. El costo del certificado digital SET se incluyen en el addendum al contrato.

8.- El término o cancelación de su contrato de afiliación, automáticamente cancelara su certificado digital SET.

9.- Visanet puede cancelar el certificado digital SET en caso de que haya algún tipo de violación de uno de los términos y/o condiciones contenidos en el presente documento, en el contrato de afiliación o en el addendum a este referente al comercio electrónico, incluyendo el uso impropio del certificado digital SET o la sospecha que involucre la seguridad en la transacción.

10.- Por el presente el establecimiento renuncia a cualquier derecho de demanda judicial o no judicial en contra de Visanet por cualquier gasto o compensación, perdida o daño que surja de su participación en el comercio electrónico seguro, incluyendo sin ningún limite cualquier incumplimiento de la seguridad, integridad o mal funcionamiento de su software o certificado digital SET.

11.- Los presentes términos y condiciones no deben, por ningún motivo, ser interpretados como revocación, alteración, o agregado de las cláusulas u obligaciones contenidas en el presente contrato de afiliación del establecimiento y/o del anexo de este, relacionado a las transacciones del comercio electrónico seguro Visa - Vsec.

12.- El establecimiento se obliga a mantener en el más absoluto secreto las informaciones relacionadas a las transacciones con tarjetas Visa, así como aquellas relacionadas con el portador de la tarjeta, sin vincular ni hacer disponibles estas informaciones a terceros, sin la previa y formal autorización de Visanet.

13.- El establecimiento debe garantizar la entrega de la mercadería en la

dirección proporcionada por el cliente, dentro de los plazos pactados. Visanet no tendrá ninguna responsabilidad por la falta de entrega de la mercadería.

14.- En caso exista alguna modificación en la operativa de atención y distribución del establecimiento, este se hace responsable de la comunicación inmediata a Visanet.

4.5.2. Comercios Afiliados

Fig. 31 www.viacompras.com

Fig. 32 www.sagafalabella.com

Fig. 33 www.cosapidata.com

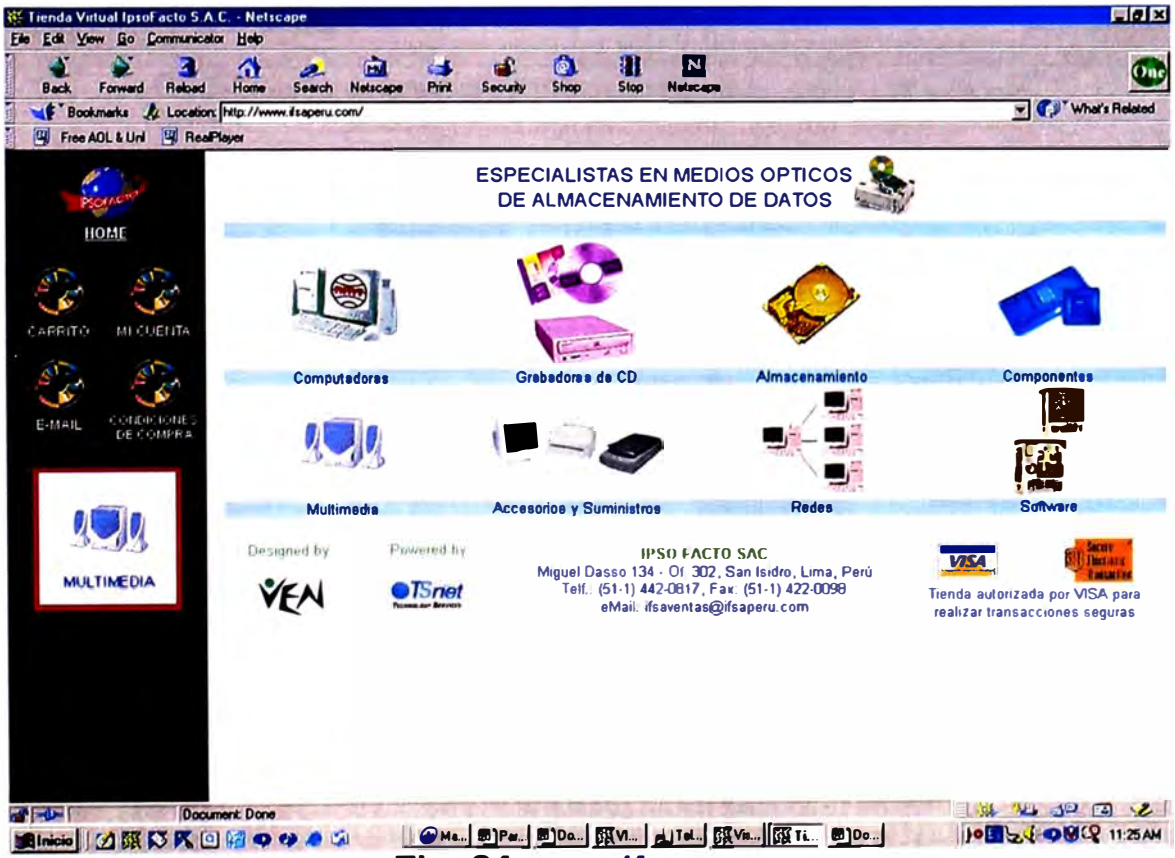


Fig. 34 www.ifsaperu.com

Fig. 35 www.teleamor.com

Fig. 36 www.cep.com.pe

Fig. 37 www.cep.com.pe

CAPITULO V
BASES LEGALES DEL COMERCIO ELECTRÓNICO EN EL PERÚ

El desarrollo del comercio electrónico, especialmente como factor de crecimiento de las PYMES, y como factor de competitividad de la industria, requiere eliminar dos grandes obstáculos. Por un lado el estado debe garantizar que Internet y las tecnologías que lo soportan sean accesibles no solamente a las empresas sino también a los ciudadanos de menores recursos. Por otro, la ausencia de una regulación a nivel de la región se constituye en una frontera legal para una generalización de Internet y los servicios que lo integran.

Los servicios que prestan las empresas en Internet cubren una amplia variedad de actividades en línea, que van de la simple información en línea, la publicidad en línea hasta la compra o contratación de servicios en línea. Para reforzar esta actividad se entiende que es indispensable iniciar o mantener comunicaciones o contactos comerciales. Estos contactos son esenciales para financiar los servicios directos e indirectos de los prestadores de servicios e incrementar el volumen de negocios derivados de estos servicios. Con relación a estos contactos comerciales los prestadores de servicios deben asumir un conjunto de obligaciones de distinto alcance. Con carácter general la empresa encargada de las comunicaciones comerciales debe identificar, claramente, la naturaleza comercial de tal comunicación, así como la titularidad o responsable de las mismas.

La promulgación de las recientes leyes Peruanas de firmas y certificados digitales (Ley 27269, 27310) además de otras que involucran legislación contra delitos informáticos (Ley 27309) es un gran avance en este campo en nuestro país, pero habida cuenta que Internet es un espacio virtual transfronterízo y de alcance universal que requiere una regulación internacional mas que regional, adicionalmente es necesario mencionar que antes de que el comercio electrónico sea una realidad, esta pendiente la solución de temas vinculados, como son, los aspectos tributarios, el tema de las leyes y sus jurisdicciones de aplicación y los derechos de propiedad intelectual.

A la fecha, en el Perú se tienen tres leyes aprobadas por el congreso de la Republica en Junio del 2000 y están referidas al B2B. Las demás modalidades de intercambio electrónico de información, tales como B2C, C2C entre otros, ya han tenido un desarrollo propio y ya son una realidad en nuestro medio (como es el caso de SET).

Tabla 7: Leyes Peruanas

Leyes vigentes en el Perú para el intercambio Electrónico de Información
Ley de Firmas y Certificados Digitales (Ley 27269, 27310)
Ley que modifica el Código Civil (Ley 27291)
Ley sobre Delitos Informáticos (Ley 27309)

Por otro lado, es importante mencionar que a la fecha se han trabajado cuatro proyectos de leyes, de los cuales solo se presentaron tres para su aprobación. El cuarto documento es el que contiene un proyecto de ley marco, bajo el concepto de la ley modelo UNCITRAL, adoptado casi íntegramente por la mayoría de los países de la región. Esta decisión de postergar este cuarto

proyecto tiene su origen en que el modelo UNCITRAL toca aspectos que aun no han sido definidos a nivel mundial, por lo tanto se considera prudente esperar a que maduren y se enriquezcan los conceptos jurídicos tales como: jurisdicción de aplicabilidad de las leyes, tributación, propiedad intelectual y tratamiento de la evidencia en juicios.

Después de la constitución Política del Perú, el código Civil es la Ley más importante ya que regula todas las relaciones humanas, desde el nacimiento de la persona hasta su muerte. Anteriormente, el código civil solo consideraba como posibles las transacciones de manera verbal o escrita. Como clases de manifestación de voluntad, las tradicionalmente aceptadas eran la expresa y la tacita, pero no se daba lugar a una tercera modalidad, es decir la contratación vía electrónica no se encontraba prevista en la legislación.

La Ley busca posibilitar que la voluntad pueda ser manifestado electrónicamente para lo cual se agrego el Art 141-A con relación a la manifestación de voluntad. Así mismo, el Art 1351 relativo a los contratos, no contemplaba esta posibilidad y traía a discusión el tema de la contratación entre presentes y entre ausentes. ¿Es la contratación electrónica una contratación entre presentes o entre ausentes?. El tema de la comunicación inmediata, no da certeza sobre la autenticidad de las personas contratantes. En el Perú se ha optado por considerar la contratación electrónica como contratación entre ausentes, a fin de dar mayor seguridad a la transacción motivo por el cual se hizo necesario modificar los conceptos relacionados a ese aspecto en el código civil.

