CAPITULO III

APLICACIÓN:

CONSTRUYENDO UNA INFRAESTRUCTURA CONFIABLE DE E-COMMERCE

Los negocios que pueden administrar y procesar transacciones comerciales a través de Internet pueden ganar en competitividad, debido a la posibilidad de alcanzar audiencia para sus ofertas a nivel mundial a bajo costo, ahora bien, hay que tener en cuenta que los clientes compran bienes y/o servicios a través de la Web sólo cuando confían en que su información personal, número de tarjeta de crédito por ejemplo, está segura; para ello el negocio debe tomar las medidas necesarias con el fin de minimizar los riesgos inherentes a la Web.

Para poder aprovechar las ventajas que proporcionan las oportunidades del e-commerce y evitar dichos riesgos, los negocios deben tener conocimiento y comprender los problemas y dudas que afectan la privacidad, seguridad y confianza en el sistema, algunas de estas preocupaciones son:

- *¿Cómo puedo estar seguro de que los datos sobre las tarjetas de crédito o débito de mis clientes, no serán accedidos por personas no autorizadas, cuando realicen una transacción supuestamente segura en la Web?*
- *¿Cómo puedo garantizar a los clientes que visitan mi site que están realizando negocios conmigo y no con un impostor?*
- *Si me he asegurado de cubrir las dudas anteriores ¿cuál es la mejor manera de hacérselo saber a los clientes para que se sientan seguros de hacer negocios conmigo?*
- *Cuando los clientes se sientan lo suficientemente en confianza para negociar en línea conmigo ¿cómo puedo darles facilidades para que me paguen usando tarjetas de crédito o débito u otros métodos?*
- *¿cómo puedo verificar la validez de la tarjeta que está usando mi cliente?*

- *¿qué hago con la información de pago que el cliente me ha enviado?*

Estas preocupaciones apuntan a los objetivos fundamentales de establecer una infraestructura confiable de e-commerce:

- Autentificación
- Confidencialidad
- Integridad
- No repudio

La solución para los objetivos propuestos incluyen 2 componentes esenciales:

- Certificados para servidores
- Sistema de Pago seguro en línea

Además se debe tener en cuenta que la seguridad debe estar en todas las etapas desde el inicio del proyecto.

III.1 SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Internet es una red insegura para todo tipo de operaciones. La única forma de poder hacer transacciones seguras es imponiéndole mecanismos de seguridad a cada una de ellas.

Una de las leyes fundamentales de la seguridad informática dice que «el grado de seguridad de un sistema es inversamente proporcional a la operatividad del mismo». Esto se debe a que darle a un sistema un determinado grado de seguridad, aunque sea mínimo, implica imponer algún tipo de restricción, lo que forzosamente disminuirá la operatividad con respecto al estado anterior en el que no se tenía seguridad.

Internet es una red insegura, porque fue diseñada con un alto nivel de operatividad. No está mal que sea insegura, ni se trata de un error de diseño, sino que para que cumpliera la función para la cual se la creó debía tener el más alto grado de operatividad, lo que trae como consecuencia un alto nivel de inseguridad.

No es cierto que, por implantar determinados mecanismos de seguridad automáticos, Internet se vuelve segura.

El parámetro fundamental a tener en cuenta, ya sea uno un usuario final o una corporación, es el siguiente: «Cuando se conectan dos sistemas, uno seguro y otro inseguro, el grado de seguridad no se promedia, sino que pasa a ser el del más inseguro para todo el sistema».