En relación a los temas aun pendientes de solución, no solo se dan a nivel nacional, sino básicamente a nivel internacional. En el caso de la

tributación por ejemplo, en los Estados Unidos, actualmente no se graban las transacciones vía Internet (Internet Tax Freedom Act) debido a la complejidad del tema, en el caso especifico tributario, el concepto de ley territorial queda destruido con el desarrollo del comercio electrónico, ya que ya no es posible la aplicación de criterios territoriales. En estos casos, la administración tributaria ha perdido su soberanía fiscal, debido al desarrollo de la globalización y las transacciones electrónicas. La solución es la búsqueda de un consenso internacional, que defina como se va a manejar la tributación por transacciones realizadas vía Internet.

Aspectos Técnico Jurídicos de las Firmas y Certificados Digitales en el Perú

Si bien el tema ha sido discutido en muchos niveles y disciplinas, es difícil llegar a un concepto unificado de lo que es el comercio electrónico y cual es su contenido, si el estado debe o no intervenir en estos temas y en que medida, en cuestiones más operativas: que es una firma digital, cual es la diferencia entre firmas digitales y firmas electrónicas (incluso si existe una diferencia), el uso y regulación de los certificados digitales; son sólo algunos de los temas que hoy en día se debaten a nivel mundial en aras de encontrar la tan ansiada compatibilidad de los sistemas que permita el desarrollo del Comercio Electrónico Internacional.

La firma digital ha sido objeto de amplios debates no sólo a nivel internacional sino también nacional, nuestro país no se ha visto exento de participar en los debates: sea participando en reuniones a nivel internacional, como en debates nacionales sobre políticas y leyes aplicables.

Aunque para muchos estudiosos del tema ni las firmas ni los certificados

digitales son parte del "Comercio Electrónico", nadie puede negar que sin el uso de los mismos no se podrían desarrollar las situaciones que hoy en día ocupan sus investigaciones en general, y particularmente el E-Commerce.

Conceptos Fundamentales

Documentos Electrónicos y Documentos Digitales

Cuando nos referimos a documento utilizamos el concepto de la Ley Marco de UNCITRAL para mensaje de datos: "información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares", lo que nos interesa de este concepto es su aplicación al ámbito del sistema de certificación que se constituye en base para el desarrollo seguro de la contratación electrónica.

Electrónico: Será todo objeto creado, conservado y manejado a través de medios electrónicos, es decir, el soporte de su existencia es electrónico. No tiene existencia material necesariamente, pero podrían tenerla, por ejemplo al imprimir un documento electrónico.

Digital: Son aquellos objetos que no tienen existencia material, es decir, son creados por medio de Sistemas Tecnológicos de Información específicos, lo que les proporciona ciertas características como seguridad, integridad y no repudiación. Es una especie de lo electrónico.

Los documentos digitales también podrían materializarse, aunque no es necesario para darle las características arriba mencionadas. De suscitarse alguna diferencia entre el documento impreso, por ejemplo, y su original digital, en principio debería preferirse el documento digital por ser el original y contar con las características de seguridad.

Lo digital, por dichas características, resulta ser el más adecuado para

equipararse a los requisitos básicos que se exigen a los documentos tradicionales (en soporte papel). Se busca trasladar los conceptos e instituciones utilizados tradicionalmente a medios electrónicos, esto es Equivalencia funcional entre los usos que se le da a la firma manuscrita (autenticar documentos) y los que puede ofrecer la firma digital.

Los documentos digitales presentan beneficios adicionales que no se podrían obtener de una firma tradicional (manuscrita sobre papel). Mientras la firma manuscrita conserva todas sus características unificadas una vez que ha sido incorporada en el documento que quiere autenticar; la firma digital puede separar dichas características, debido a su propia naturaleza, y obtener efectos diferentes dependiendo de que características se desee utilizar.

Equivalencia funcional

Nuestro sistema normativo no tiene una definición de la firma manuscrita, ni tampoco una regulación de tipo específico al respecto. Por costumbre la firma se puede definir como un conjunto de caracteres escritos realizados por una persona para identificarse, se puede decir que forma parte de los rasgos de su identidad.

Debido a que dos personas no pueden tener la misma firma, ésta constituye un mecanismo idóneo para vincular al autor de la firma con los documentos en los que aplica su firma, de hecho hasta hace algunos años atrás era la única forma segura de autenticar un documento y su contenido, debido a que era susceptible de comprobación.

Se puede determinar mediante una pericia grafo técnica si la firma pertenece o no a la persona a quien se le pretende atribuir. Las funciones Hash son capaces de cumplir el mismo rol para las firmas digitales, que la pericia

grafo técnica para la firma manuscrita, con la ventaja adicional de que es una verificación inmediata.

La equivalencia funcional entre la firma manuscrita y la firma digital se logra asegurando que los medios tecnológicos empleados son adecuados para hacer que la firma digital tenga sobre los documentos electrónicos, los mismos efectos jurídicos que la firma manuscrita tiene sobre los documentos tradicionales.

La firma manuscrita revela el acuerdo del firmante con el contenido del documento y su conformidad con quedar obligado de acuerdo a dicho contenido. La firma es única por lo tanto el firmante no puede negar que le pertenece.

Dadas las características que la tecnología le da a la firma digital ésta cumple con igual efectividad las funciones de la firma manuscrita. Para cada función que el derecho reconoce a la firma, por ser inherentes a su naturaleza, la tecnología ha previsto un mecanismo que asegura el cumplimiento de dicha función.

Sistema de criptografía asimétrica

Se trata de dar mediante las matemáticas las características de seguridad adecuadas a los mensajes; basadas en un par de claves que se corresponden entre sí: una pública para conocimiento de los destinatarios y una privada de uso exclusivo del titular de la firma.

También es llamada Criptografía de Clave Pública (en alusión a una de las claves que emplea) ofrece una respuesta a los problemas de autentificación e integridad de los documentos electrónicos. Mediante una metodología

preestablecida se aplica una fórmula matemática a un documento electrónico cualquiera y se le convierte en una suma.

La aplicación de dichas fórmulas es una "Función Hash", al resultado que se obtiene de la mencionada aplicación se le cifra con la clave privada del emisor del mensaje; lo que finalmente se obtiene es la FIRMA DIGITAL, un "mensaje" ininteligible, a no ser que se le aplique la clave pública para descifrar el contenido.

5.1. Firmas Electrónicas y Firmas Digitales

La Firmas Electrónica de acuerdo a La Ley Marco de UNCITRAL se define como: datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos e indica que el titular de la firma aprueba la información contenida en el mensaje de datos.

Es un término genérico frente al de firma digital. Mientras la primera implica simple conformidad, la segunda va más allá, logra vincular al titular con el mensaje indubitablemente. La firma electrónica no necesariamente otorga la seguridad que da la firma digital, porque no están respaldadas por el Sistema de certificación de las Entidades de Certificación, Registro y Depósito; se pueden obtener por medio de software que generan las claves para el usuario. No existe una tercera parte involucrada en la transacción que de fe sobre el uso debido y la vigencia de la firma digital (de acuerdo al certificado respectivo).

La firma digital es, por excelencia, el instrumento de la seguridad en las transacciones electrónicas. Tienen ventajas innegables frente a la firma

electrónica: permite determinar, de forma fiable, la identidad de las partes que intervienen en las transacciones, y también si el contenido del contrato celebrado fue alterado de alguna forma posteriormente a la aplicación de la firma.

La firma digital, en sí misma, es difícil de conceptuar, se le suele definir a través de sus elementos, sus características y la forma como se usa, debido a que en realidad es un procedimiento, una aplicación. Quizá presente la misma dificultad de definición que la tan conocida firma manuscrita y al igual que ella "representa" en cierta medida a su titular, cumple las funciones de la firma manuscrita, pero no puede definirse en los mismos términos.

La firma digital es la transformación de un mensaje en un texto incomprensible, mediante la utilización de las claves pública y privada (cifrado asimétrico). Resulta tan efectiva en su función de dar seguridad al mensaje, porque al ser aplicada a éste se fusiona en él, además es distinta en cada mensaje en el que se aplica.

A diferencia de la firma manuscrita, la firma digital permite generar diversos efectos de acuerdo a como se usen las claves en el cifrado del mensaje. Primordialmente permite determinar inmediatamente: Si la transformación se hizo utilizando la clave privada correspondiente a la clave pública del firmante, si el mensaje firmado ha sido alterado desde que la transformación fue hecha.

Para determinar eficazmente lo antes mencionado, se deben cumplir los siguientes requisitos:

a. Depende de la persona que firma y del contenido de lo que se firma

b. Sólo el titular de la firma es capaz de crear la firma digital para un mensaje específico.

c. Cualquiera es capaz de verificar la firma digital pues tiene acceso a la clave pública del firmante.

5.2 Funciones Legales de las Firmas

Si bien nuestro sistema normativo no tiene una definición de la firma manuscrita, ni tampoco una regulación de tipo específico al respecto. Por costumbre la firma se puede definir como un conjunto de caracteres escritos realizados por una persona para identificarse, se puede decir que forma parte de los rasgos de su identidad.