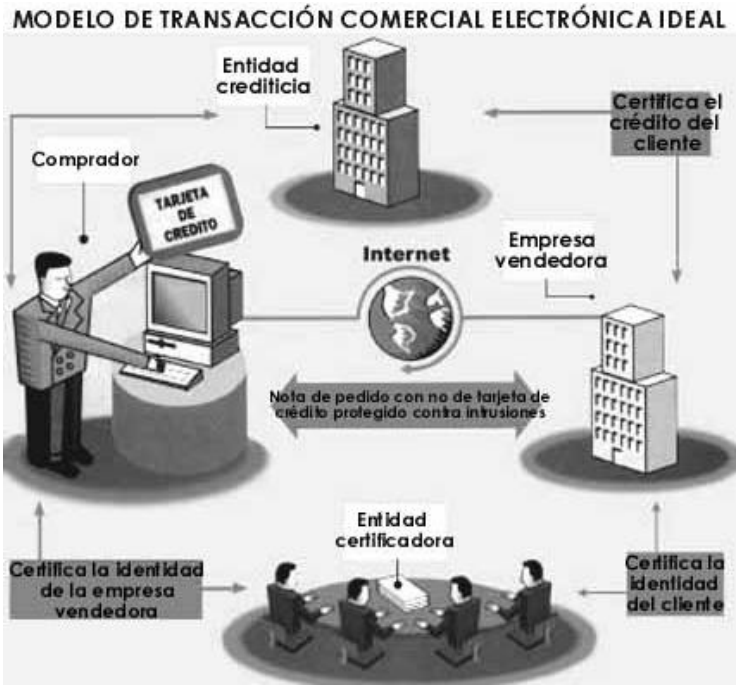
Por lo tanto, a partir de la conexión de un sistema seguro (el suyo propio) con otro inseguro (Internet) se deberá aumentar el grado de seguridad. Dicho de otra manera:

«Cada vez que se agregue algo a un sistema que lo vuelva más abierto (por ejemplo una conexión a Internet) se deberá actualizar la estrategia de seguridad informática del mismo».

Las notas de compra que completa el usuario en su computadora son enviadas por Internet a la empresa vendedora en forma de mensaje. Como estas notas contienen información sensible (número de la tarjeta de crédito del comprador), y como cualquier tipo de mensaje que circula por Internet puede ser interceptado por un intruso con el fin -entre otros- de obtener números de tarjetas de crédito en vigencia, es necesario utilizar algún mecanismo de seguridad que minimice este riesgo.

La posibilidad de que un intruso intercepte un mensaje que circula por Internet no se puede evitar, pues es parte de la inseguridad propia de Internet. Poniéndonos en el caso más desfavorable, que implicaría que todo mensaje que enviemos por Internet será interceptado, lo que tenemos que lograr es que, una vez que sea interceptado, la información que contiene no sea útil para el intruso.

Una forma de lograr esto es por medio de la encriptación de la información del mensaje.



EL APORTE DE LA ENCRIPTACIÓN

La encriptación aplicada a un caso como éste funciona codificando por medio de una clave la información que contiene el mensaje.

De esta manera, el contenido sólo puede ser conocido por quienes tengan la clave para decodificarlo (el comprador y la empresa vendedora).

Aunque un intruso intercepte el mensaje, lo que verá en él le resultará incomprensible, pues no tiene la clave de decodificación para hacerlo legible.

En la práctica, estos mecanismos se implementan con sistemas de doble encriptado o de clave pública, que además de tener un buen nivel de seguridad contra ataques de decodificación, permiten determinar que el mensaje ha sido generado por una determinada persona.

LA IDENTIDAD DEL COMPRADOR Y LA EMPRESA VENDEDORA

En una transacción comercial física, la identidad del emisor puede ser probada por medio de un documento, y la de la empresa vendedora por medio de sus comprobantes de venta.

Pero una de las características más particulares de la comunicación electrónica (como es la comunicación a través de Internet), es la capacidad de anonimato y de presentarse bajo una identidad falsa.

El sistema de doble encriptado garantiza que la orden de compra fue emitida por el propietario de una determinada dirección de correo electrónico, pero la pregunta que surge es:

¿será el propietario de esa dirección de correo electrónico quien dice ser, y por lo tanto el titular de la tarjeta de crédito?

Con respecto a la empresa vendedora también cabe preguntarse: ¿la página web que estoy viendo en la pantalla de la computadora es auténtica o sólo es una trampa para recolectar números de tarjeta de crédito de incautos?

El mecanismo propuesto para estos casos es el uso de Certificados Digitales emitidos por una Autoridad de Certificación.

La Autoridad Certificadora se encarga de certificar que una determinada dirección de correo electrónico pertenece a una persona específica, y que una determinada dirección de página web pertenece a una empresa específica. De esta manera, por medio de la AC quedarían aseguradas las identidades del comprador y de la empresa vendedora.

El grado de seguridad y el de operatividad de un sistema son inversamente proporcionales, tal como se ha visto líneas arriba; es por esto que el arte del consultor en seguridad informática, consiste en llevar un sistema a una relación de equilibrio entre estos dos factores.

En una transacción electrónica ideal el comprador y la empresa vendedora se comunican a través Internet.

La empresa llega al comprador a través de su página Web, que debería estar certificada en cuanto a su identidad por una AC.

Los pedidos del usuario llegan a la empresa vendedora por medio de un mensaje protegido por encriptación, para que, en caso de ser interceptado, no se conozca el número de tarjeta de crédito. La identidad del usuario también debería estar certificada. La entidad crediticia que emite la tarjeta de crédito seguirá existiendo para avalar el crédito del usuario hasta que se implementen otros mecanismos de pago como el dinero electrónico.

PROTOCOLOS

Determinados protocolos aseguran la confidencialidad e integridad de la información transmitida a través de la Red y garantizan la viabilidad de cualquier orden de pago.

Una de las principales preocupaciones que tiene el consumidor en el uso del comercio electrónico es la seguridad. ¿Qué pasa si doy mi número de tarjeta para comprar en una tienda? ¿Es seguro? ¿Me robarán los datos? ¿Y el dinero? ¿Es Internet un medio de pago seguro?

Para ello se han creado dos protocolos estándar de seguridad: **el protocolo SET y el protocolo SSL**.

Una vez que ingresas a Internet para comprar, los comercios virtuales te avisan de que vas a entrar en un servidor seguro y podrás comprobarlo cuando en la parte superior de tu navegador la dirección empieza por https. Esa "s" indica servidor seguro. A partir de ese momento, has entrado en una página protegida por SSL o por SET. Los protocolos SSL y SET son medios de encriptación de datos. Es decir, una vez entregados tus datos, nadie podrá interceptarlos, copiarlos o modificarlos.

SSL (Secure Sockets Layer): es un protocolo de propósito general para establecer comunicaciones seguras, propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator. Hoy constituye la solución de seguridad implantada en la mayoría de los servidores web que ofrecen servicios

de comercio electrónico. Para pagar, el usuario debe rellenar un formulario con sus datos personales (tanto para el caso del envío de los bienes comprados, como para comprobar la veracidad de la información de pago), y los datos correspondientes a su tarjeta de crédito (número, fecha de caducidad, titular). Esta arquitectura no exige que el servidor disponga de capacidades especiales para el comercio. Basta con que se utilice como mínimo un canal seguro para transmitir la información de pago y el comerciante ya se ocupará manualmente de gestionar con su banco las compras. El canal seguro lo proporciona SSL. Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura (debido a que los navegadores utilizan 40 bits de longitud de clave, protección muy fácil de romper). SSL deja de lado demasiados aspectos para considerarse la solución definitiva y esto porque:

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

El estándar SET (Secure Electronic Transaction): fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de gigantes de la industria del software, como Microsoft, IBM y Netscape, con la finalidad de superar los inconvenientes y limitaciones anteriores.

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

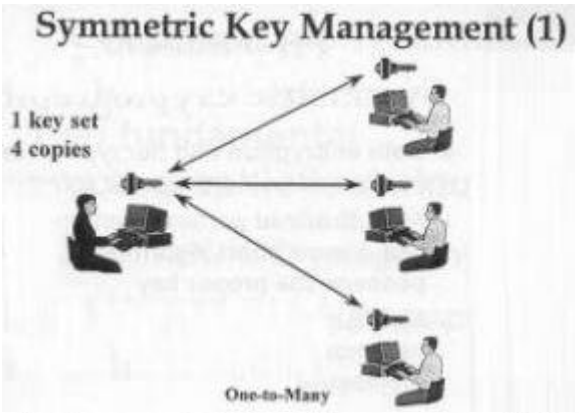
ya que SET gestiona tareas asociadas a la actividad comercial de gran importancia, como registro del titular y del comerciante, autorizaciones y liquidaciones de pagos, anulaciones, etc.