Debido a que dos personas no pueden tener la misma firma, ésta constituye un mecanismo idóneo para vincular al autor de la firma con los documentos en los que aplica su firma, puesto que mediante una pericia grafo técnica se puede comprobar si la firma pertenece o no a la persona a quien se le pretende atribuir.

Paralelos a los requisitos de forma que las legislaciones puedan solicitar para la formación de contratos, las firmas electrónicas por sí mismas requieren observar algunas funciones legales, dichas funciones variarán según el sistema legal a que se apliquen:

5.2.1. Consentimiento

Cuando el titular firma, señala que conoce el contenido y que lo aprueba. El consentimiento debe reflejar la voluntad del firmante, por ello es absolutamente necesario que el autor del documento inicie el comando de firmado.

5.2.2. Prueba

En caso de alguna controversia los documentos digitales pueden ser usados como evidencia. Debido a que son verificables y seguros (cuando se aplica el sistema de certificación adecuada), son medios idóneos para poder crear convicción en el juez.

Permiten identificar al autor del documento y titular de la firma digital por lo tanto se comprueba que en uso de su autonomía de voluntad decidió obligarse en determinado sentido, lo cual consta en el documento firmado digitalmente.

5.2.3. Vigencia de la Firma

La firma digital debe tener un período de vigencia para su utilización. Se entiende que la entidad de certificación que maneja los datos ha verificado estos y existe un tiempo por el cual puede afirmar su certeza y veracidad con respecto a los hechos.

Dichos datos son tomados en cuenta por los terceros que se vinculan con el titular de la firma, por lo tanto es importante que conozcan el plazo durante el cual pueden confiar en que esa firma otorga plenos efectos vinculatorios respecto del titular.

Los documentos que contienen o comprueban la existencia de derechos deben ser conservados por un tiempo prudencial que permita verificar las condiciones de transmisión y uso de dichos derechos. El plazo máximo que contempla nuestra legislación es de 10 años, salvo los plazos establecidos en leyes especiales.

En principio los certificados de firmas electrónicas deben ser

conservados cuando menos por el tiempo que puedan existir derechos dependientes de ellos.

Cabe la posibilidad de que la persona titular del certificado de firma quiera cancelar el servicio que le presta la entidad de certificación con dicho certificado. Esto es perfectamente posible, pero por seguridad de los terceros debe figurar de manera adecuada para tener publicidad. Con la solicitud de cancelación del titular debe retirarse de la circulación el certificado.

También podría ocurrir que en ciertos casos la entidad de certificación tenga que revocar el certificado. Se debe dar la misma publicidad a dicha revocación que a la cancelación.

Los documentos y/o firmas deben ser manejados de tal modo que:

a. No puedan ser manipulados después de su cancelación, revocación o término de la vigencia.

b. Las firmas digitales anteriores sean verificables.

Es importante por ello, tener una Lista actualizada que publicite las firmas que han sido canceladas, revocadas o cuya vigencia ha expirado por el simple transcurso del tiempo.

5.2.4. Relacionar al Titular

La firma digital tiene que vincular al titular de la misma con el documento firmado, puesto que está dentro de su esfera de dominio.

Dicha correspondencia es declarada a través de un certificado, se emplea un sistema de reconocimiento que hace verificable que el documento fue enviado y firmado por el titular de la firma digital.

Tiene que declararse esa correspondencia porque si alguien diferente del titular tiene acceso a la clave privada puede firmar el documento. En tal

caso, la asignación de responsabilidades dependerá del uso que se haya dado a la firma y el titular tendrá que probar que no fue él quien firmó (entre otras cosas), para poder negar la transacción.

5.2.5. Oponibilidad

Los datos con los que cuenten las entidades para dar los certificados a los terceros que lo necesiten, deben ser veraces y recoger la información acorde con la realidad.

Implica que se identifique el rol de la persona firmante para determinar los efectos de la firma digital. Quien firma no sólo debe tener la capacidad jurídica exigida por leyes generales para la validez de los actos que pretende celebrar, sino que además debe estar facultado para generar los efectos jurídicos con el uso de la firma digital.

Para el caso de personas jurídicas se aplican las reglas generales de representación y apoderamiento. Porque no sólo pueden sus funcionarios tener firmas digitales propias, sino que deben estar autorizados para actuar en nombre de la persona jurídica.

5.2.6. Integridad

Los contratos son fiables solamente si corresponden exactamente con la voluntad de los contratantes. En el caso de los documentos digitales, su integridad depende del correcto empleo de las aplicaciones de firma y de la confidencialidad que se deposita en las certificadoras.

Quien verifique debe estar seguro de que la firma digital verificada no ha sido manipulada durante la transmisión de la comunicación. Para ello se emplean las funciones Hash, sobre las cuales se da información líneas más abajo.

5.2.7. Verificable

La identidad del titular de la firma, el rol y la razón de la firma deben ser susceptibles de verificación por medios de tecnología de la información. Los datos son confidenciales pero comprobables por determinados métodos que no afectan dicha confidencialidad.

Debido a que las claves están ligadas al titular mediante los certificados emitidos por las Entidades de Certificación respectivas, la verificación se hace a través de la clave pública y su correspondiente certificado pero sin tener acceso al contenido del certificado en sí
mismo, ni a la clave privada del titular de la firma.

5.2.8. De Advertencia

Para el caso de las firmas manuscritas es más evidente que cuando una persona, puede ser identificada plenamente y por lo tanto con su firma se obliga en el contenido del documento que firma.

En cuanto a las transacciones por medios electrónicos es necesario que exista información adicional que indique al titular de la firma que en el momento de emplearla se obliga en cuanto a los términos contenidos en el documento.

Las partes deben de estar informadas que el acto de firmar el documento trae consigo consecuencias legales. Hace que el firmante confirme que reconoce y acepta las implicancias legales de su firma.

5.3. Mecanismos Tecnológicos para realizar las funciones legales de las firmas digitales

Tecnológico implica que son mecanismos informáticos utilizados para realizar los requisitos legales en las firmas digitales.

Debido a que las firmas digitales no tienen inherentes a ellas las

características que tienen las firmas manuscritas, éstas les son atribuidas mediante mecanismos tecnológicos. Es decir, son medios para lograr la "equivalencia funcional"

La firma digital no puede existir independiente de un certificado digital que lo contenga, porque la firma, entendida como un conjunto de datos, es una característica del certificado. La aplicación correcta de los mecanismos tecnológicos requiere de todo un Sistema de Certificación adecuado, que no sólo implica medios tecnológicos sino también a las entidades que interactúan para conseguir la aplicación segura de los mismos.

5.3.1. Encriptación

Un texto legible normalmente es transformado en uno cifrado, el cual si la comunicación pudiera ser interceptada, no podría ser leída por el interceptor. Aún si fuese modificada, invalidaría el documento electrónico porque automáticamente se comprobaría la alteración del mismo.

En la encriptación asimétrica se utilizan un par de claves: una privada (que es secreta) usada para generar la firma digital, y otra pública (a la que todos tienen acceso) que se usa para verificar dicha firma digital.

La coherencia entre el contenido del documento y las atribuciones, limitaciones y demás datos que contienen los certificados es verificado por medio de funciones hash, que hacen posible claramente identificar al autor del documento electrónico, que acepte el contenido firmado como su voluntad (no repudio) y se pueda usar como evidencia en un eventual juicio, de ser el caso.

Los mecanismos de encriptación aseguran la integridad del documento y la identidad del titular de la firma, sólo en combinación con sistemas de certificación adecuados a ese propósito.

5.3.2. Entidades de Certificación

Entidad que da testimonio de la pertenencia o atribución de una determinada firma digital a un usuario o a otro certificador de nivel jerárquico inferior.

La emisión de certificados y la creación de claves privadas para firmas digitales acostumbran depender de una pluralidad de entidades que están jerarquizadas de una manera que las de nivel inferior obtienen su capacidad de certificación de otras entidades de nivel superior. Finalmente, en la cúspide de la pirámide suele hallarse una autoridad certificadora, que puede pertenecer al Estado, y que en el proyecto alemán coincide con el organismo que controla las telecomunicaciones. Las autoridades certificadoras tienen la función de emitir, suspender y revocar certificados, así como dar a conocer la situación actual de un certificado y crear claves privadas.

Los certificados indican la autoridad certificadora que lo ha emitido, identifican al firmante del mensaje o transacción, contienen la clave pública del firmante, y contienen a su vez la firma digital de la autoridad certificadora que lo ha emitido.

De esta manera, las partes que intervienen en una transacción aportan como credencial los certificados de su correspondiente entidad certificadora. Por ejemplo, la entidad certificadora A da fe de la identidad del usuario A1 cuando éste adquiere un bien al usuario B1, que es a su vez identificado por la entidad certificadora B.

Para llegar a ser una entidad certificadora deberá mediar una solicitud a una autoridad certificadora de nivel superior, que podrá denegar la licencia si el solicitante no ofrece la fiabilidad o los conocimientos necesarios, ni cumple los

requisitos establecidos en la ley.

No sólo otorgan y verifican los pares de claves sino que conservan y archivan información adicional

Toda la información contenida, sea sobre firmas, contratos o cualquier otro documento, no puede ser manipulada debe ser protegida su confidencialidad.

La Entidad de Certificación no es quien necesariamente asume las funciones que se necesitan para dar el respaldo y la credibilidad adecuada a los certificados, muchas veces actúa interrelacionado con otras entidades que asumen algunas de las funciones que se requieren. Dichas funciones son:

A. La función de certificación es la emisión misma del certificado como una aplicación tecnológica para seguridad de los documentos electrónicos emitidos conforme a los requerimientos de seguridad.

B. El registro de la información es cotejar la correspondencia de los datos y de la información del titular con la realidad. Se comprueban la veracidad de la información y la identidad del solicitante de la firma digital.

C. El almacenamiento de la información se hace sobre la estrictamente necesaria para el funcionamiento de la firma. No se puede atentar contra la privacidad de las personas conservando información irrelevante para la firma digital.

Será una decisión de administración de las certificadoras si es que ellas mismas realizarán las funciones de certificación, registro y almacenamiento o si trabajaran con otras entidades idóneas para cumplir con las funciones de registro y almacenamiento.

Dichas entidades intervienen como Terceros de confianza en las relaciones que las partes puedan llevar a cabo por medios electrónicos.

Toda la información contenida, sea sobre firmas, contratos o cualquier otro documento, no puede ser manipulada aleatoriamente, deben darse las condiciones adecuadas que aseguren su protección. Esto para no interferir con un derecho tan importante como lo es la Privacidad de la información, por lo tanto debe dársele carácter de confidencial.

5.3.3. Concepto de Certificados Digitales

Son aquellos documentos digitales que contienen datos que permiten identificar a la persona que usará la firma, la clave pública y confirma que el firmante identificado con el certificado posee exclusivamente la clave privada correspondiente a la clave pública contenida en el certificado.

El certificado tiene la función primordial de hacer seguros los documentos electrónicos mediante el uso de firmas digitales, debido a que no sólo vincula la clave pública con su respectiva clave privada, sino que además vincula indubitablemente ambas claves con su titular.

Contienen toda la información relevante, sea sobre firmas, contratos o cualquier otro documento, para dar el respaldo adecuado a las firmas digitales y pueda verificarse eficientemente la correspondencia de las claves con el titular, la identidad de éste, sus atribuciones y limitaciones.

Debido a que se pueden establecer firmas para determinados actos y vinculadas exclusivamente a las personas, es importante recalcar que los efectos que puedan generar las firmas están directamente relacionados con la información que la entidad de certificación recabe y verifique para el otorgamiento del certificado. Esto se hace así para otorgar protección y

seguridad a quienes quieren contratar por medios electrónicos. Para que los certificados puedan cumplir con su finalidad se requiere no sólo de una entidad que actúe como tercero "verificador" en las transacciones, primordialmente se requiere que se cumplan ciertas "funciones" eficazmente, sin importar la "persona" que las realiza, en sí misma.

El Certificado Digital además identifica a la autoridad certificadora que lo ha emitido, identifica al firmante del mensaje o transacción, contiene la clave pública del firmante, y contiene a su vez la firma digital de la autoridad certificadora que lo ha emitido (tiene todas las características de seguridad que lo hacen confiable).

5.3.4. Funciones Hash

Son funciones matemáticas por las que un "mensaje" de información corriente, es transformado en una suma decimal. Éstas sumas se utilizan para notar una coherencia cercana entre los contenidos del documento y la firma digital.

Al mensaje que se desea enviar se le aplica la función hash y la suma resultante es lo que se firma digitalmente.

Si sólo una letra del mensaje original es cambiado, la función hash genera una sumatoria que es diferente de la calculada y firmada inicialmente. Mediante este hecho se puede comprobar que el documento fue alterado con posterioridad a su envío, lo que provocaría
que no sea idóneo para producir los efectos que se pretendían de acuerdo a su contenido.

La firma digital otorga certeza de la integridad del documento. Una vez

que se ha cambiado algún dato, es inútil para cualquiera que reclame ser el titular de la firma.

Las funciones Hash aplicadas a una firma digital cumplen la misma función que un peritaje grafo técnico respecto de la firma manuscrita, con la amplísima ventaja de que es automático, se obtiene la verificación inmediata.

Cuando se aplican a un documento dan como resultado una suma determinada, de alterarse algún dato por mínimo que este sea, la función Hash lo revela dando un resultado diferente al que inicialmente se obtuvo de dicho documento.

5.4. Marco Legislativo Actual

Las regulaciones marco para asegurar la autenticación deben facilitar el desarrollo y la difusión de las tecnologías de autenticación existentes sin por ello constituir una desventaja para las tecnologías emergentes.

La primera ley que ha regulado los aspectos jurídicos de la firma digital como instrumento probatorio se aprobó el año 2000 en Utah, luego surgieron proyectos en Georgia, California y Washington. En Europa, el primer país que ha aprobado una Ley sobre la materia ha sido Alemania.

Sin embargo es necesario notar que la eficacia de éste tipo de leyes radica en su uniformidad, puesto que si su contenido difiere hasta hacerlas incompatibles, será difícil su aplicación a un entorno global como Internet.

El esfuerzo que se viene realizando es conseguir un modelo que pueda ser implantado de manera uniforme en las leyes nacionales. Tal tarea puede encomendarse a organismos internacionales como UNCITRAL, que ya dispone de experiencia en iniciativas similares en materia de EDI.

Siguiendo esta idea, fue formulado el año 2000 en nuestro el Proyecto de Ley Nº 5070-99 CR por el congresista Jorge Muñíz, el cual fue aprobado por unanimidad por la Comisión de Reforma de Códigos para su presentación a debate al pleno del Congreso de la República. Además de los Proyectos sobre Contratación Electrónica y el sobre Delitos Informáticos.

El Dictamen de la Comisión de Reforma de Códigos tomó en consideración tanto antecedentes legislativos propios de nuestras leyes como legislación comparada para aprobar el Proyecto de Ley, ellos reflejan la importancia que tiene en nuestro medio la dación de una ley de este tipo y sobre todo la coherencia que debe guardar no sólo con modelos internacionales (para su operatividad) sino con el ordenamiento legislativo nacional.

5.4.1. Antecedentes Legislativos de la ley peruana

La Constitución Política del Perú dispone en su art. 58 que ".... El Estado orienta el desarrollo del país, y actúa principalmente en las áreas de promoción de empleo, salud, educación, seguridad, servicios públicos e infraestructura.", resulta necesario dar un marco legal adecuado que permita el desarrollo de las distintas empresas a través de una nueva forma de acceder al mercado.

Debido al proceso de Globalización de la economía que se viene dando a nivel mundial, el acceso a los mercados a través de medios electrónicos se presenta como una necesidad de toda empresa, grande o pequeña, para poder competir.

En el art. 59 la Constitución Política del Perú establece que "El Estado estimula la creación de riqueza y garantiza la libertad de trabajo y la libertad de empresa, comercio e industria."

Además en el último párrafo del mencionado artículo dispone que "El Estado brinda oportunidades de superación a los sectores que sufren cualquier desigualdad; en tal sentido, promueve las pequeñas empresas en todas sus modalidades."

Es una gran oportunidad de desarrollo de las PYMES y de las exportaciones del país debido a que permite que la oferta llegue a los consumidores potenciales libre de las diferencias del país de origen, del tamaño de la empresa y con una inversión menor a lo que hubiese costado un ingreso físico en el mercado.

También resultaría un incentivo para la comercialización de productos al interior del país por la facilidad de acceso.

El Art. 61 de la Constitución Política establece que "El Estado facilita y vigila la libre competencia. Combate toda práctica que la limite y el abuso de posiciones dominantes o monopólicos.", por lo tanto, fluye de la razón de la norma que es de interés general la promoción de mercados internos competitivos que puedan integrarse a la economía mundial y generen un crecimiento económico para el país.

En concordancia con el Art. 1354 del Código Civil que establece que "Las partes pueden determinar libremente el contenido del contrato, siempre que no sea contrario a normas de carácter imperativo.", entonces el Estado debe disponer la manera más adecuada para que los privados puedan ejercer este derecho, definiendo los marcos legales que permitan el desarrollo de nuevos mercados a través de medios electrónicos.

Las Naciones Unidas a través de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) determinó mediante un de

informe que dicho acceso al mercado a través de medios electrónicos requiere un Sistema de certificación que permita que la "firma" generada por medios electrónicos tenga las funciones que la firma manuscrita tiene para producir efectos jurídicos.

5.4.2. Legislación Comparada

La mayoría de legislación internacional recientemente adoptada se basa en la Ley Modelo UNCITRAL por ser flexible, de ser adaptada a la legislación propia de cada país. A su vez plantea marcos tecnológicos que permiten en cierta forma uniformizar este acceso electrónico a los mercados, evitando que se generen barreras que obstaculizarían el desarrollo de las economías.

La finalidad de la Ley Modelo es la de ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permita un desarrollo más seguro de las vías electrónicas de negociación.

Distintos países latinoamericanos han desarrollado ya la legislación pertinente para la implementación de las firmas electrónicas. En muchos casos el sector público ha sido el primero en ser regulado y en poner en práctica dichos medios electrónicos.

La legislación colombiana mediante la Ley 527, que define y reglamenta el acceso y uso de mensajes de datos, del comercio electrónico y de las firmas digitales, y establecen las entidades de certificación y otras disposiciones, en su Art. 2, define:

Firma Digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido,

vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación; Entidad de Certificación. Es aquella institución que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

La República Argentina tiene una Comisión Redactora del Anteproyecto de Ley de Firma Digital cuyo Art. 1 señala que el objeto de dicha ley es ".... habilitar el empleo de la firma digital dentro del principio de libertad de formas". El uso de una infraestructura de Firma Digital para el Sector Público se ha regulado mediante el Decreto Nº 427.