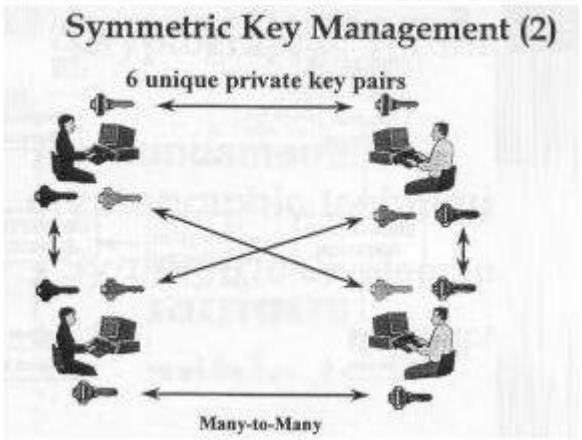
Entonces, si todo son alabanzas, ventajas y puntos fuertes, ¿por qué SET no termina de implantarse? ¿Por qué no goza de la popularidad de SSL, si se supone mejor adaptado? En primer lugar, su despliegue está siendo muy lento. Exige software especial, tanto para el comprador (aplicación de monedero electrónico) como para el comerciante (aplicación POST o terminal de punto de venta), que se está desarrollando con lentitud. En segundo lugar, aunque varios productos cumplan con el estándar SET, esto no significa necesariamente que sean compatibles. Este es un problema que exige mayores esfuerzos de coordinación y más pruebas a escala mundial para asegurar la interoperabilidad. Sus puntos fuertes son también su talón de Aquiles: la autenticación de todas las partes exige rígidas jerarquías de certificación, ya que tanto los clientes como comerciantes deben adquirir certificados distintos para cada tipo de tarjeta de crédito, trámites que resultan engorrosos, cuando no esotéricos, para la mayoría de los usuarios.

En definitiva, SET es un elefante de gran tamaño y fuerza, pero de movimientos extraordinariamente pesados. SSL es una liebre que le ha tomado la delantera hace años. No es tan perfecto, no ofrece su seguridad ni sus garantías, pero funciona.

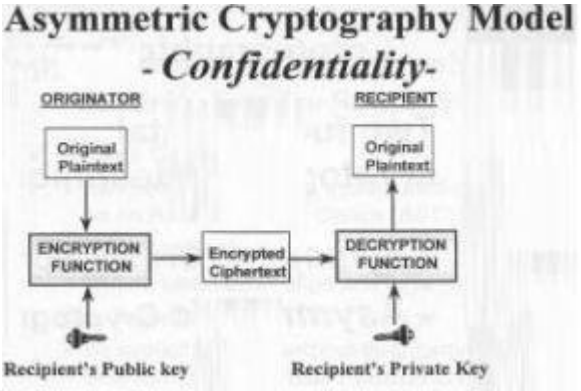
TÉCNICAS CRIPTOGRÁFICAS

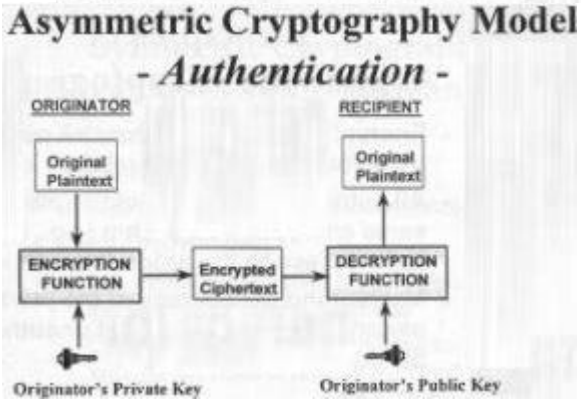
Como hemos visto en un capítulo anterior, existen dos técnicas criptográficas básicas. **La Criptografía *Simétrica* y la Criptografía *Asimétrica*.**





La *Criptografía Simétrica* está basada en la encriptación y decriptación de datos utilizando la misma llave. Todas las partes autorizadas deberán utilizar el mismo algoritmo de encriptación y poseer la misma llave. El control de accesos puede ser garantizado por una tercera parte, que puede ser un Centro de Control de Accesos (ACC por sus siglas en inglés). La ventaja es la de tener un rápido proceso de encriptado/desencriptado, y es una tecnología fácil de comprender y utilizar. La gran desventaja que existe al utilizar este método de encriptación, es la de que mucha gente olvida su password, haciendo así ilegible todo mensaje cifrado que le llegue. Para evitar la pérdida de esta información, existe una entidad llamada Autoridad de Certificación (CA por sus siglas en inglés), que tendrá la responsabilidad de contar con un mecanismo de recuperación. Este debe contar con altísimas medidas de seguridad, de tal modo que pueda garantizar que las llaves privadas no serán utilizadas por otras personas. Además, debe existir mucha confianza entre esta autoridad y los usuarios, de tal manera que confiemos plenamente que el usuario que utiliza una llave autorizada por la CA, es quien dice ser.