Chile mediante el Decreto Nº 81 del presente año, ha regulado el uso de la firma digital y los documentos electrónicos en la administración del Estado

En países latinoamericanos como Brasil y Ecuador, se han presentado Anteproyectos de Ley sobre el tema de la firma electrónica.

México ha planteado el tema de las firmas electrónicas como un motivo de reforma de su código de comercio.

La Propuesta de Directiva del Parlamento Europeo establece las normas básicas para que los países miembros se adapten a ellas, y sea factible desarrollar el comercio por medios electrónicos. Las legislaciones nacionales deben de adaptarse a ella sólo en caso de que sea necesario, pero en ningún caso podrán desconocer normas de protección de salud pública o del

consumidor, recogidas en documentos comunitarios.

Los países latinoamericanos no están fuera de la tendencia actual, de reconocer que el uso de medios electrónicos en el comercio, tanto interno como externo, al reconocer que éste ofrece importantes beneficios que deben ser aprovechados para el desarrollo económico de los países.

La legislación existente y la que se pueda dar a futuro es sólo un afán para dotar de un marco jurídico a una realidad social creciente (no sólo en los países más desarrollados tecnológicamente, sino también en los receptores de la tecnología). En este orden de ideas, tenemos que considerar que la decisión de política legislativa que se tome, con respecto de las firmas y los certificados digitales, es trascendental para el desarrollo del comercio en general.

Es importante acotar que el proceso de reglamentación de las leyes antes citadas está siendo estudiado por los distintos países en Comisiones especialmente encargadas para ello. En España se promulgó recientemente el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, el 21 de febrero del 2001.

El reglamento español establece un doble sistema de "evaluación", no sólo del Prestador del Servicio de Certificación, sino del "producto" informático que el mercado ofrece y que dichas entidades utilizan para administrar la información. Es un sistema voluntario que funciona como un sello de calidad

Se implementó de ésta manera con una finalidad clara de fomentar la adopción de prácticas que garanticen que los servicios y los productos se ofrecen en condiciones satisfactorias de Calidad y Seguridad técnica. Es mejor que los mismos agentes del mercado internalicen éste tipo de conductas y las

apliquen a sus servicios como parte de su política económica.

La acreditación, bien sea de la Entidad o del producto, la otorga la Secretaría General de Comunicaciones del Ministerio de Fomento mediante la emisión de una Resolución que confirma la evaluación hecha por unos organismos privados especialmente encomendados a éste fin.

Los organismos de evaluación son autorizados por la Entidad Nacional de Evaluación a través de "Convenios de Colaboración". Dicha entidad se encarga de su evaluación y aprobación para asegurar que tenga la tecnología necesaria para evaluar los productos y a los Prestadores de Servicios de Acreditación.

5.5. Aplicación de la ley: Casos Prácticos

Aunque aún no se han presentado casos reales, por lo menos no de los cuales se tenga conocimiento en el país, los casos prácticos hipotéticos presentados a continuación, son un ejercicio útil en la comprensión de la Ley de Firmas y Certificados Digitales que se debate actualmente en el Congreso de la República.

1º Desconocimiento de una firma digital

JUGOS S.A. es un distribuidor de jugos naturales que ha decidido ofrecer a sus consumidores mayoristas una forma más rápida de hacer sus pedidos, a través de su página en Internet, para lo cual informó a todos sus clientes de la nueva opción que ofrecía. Ana, propietaria de una bodega y cliente de JUGOS S.A., decide tomar los servicios de MEGA, entidad de certificación, para obtener un certificado digital.

MEGA recopila los datos que necesita de Ana para identificarla plenamente, los verifica a través de su oficina de registro (que hace las veces

de la entidad de registro) y los almacena en su propio banco de datos. Luego emite el certificado digital para Ana, conteniendo la clave pública, los datos de Ana, los datos de MEGA, la metodología que se usa para verificar la firma digital, el número de serie del certificado y la vigencia con la que se otorga.

Ana recibe la clave privada que corresponde a su clave pública y suscribe para MEGA un documento, con fecha y hora de entrega, de conformidad con los datos que contiene su certificado por considerarlos fidedignos. Luego ingresa al catálogo de JUGOS S.A. En su página, revisa la información sobre los productos y decide hacer un pedido de 3 cajas de 24 botellas del nuevo jugo de Tuna, ingresa a la página de pedidos de compra, revisa los términos del contrato y firma digitalmente su compra aplicando su clave privada.

Por la noche, en un restaurante, Ana prueba el jugo de Tuna y no le agrada. JUGOS S.A. comprueba a través de MEGA que el certificado corresponde a Ana y envía el pedido. En la mañana cuando llega su compra, Ana niega haber hecho el pedido de compra, alegando que otra persona pudo hacerlo en su nombre o que pudo ser un error de MEGA. JUGOS S.A. demanda la indemnización por daños y perjuicios originados por incumplimiento de obligación contractual contra Ana.

Aplicación

Mega.- Fue diligente y verificó los datos de Ana como debía, se aseguró de entregar la clave privada personalmente a Ana, además documentó la conformidad de Ana con los datos del certificado y puede probar la fecha y hora de entrega. No es responsable por el uso indebido del certificado digital.

JUGOS S.A.- Tenía las características de sus productos (información relevante) al alcance de sus clientes, los términos del contrato estaban claros,

tenía una página distinta del catálogo para que sus clientes realicen sus pedidos de compras.

Ana.- Cuando Ana accedió a la página de compras era claro que se obligaba. Tenía la información a su alcance y no puede negar que ella hizo el pedido pues la clave privada con la que se aplica la firma sólo la conocía ella. Si adujese que alguien más tuvo acceso a su clave, sería negligencia suya no imputable ni a JUGOS S.A. ni a MEGA. Para negar su responsabilidad tendría que probar que el certificado fue emitido en condiciones inseguras y dados los antecedentes del caso no podrá hacerlo.

2º No verificación de autenticidad del certificado

Modificando el supuesto anterior podemos obtener un resultado diferente de la aplicación de la ley. Supongamos que Ana, quien trabaja en una imprenta y es la encargada de los pedidos al proveedor de papelería, perdió su clave privada contenida en un disquete, por lo tanto, tuvo que solicitar a MEGA la cancelación inmediata de su certificado digital. MEGA, una vez recibida la solicitud automáticamente canceló el certificado de Ana.

Al siguiente día Carlos, quien fue despedido el día que Ana perdió el disquete, lo encontró accidentalmente en las oficinas, al revisar su contenido y darse cuenta de que era la clave privada que Ana utilizaba, decidió hacer compras a nombre de la empresa. Entró a la página de PAPEL S.A., proveedor de papel, y realizó un pedido de 100 millares del papel más caro que encontró, también se contactó con la página de INK, proveedor de la tinta que utilizaban en la impresión y realizó otro pedido 10 cajas de tinta de cada uno de los 50 colores que normalmente usaban en la impresión.

En PAPEL S.A. el encargado de procesar los pedidos para el almacén,

conocía que era un pedido de Ana y no solicitó la autenticación del certificado usado para realizar la compra y simplemente tramitó el pedido. Cuando llegó el pedido de papel, Ana se negó a recibirlo porque la clave utilizada en el pedido fue cancelada con el certificado respectivo.

INK verificó con MEGA el certificado digital que correspondía al pedido y lo encontró cancelado. Además decidió confirmarlo por teléfono y Ana les informó que no requerían el pedido, por lo tanto no lo tramitaron.

Aplicación

Mega.- Actuó de acuerdo a lo que estipula la ley, cancelando el certificado digital automáticamente con la solicitud del titular, en razón de lo cual no tiene responsabilidad alguna de los daños que sufrió PAPEL S.A.

Ana.- Fue diligente y realizó un uso adecuado de sus claves y su certificado, por lo que no le es exigible que acepte los pedidos que llegaron mediante el uso de la clave cancelada con anterioridad.

PAPEL S.A.- No tuteló adecuadamente sus intereses, fue negligente al dar trámite a un pedido hecho por medios electrónicos sin hacer la debida comprobación del contenido y la vigencia del certificado. Por éste motivo no podría tratar de imputar culpabilidad en ninguno de los otros "participantes" en la transacción.

INK.- No sólo fue diligente al verificar el certificado con el que se presentó el pedido de compra, sino que además se preocupó de su imagen empresarial, lo cual es sumamente importante debido a que éste tipo de transacciones se basan en la confianza entre las partes.

Carlos.- No sólo es responsable civil de daños y perjuicios ocasionados a PAPEL S.A. sino que incluso se le puede imputar responsabilidad de tipo

penal, cometió un fraude.

3º Entidades de Certificación que no trabajen con una adecuada Entidad de Registro

Tomemos ahora el supuesto de que MEGA sea una Entidad de Certificación extranjera que distribuye sus certificados a nivel internacional totalmente "en línea". Ana es una usuaria local que tiene un negocio de importación de artesanía.

Ana solicita un certificado digital a la empresa ABC (entidad de certificación extranjera), que trabaja con una Entidad de Registro que verifica los datos del solicitante del certificado antes de comunicar a ABC que puede emitirlo. ABC entregará el certificado a Ana a través de la Entidad de Registro, una vez que ella pruebe indubitablemente su identidad.