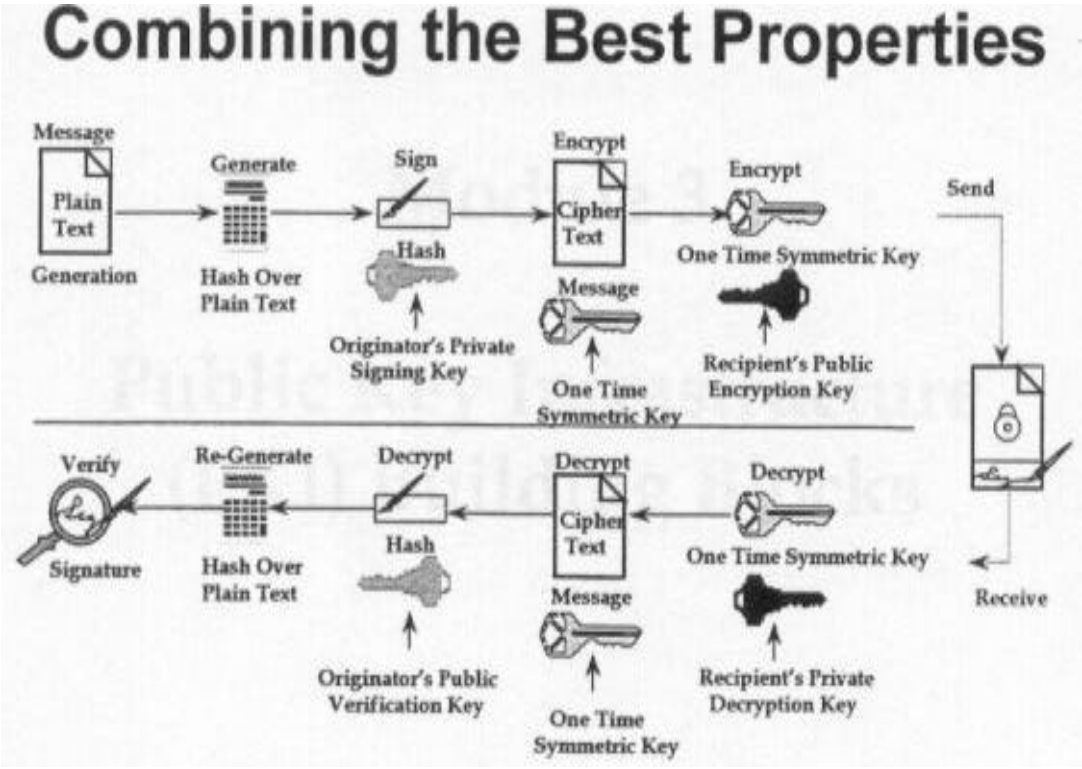
La *Criptografía Asimétrica* está basada en la encriptación y desencriptación utilizando dos llaves diferentes (pero relacionadas entre sí). Todas las partes autorizadas deberán utilizar el mismo algoritmo de encriptación, por ejemplo el Rivest, Shamir, Adleman (RSA); y tener acceso a las llaves. Las llaves privadas deben ser distribuidas de manera segura a individuos específicos. Las llaves privadas de autenticación deben ser generadas localmente y nunca ser reveladas a alguien. Las llaves públicas deben ser fácilmente obtenibles. Su integridad debe ser mantenida todo el tiempo. La autenticidad de la llave pública debe ser verificable, y pueden ser revocadas. Sus ventajas son la de ser una tecnología conocida y muy bien comprendida, soporta todos los requisitos de servicios de seguridad. La desventaja es la de tener un proceso sobrecargado de encriptación/decriptación.