Fernando competencia de Ana, decide contactarse con MEGA y solicitar un certificado digital con el nombre de Ana y dando datos falsos. MEGA le entrega el certificado a Fernando sin verificar si los datos presentados por éste coinciden con la realidad o no. Con el certificado Fernando se pone en contacto con unos inversionistas (quienes no verifican la autenticidad del certificado que utilizan para enviarles las ofertas) y cierra un negocio a nombre de Ana para incumplir luego.

Aplicación

Mega.- Es una empresa que no opera dentro de los estándares internacionales de seguridad. No está registrada ante la Autoridad Administrativa nacional, por lo tanto no se avala la seguridad de los medios que emplean. Es responsable por emitir un certificado que induce a error a los contratantes, acreditan la identidad que no han verificado en la realidad.

No es responsable por el negocio realizado a su nombre, MEGA no tiene como probar si fue ella quien realmente solicitó el certificado utilizado para cerrar la transacción.

Fernando.- Es responsable civil (daños y perjuicios) y penal (fraude). Pero como MEGA no verifica la información que se le proporciona al solicitar los certificados, no puede imputarle responsabilidad alguna.

ABC.- Es una empresa que respeta los estándares internacionales de seguridad, esto es comprobado por la Autoridad Administrativa y figura en sus registros de empresas que operan de forma segura. Los verdaderos afectados serán quienes contrataron en base al certificado con datos falsos. Pero como también fueron negligentes al no comprobar la autenticidad del certificado, difícilmente podrán obtener un resarcimiento de MEGA.

CONCLUSIONES

Hace una década atrás, nadie esperaba que Internet, o mas concretamente, la World Wide Web, creciera al ritmo exponencial de los últimos años, sus posibilidades para el comercio fueron rápidamente vislumbradas llegando a convertirse en un tiempo record en el teatro de transacciones comerciales, financieras y de todo tipo. Había que vender, pero vender ya. No podía esperarse a magníficos estándares que velaran por la rigurosa implementación de todos los detalles, es de esta forma que, viendo la facilidad del método de pago con tarjeta de crédito, esta termino por imponerse, y como respuesta a las preocupaciones de los usuarios por la seguridad se estableció el uso de canales seguros para la transmisión de los números de las tarjetas de crédito. Fue así como en poco tiempo se impuso como norma tácitamente acordada el emplear SSL para facilitar / asegurar el envió de datos personales, entre ellos el numero de tarjeta de crédito.

Como se vio, SSL es un protocolo de propósito general para establecer comunicaciones seguras, propuesto en 1994 por Netscape Corporation y que hoy en día se constituye en la solución de seguridad implantada en la mayoría de los servidores web que ofrecen servicios de comercio electrónico, debido principalmente a que la arquitectura SSL no exige que el servidor disponga de capacidades especiales y que para asegurar la transmisión de los datos le basta con el establecimiento de un canal seguro para transmitir la información de pago, ya que el comerciante se ocupara manualmente de gestionar con su

Banco las compras. Sin embargo, este enfoque, aunque práctico y fácil de implementar, no ofrece una solución comercialmente integrada ni totalmente segura debido principalmente a que los navegadores utilizan normalmente claves de 40 bits de longitud, las cuales son "fáciles" de romper. Realmente SSL deja de lado demasiados aspectos para considerarse la solución definitiva como son:

- Solo protege transacciones entre dos puntos (el servidor del comerciante y el navegador del comprador). Sin embargo, una operación de pago con tarjeta de crédito involucra mínimo tres partes: el consumidor, el comerciante y el emisor de la tarjeta.
- No protege al comprador del riesgo de que un comerciante deshonesto utilice ilícitamente su tarjeta.
- Los comerciantes corren el riesgo de que el numero de la tarjeta de un cliente sea fraudulento o que esta no haya sido aprobada.

Como se ve, son demasiados los problemas e incertidumbres como para dejar las cosas como están, de modo que se hacia necesaria la existencia de un protocolo mas especifico para el pago que superase todos los problemas e inconvenientes anteriores, motivo por el cual se creo SET.

La gran ventaja de SET con relación al SSL es que este protocolo ofrece autenticación de todas las partes implicadas en la transacción (el cliente, el comerciante y los bancos, emisor y adquiriente) además de confidencialidad e integridad gracias a las técnicas criptográficas robustas que impiden que el comerciante acceda a la información de pago (eliminando así su potencial de fraude) y que el banco acceda a la información de los pedidos (previniendo que confeccione perfiles de compra). SET ofrece la gestión del pago mediante la

gestión de tareas asociadas a la actividad comercial, como son: registro del titular y del comerciante, autorizaciones y liquidaciones de pago, anulaciones, etc.

Entonces, si SET es tan bueno, por que no termina por implantarse y por que no goza de la popularidad del SSL. En primer lugar el despliegue de SET esta siendo muy lento debido principalmente a que exige software especial tanto para el comprador (aplicación monedero electrónico) como para el comerciante (aplicación POST o terminal de punto de venta) que se esta desarrollando con lentitud, en segundo lugar, por que aunque varios productos cumplan con el estándar SET esto no significa que necesariamente sean compatibles. Sus puntos fuertes son también su talón de Aquiles ya que la autenticación de todas las partes exige rígidas jerarquías de certificación, ya que tanto los clientes como los comerciantes deben adquirir certificados distintos para cada tipo de tarjeta de crédito, trámites que resultan por demás engorrosos para la mayoría de los usuarios comunes y corrientes.

En definitiva, SET es un elefante de gran tamaño y fuerza pero de movimientos extremadamente pesados, por otro lado SSL es una liebre que le ha tomado la delantera hace años. No es tan perfecto, no ofrece la seguridad y las garantías de SET, pero funciona. Y lo que es más importante: un usuario común y corriente no tiene que hacer nada mientras SET llega a la meta o muere en el camino.

Las leyes son importantes en el desarrollo del tema del comercio electrónico pues son la base sobre la que las transacciones pueden darse en términos seguros. La seguridad es muy importante en el mercado digital, no sólo la seguridad tecnológica sino también la jurídica; ambas se desarrollan

paralelamente y depende una de la otra.

Un marco jurídico adecuado contribuirá a que el ya acelerado crecimiento del comercio electrónico sea seguro para todos los agentes del mercado. Es necesario acabar con mitos como el que afirma que es aún mayor la dificultad de probar la existencia de obligaciones celebradas y contenidas en medios electrónicos. La verdad es que si se es cuidadoso al documentar adecuadamente las transacciones que se realiza no se pueden tener problemas ni en documentos en soporte papel ni en documentos de soporte electrónico. Después de todo esta nueva manera de hacer negocios gana más adeptos día a día y es necesario estar preparados para afrontar la masificación de su uso.

ANEXOS

ANEXO A
LEY DE FIRMAS Y CERTIFICADOS DIGITALES (Ley No. 27269)

LEY No. 27269

Promulgada el 26.MAYO.2000

publicada el 28.MAYO.2000

Ley No. 27269

EL PRESIDENTE DE LA REPÚBLICA;

POR CUANTO:

El Congreso de la República ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

Artículo 1o.- Objeto de la ley

La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Artículo 2o.- Ámbito de aplicación

La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos,

puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

DE LA FIRMA DIGITAL

Artículo 3o.- Firma digital

La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

DEL TITULAR DE LA FIRMA DIGITAL

Artículo 4o.- Titular de la firma digital

El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5o.- Obligaciones del titular de la firma digital

El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

DE LOS CERTIFICADOS DIGITALES

Artículo 6o.- Certificado digital

El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Artículo 7o.- Contenido del certificado digital

Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación.

Artículo 8o.- Confidencialidad de la información

La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley. Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9o.- Cancelación del certificado digital

La cancelación del certificado digital puede darse:

1. A solicitud del titular de la firma digital.
2. Por revocatoria de la entidad certificante.
3. Por expiración del plazo de vigencia.
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10o.- Revocación del certificado digital

La Entidad de Certificación revocará el certificado digital en los

siguientes casos:

Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.

1. Por muerte del titular de la firma digital.
2. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.

Artículo 11o.- Reconocimiento de certificados emitidos por entidades extranjeras

Los Certificados de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

DE LAS ENTIDADES DE CERTIFICACIÓN Y DE REGISTRO

Artículo 12o.- Entidad de Certificación

La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.

Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.

Artículo 13o.- Entidad de Registro o Verificación

La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de

certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Artículo 14o.- Depósito de los Certificados Digitales

Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley.

El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización.

A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten.

Artículo 15o.- Inscripción de Entidades de Certificación y de Registro o Verificación

El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades.

La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales.

Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación.

Artículo 16o.- Reglamentación

El Poder Ejecutivo reglamentará la presente ley en un plazo de 60 (sesenta) días calendario, contados a partir de la vigencia de la presente ley.

DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES

PRIMERA.- Mientras se cree el Registro señalado en el artículo 15o, la validez de los actos celebrados por Entidades de Certificación y Entidades de Registro o Verificación, en el ámbito de la presente ley, está condicionada a la inscripción respectiva dentro de los 45 (cuarenta y cinco) días siguientes a la creación el referido Registro.

SEGUNDA.- El Reglamento de la presente ley incluirá un glosario de términos referidos a esta ley y a las firmas electrónicas en general, observando las definiciones establecidas por los organismos internacionales de los que el Perú es parte.

TERCERA.- La autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los ocho días del mes de mayo del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO

Presidenta del Congreso de la República

RICARDO MARCENARO FRERS

Primer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de mayo del año dos mil.

ALBERTO FUJIMORI FUJIMORI

Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE

Presidente del Consejo de Ministros y

Ministro de Justicia

ANEXO B
LEY QUE MODIFICA EL ART. 11° DE LA LEY N° 27269 (Ley N° 27310)

LEY No. 27310

Promulgada el 26.Junio.2000

Publicada el 28.Junio.2000

Ley No. 27310

EL PRESIDENTE DE LA REPÚBLICA;
POR CUANTO:

El Congreso de la República ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Antecedentes:

Artículo 11 y los problemas del reconocimiento.

De la redacción actual del artículo 11 se desprende que la validez y eficacia jurídica de los certificados digitales emitidos por Autoridades de Certificación Extranjeras, está condicionada al reconocimiento que ésta reciba de una Autoridad de Certificación Nacional. Es decir, cualquier entidad certificadora nacional definiría en ultima instancia, el habilitar el normal funcionamiento de una entidad certificadora extranjera en el mercado peruano.

Si lo que en el fondo se busco al promulgar la Ley 27269 era ampliar nuestros mercados vía Internet, facilitar el comercio electrónico en general y ser agentes activos en este escenario global, el reconocimiento que exige la ley a los certificados emitidos por entidades extranjeras cierra, en la actualidad, el

mercado a la libre competencia.

Con esta condición potencialmente se estaría impidiendo dos cosas:

- Que los usuarios cuenten con certificados digitales de Autoridades de Certificación Extranjeras que ostenten un respaldo financiero y tecnológico reconocido en el ámbito internacional.
- Que los usuarios puedan tener plena libertad de elección en cuanto a la calidad y precio de la prestación del servicio.

Artículo 11 y el incipiente mercado de certificación digital peruano.

En una primera aproximación, se puede apreciar que actualmente en el ámbito nacional, no existen Autoridades de Certificación nacionales por lo que se pone una barrera a la entrada de Autoridades de Certificación Extranjeras a nuestro mercado puesto que no habría quien reconozca en el corto plazo.

De una rápida evaluación en función a la demanda del mercado, se evidencia una limitación para la constitución de entidades de certificación nacionales dado el alto costo de inversión para constituir la infraestructura requerida para este tipo de empresas, situación que podría facilitar la existencia de un monopolio.

Adicionalmente, en el supuesto de que exista la intención de invertir en la infraestructura requerida para una autoridad de certificación nacional, a ésta no le interesaría que reconocer los certificados de una entidad de certificación extranjera pues ésta sería su competencia directa; amenazando su mercado durante el período de recuperación de la inversión.

Luego, sería probable que a las entidades de certificación nacionales no les interese el reconocer la validez y eficacia jurídica a certificados emitidos por entidades extranjeras, con lo cual éstas verían restringidas

sus posibilidades de competir y ofrecer sus servicios en el mercado peruano.

Artículo 11 y su relación con la Constitución Política del Perú.

En un análisis normativo, a nivel constitucional, este artículo de la ley entra en conflicto con el artículo 63 de la Constitución Política del Perú, que a la letra prescribe: "La inversión nacional y la extranjera se sujetan a las mismas condiciones". Además especifica claramente que: "La producción de bienes y servicios y el comercio exterior son libres". En ese sentido, el artículo 11 de la Ley 27269 hace que las entidades de certificación nacionales y extranjeras no estén en las mismas condiciones jurídicas pues las segundas quedan supeditadas al reconocimiento de las primeras.

De otro lado, mediante este mecanismo, se le dota a las entidades de certificación nacionales de un poder de mercado innecesario pues, mediante el reconocimiento podrían controlar el número de entidades de certificación extranjeras en el mercado peruano o inhibir la entrada de las mismas mediante entidades de registro, en el considerando que los agentes económicos podrían evitar adquirir estos certificados digitales al carecer de valor y eficacia jurídica.

De lo anterior, se puede observar que el mecanismo de reconocimiento puede generar un conflicto de intereses no deseado por la ley en su conjunto, ya que finalmente ambos son agentes prestadoras del servicio en el mercado.

Por lo tanto, colisionaría con una de las funciones fundamentales del Estado que es, según el artículo 61 de la Constitución, facilitar y vigilar la libre competencia.

Recordando que el espíritu de instituir la figura de las Entidades de Registro era crear un mecanismo para facilitar la importación de los servicios de certificación digital, el artículo 11 de la ley contraviene el artículo 63 de la

Constitución en la parte que señala que: "La producción de bienes y servicios y el comercio exterior son libres".

Artículo 11 y su relación con las leyes de inversión extranjera.

Adicionalmente, nuestra legislación no desconoce este valor de la igualdad de condiciones entre lo que es fuente de inversión extranjera y lo que constituye la inversión nacional, ambos requeridos y favorecidos para el desarrollo económico de nuestro país.

Justamente, encontramos que existe un conflicto entre la Ley 27269 y el Decreto Legislativo N° 662 que sobre la Inversión Privada, declara en su artículo 1:

"El Estado promueve y garantiza las inversiones extranjeras en el país, en todos los sectores de la actividad económica y en cualquiera de las formas empresariales o contractuales permitidas por la legislación nacional."

Seguidamente determina:

"Para estos efectos, serán considerados como inversionista extranjeros las inversiones provenientes del exterior que se realicen en actividades económicas generadoras de renta (...)".

Pero donde se revela ese valor o principio de igualdad de condiciones lo declara el artículo 2 de este Decreto Legislativo:

"Los inversionistas extranjeros y las empresas en las que éstos participan tienen los mismos derechos y obligaciones que los inversionistas y empresas nacionales (...)".

Y seguidamente expresa enfáticamente:

"En ningún caso el ordenamiento jurídico nacional discriminará entre inversionistas ni entre empresas en función a la participación nacional o

extranjera en las inversiones"

Concluyendo en el artículo 6 del citado decreto:

"Los inversionistas extranjeros gozan de los derechos a la libertad de comercio e industria..."

Entendido para el mercado de certificación digital, estas normas invocadas buscan presentar la necesidad de permitir un mercado abierto a las inversiones nacionales y extranjeras que permitan al usuario elegir la mejor tecnología o solución de acuerdo a sus requerimientos; solución que debe darle seguridad técnica y jurídica a sus operaciones realizadas mediante medios electrónicos.

En el caso que, un usuario elija los servicios de una entidad certificadora extranjera para determinadas operaciones porque, a su entender, le permite una mejor gestión de sus actividades en el mercado virtual; éste estaría sujeto al trámite de que el certificado que respalda su firma digital tenga el necesario reconocimiento de una entidad certificadora nacional, implicándole sobre costos.

Para finalizar, es importante que un esquema razonable para garantizar la competencia entre las entidades nacionales y extranjeras, prestadoras del servicio de certificación, estaría en la participación de una Autoridad de Registro como representante de la Autoridad de Certificación Extranjera.

Artículo 11 y el rol de la Autoridad Competente.

Creemos que el llamado a reconocer validez y eficacia jurídica a los certificados de firmas digitales emitidos por entidades extranjeras, no podrían ser sus propios competidores que prestan el servicio -las entidades nacionales-, sino la Autoridad Competente, que es el órgano administrativo encargado de

la autorización y de la regulación de las entidades certificadoras; la cual, además, goza de una posición de independencia.

Efecto de la Vigencia de la Norma sobre la Legislación Nacional

Análisis Costo Beneficio

El artículo 11º de la ley 27269 tal como esta redactado colisiona con artículos constitucionales y legislación especial sobre inversión privada. Lo que daría derecho a iniciar acciones que dejen sin efecto la norma. Por otro lado se estaría evitando la creación de monopolios y una situación de discriminación generados por una redacción defectuosa del articulo 11º el mismo que se introdujo en el debate del Pleno con una intención distinta y que se pretende aclarar para un mejor desarrollo del comercio electrónico en nuestro país cuyos efectos en la economía serán del todo positivas.

Formula Legal

Texto del Proyecto

La Congresista de la República que suscribe, Graciela Fernández Baca de Valdez , miembro del grupo parlamentario Independiente, en ejercicio del derecho de iniciativa que le confiere el artículo 107 de la Constitución Política del Perú .

CONSIDERANDO:

Que, el articulo 11º de la Ley Nº 27269 Ley de Firmas y Certificados Digitales señala que "Los Certificados de Firmas Digitales emitidos por Entidades Extranjeros tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una Entidad de certificación nacional que garantice, en la misma forma que lo

hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento así como la validez y la vigencia del certificado."

Que, de la redacción actual del artículo 11º se desprende que la validez y eficacia jurídica de los certificados digitales emitidos por Entidades de Certificación Extranjeras, está condicionada al reconocimiento que ésta reciba de una Entidad de Certificación Nacional. Es decir, cualquier entidad certificadora nacional definiría en ultima instancia, el habilitar el normal funcionamiento de una entidad certificadora extranjera en el mercado peruano.

Que, si el objeto primordial de la Ley 27269 es ampliar nuestros mercados vía Internet, facilitar el comercio electrónico en general y ser agentes activos en este escenario global, el reconocimiento que exige la ley a los certificados emitidos por entidades extranjeras cierra, en la actualidad, el mercado a la libre competencia.

Que, el referido articulo 11º estaría impidiendo por un lado que los usuarios cuenten con certificados digitales de Entidades de Certificación Extranjeras que ostenten un respaldo financiero y tecnológico reconocido en el ámbito internacional y que los usuarios puedan tener plena libertad de elección en cuanto a la calidad y precio de la prestación del servicio.

Que, De una rápida evaluación en función a la demanda del mercado, se evidencia una limitación para la constitución de entidades de certificación nacionales dado el alto costo de inversión para constituir la infraestructura requerida para este tipo de empresas, situación que podría facilitar la existencia de un monopolio.

Que, Adicionalmente, en el supuesto de que exista la intención de invertir en la infraestructura requerida para una entidad de certificación

nacional, a ésta no le interesaría reconocer los certificados de una entidad de certificación extranjera pues ésta sería su competencia directa; amenazando su mercado durante el período de recuperación de la inversión.

Que, En un análisis normativo, a nivel constitucional, este artículo de la ley entra en conflicto con el artículo 63 de la Constitución Política del Perú, que a la letra prescribe: "La inversión nacional y la extranjera se sujetan a las mismas condiciones". Además especifica claramente que: "La producción de bienes y servicios y el comercio exterior son libres".

Que, en ese sentido, el artículo 11 de la Ley 27269 hace que las entidades de certificación nacionales y extranjeras no estén en las mismas condiciones jurídicas pues las segundas quedan supeditadas al reconocimiento de las primeras.

Que, de otro lado, mediante este mecanismo, se le dota a las entidades de certificación nacionales de un poder de mercado innecesario pues, mediante el reconocimiento podrían controlar el número de entidades de certificación extranjeras en el mercado peruano o inhibir la entrada de las mismas mediante entidades de registro, en el considerando que los agentes económicos podrían evitar adquirir estos certificados digitales al carecer de valor y eficacia jurídica.

Que, De lo anterior, se puede observar que el mecanismo de reconocimiento puede generar un conflicto de intereses no deseado por la ley en su conjunto, ya que finalmente ambos son agentes prestadoras del servicio en el mercado. Por lo tanto, colacionaría con una de las funciones fundamentales del Estado que es, según el artículo 61 de la Constitución, facilitar y vigilar la libre competencia.

Que, Adicionalmente , nuestra legislación no desconoce este valor de la igualdad de condiciones entre lo que es fuente de inversión extranjera y lo que constituye la inversión nacional, ambos requeridos y favorecidos para el desarrollo económico de nuestro país.

Que, el artículo 11º de la Ley 27269 colisiona involuntariamente con el Decreto Legislativo N° 662 sobre la Inversión Extranjera así como con el Dleg.757 referida a Inversión privada.

Que, consideramos que el llamado a reconocer validez y eficacia jurídica a los certificados de firmas digitales emitidos por entidades extranjeras, no podrían ser sus propios competidores que prestan el servicio – las entidades nacionales -, sino la Autoridad Competente, que es el órgano administrativo encargado de la autorización y de la regulación de las entidades certificadoras.

Que, el articulo 11º de la Ley 27269 originalmente no se encontraba incluido en el dictamen de la comisión de reforma de códigos, su inclusión se dio en el debate del Pleno no obstante la redacción final no recogió en su oportunidad la intención misma de la propuesta, que es precisamente la que se plantea en el presente proyecto de ley.

Por las razones expuestas , se propone a consideración del Congreso de la República , el proyecto de ley siguiente:

EL CONGRESO DE LA REPUBLICA

HA DADO LA LEY SIGUIENTE:

Ley que modifica el artículo 11 º de la Ley 27269

Articulo único.- Modificase el artículo 11º de la Ley 27269 el mismo que quedará redactado de la siguiente manera:

ARTÍCULO 11.- Los Certificados de Firmas Digitales emitidos por Entidades

Extranjeras tendrán la misma validez y la eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por la Autoridad Competente.

Lima, 13 de Junio del 2000

Graciela Fernández Baca

Congresista de la República

TEXTO OFICIAL DEL "EL PERUANO"

Lima, lunes 17 de julio de 2000

LEY N° 27310

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA

ha dado la Ley siguiente:

LEY QUE MODIFICA EL ARTÍCULO 11° DE LA LEY N° 27269

Artículo Único.- Objeto de la ley

Modifíquese el Artículo 11° de la Ley N° 27269, el mismo que quedará redactado de la siguiente manera:

"Artículo 11".- Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en el presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente."

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veintiséis días del mes de junio del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO

Presidenta del Congreso de la República

LUIS DELGADO APARICIO

Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los quince días del mes de julio del año dos mil.

ALBERTO FUJIMORI FUJIMORI

Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE

Presidente del Consejo de Ministros y Ministro de Justicia

ANEXO C
LEY DE DELITOS INFORMÁTICOS (Ley N°. 27309)

LEY No. 27309

Promulgada el 27.Julio.2000

Publicada el 27.Julio.2000

Ley No. 27309

EL PRESIDENTE DE LA REPÚBLICA;

POR CUANTO:

El Congreso de la República ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Fundamentos

Efecto de la Vigencia de la Norma sobre la Legislación Nacional

Análisis Costo Beneficio

Texto del Proyecto

CONSIDERANDO:

Que, el desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Que, en los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Que, los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, el presente proyecto se dirige a la regulación penal de las posibles medidas preventivas de carácter penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos, alcance en el país los niveles de peligrosidad que se han dado en otros países.

Propone el siguiente Proyecto de Ley:

LEY DE DELITOS INFORMÁTICOS

Artículo único.- Incorpórese al Código Penal, promulgado por Decreto Legislativo N° 635, el Capítulo SI, Delitos Informáticos, los artículos 208a y 208b; con los siguientes textos:

Artículo 208 a.- El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de la libertad no mayor de dos años, o con prestación de servicios comunitario de cincuenta y dos a ciento cuatro jornadas.

Artículo 209 b.- El que indebidamente, interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, sistema o red será reprimido con pena privativa de la libertad no mayor de dos años.

Lima, 18 de agosto de 1999

JORGE MUÑIZ ZICHES

Congresista de la República

TEXTO OFICIAL DE "EL PERUANO"

Lima, lunes 17 de julio de 2000

LEY N° 27309

EL PRESIDENTE DE LA REPÚBLICA
POR CUANTO:

EL CONGRESO DE LA REPÚBLICA;

ha dado la Ley siguiente:

LEY QUE INCORPORA LOS DELITOS INFORMÁTICOS AL CÓDIGO PENAL

Artículo Único.- Objeto de la ley

Modificase el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo N° 635, con el texto siguiente:

"TÍTULO V"

CAPÍTULO X

DELITOS INFORMÁTICOS

Artículo 207°-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar,

acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de la libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207°-B .- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multas.

Artículo 207°-C.- En los casos de los Artículos 207°-A y 207°-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

CAPÍTULO XI

DISPOSICIÓN COMÚN

Artículo 208°.- No son reprimibles, sin perjuicio de la reparación civil, los hurtos, apropiaciones, defraudaciones o daños que se causen:

Los cónyuges, concubinos, ascendientes, descendientes y afines en línea recta.

El consorte viudo, respecto de los bienes de su difunto cónyuge, mientras no hayan pasado a poder de tercero.

Los hermanos y cuñados, si viviesen juntos. “

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veintiséis días del mes de junio del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO

Presidenta del Congreso de la República

LUIS DELGADO APARICIO

Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los quince días del mes de julio del año dos mil.

ALBERTO FUJIMORI FUJIMORI

Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE

Presidente del Consejo de Ministros y Ministro de Justicia

BIBLIOGRAFÍA

Libros:

Título	Web Commerce Technology Handbook – McGraw-Hill Series
Autor	Daniel Minoli – Emma Minoli.
Título	Internet Firewalls – O'Reilly – McGraw-Hill Series
Autor	Brend Chapman – Elizabeth Zwicky
Título	Protecting Networks with SATAN – O'Reilly
Autor	Martin Freiss

Web Sites:

Visa Internacional	:	www.visa.com
MasterCard	:	www.mastercard.com
SETCO	:	www.setco.org
RSA Data Security Inc.	:	www.rsa.com
Terisa Systems	:	www.terisa.com
Hp-Verifone	:	www.verifone.com
Verisign, Inc	:	www.verisign.com
GTE Cybertrust	:	www.cybertrust.gte.com
SAIC	:	www.saic.com
IBM	:	www.internet.ibm/commercepoint
Microsoft Corp.	:	www.microsoft.com
Netscape Comunications Inc.	:	www.netscape.com
First Virtual Holdings Inc.	:	www.fv.com
CyberCash, Inc.	:	www.cybercash.com
DigiCash	:	www.digicash.com
NetBill	:	www.ini.cmu.edu/netbill
NetCheque/NetCash	:	nii.isi.edu/info/Netcheque
CheckFree Corporation	:	www.checkfree.com
The NetMarket Company	:	www.netmarket.com/sa/pages/home
Open Market	:	www.openmarket.com
Mondex International	:	www.mondex.com
Financial Services Technology Consortium (FSTC)	:	www.fstc.org
ComerceNet	:	www.commerce.com
Kriptopolis	:	www.kriptopolis.com
Cyberpunks	:	www.cyberpunks.to
SSLeay	:	www.ssleay.org
E-commerce E-mail List	:	www.comercio-electronico.org
Librería Amazon	:	www.amazon.com

Kagi	www.kagi.com
Microsoft Wallet	www.microsoft.com/wallet/default.asp
E-Wallets en Java	java.sun.com/products/commerce
E-commerce Europa	www.ispo.cec.be/ecommerce/