COMBINANDO LAS MEJORES PROPIEDADES

Dado que la velocidad de encriptación/desencriptación de la encriptación simétrica es mucho más veloz que la de encriptación asimétrica, es preferible utilizar ambos. Teniendo los datos listos para enviar, estos son encriptados, y luego firmados con la llave privada del autor. Son nuevamente encriptados y nuevamente firmados con una llave simétrica de un solo uso, y nuevamente encriptado utilizando la llave pública del destinatario. El proceso de desencriptado

es hecho a la inversa, y de esta manera tenemos una manera segura y confiable de asegurar que los datos recibidos son de quien dice ser.

Debemos mencionar que los procesos de firma y cifrado se hacen de manera independiente. Podemos hacerlo de manera conjunta o separada. Además, todos los procesos son hechos de manera automática por nuestro sistema, no teniendo nosotros que preocuparnos de verificar los certificados uno por uno, sino que el sistema lo hará automáticamente.



AMENAZAS A LA SEGURIDAD Y SOLUCIONES

Amenaza	Seguridad y solución	Función	Tecnología
Datos interceptados, leídos o modificados ilícitamente.	Encriptamiento	Los datos se codifican para evitar su alteración.	Encriptamiento simétrico y asimétrico.
Los usuarios asumen otra identidad para cometer un fraude.	Autentificación.	Verifica la identidad del receptor y emisor.	Firmas digitales.
Un usuario no autorizado en una red obtiene acceso a otra red	Firewall	Filtra y evita que cierto tráfico ingrese a la red o servidor.	Firewall; redes virtuales privadas.

ESTANDARES DE SEGURIDAD PARA INTERNET

Estándar	Función	Aplicación
Secure HTTP (S-HTTP)	Asegura las transacciones en el web.	Exploradores, servidores web, aplicaciones para Internet.
Secure Sockets Layer (SSL)	Asegura los paquetes de datos en la capa de la red.	Exploradores, servidores web, aplicaciones p/ Internet
Secure MIME (S/MIME).	Asegura los anexos de correo electrónico en plataformas múltiples.	Paquetes de correo electró-nico con encriptamiento RSA y firma digital.
Secure Wide-Area Nets (S/WAN)	Encriptamiento punto a punto entre cortafuegos y enrutadores.	Redes virtuales privadas.
Secure Electronic Transaction (SET)	Asegura las transacciones con tarjeta de crédito.	Tarjetas inteligentes, servidores de transacción, comercio electrónico.

III.2 CERTIFICADOS DIGITALES

Es la **Certificación Electrónica** que vincula unos datos de verificación de firma a un signatario y **confirman su identidad.**

El Certificado Digital es un conjunto de datos a prueba de falsificación protegidos por una contraseña y con validez de un año o más. Se almacena en la base de datos del navegador de Internet o en otro tipo de dispositivo de almacenamiento, permitiendo la transferencia segura de información a través de redes abiertas como Internet.

Características del Producto:

- El cifrado y la firma digital que un certificado nos permite, se debe a que está basado en Criptografía Asimétrica la cual trabaja con un par de claves que se generan al momento de descargar un certificado.
- La clave pública: aquella que se difunde al resto de los usuarios para poder verificar la firma de un texto o cifrar mensajes.
- La clave privada: utilizada por el usuario para poder descifrar mensajes recibidos o para firmar digitalmente.

¿QUIÉN EMITE LOS CERTIFICADOS?

- **ACE** (Agencia de Certificación Electrónica), es la Autoridad de Certificación (CA) que emitirá los certificados una vez que los datos proporcionados hayan sido verificados por la Autoridad de registro designada (Por ej. Telefónica Data).

- **VeriSign** es aquella que suministra servicios de seguridad electrónica en Internet, tiene una red global de afiliados.

- **Telefónica Data Perú,** es una Entidad de Certificación, diferente de los suscriptores de certificados que se encarga de gestionar y validar las solicitudes de certificados en base a determinados procedimientos de identificación.

- **Cosapi Soft,** otorga certificados SSL y de usuario

- **Qnet/GMD,** ofrece certificados SSL pero sólo si la solución lo requiere.

- **IDCert,** otorga certificados SSL y de usuario y presta servicio de timestamp.

- **ATM Technology,** representante de IDENTIDATA otorga sólo un tipo de certificado. 1certificado, 1 lectora, tarjeta inteligente y sw de instalación.

Dependiendo del navegador que utilice el comprador puede comprobar que se encuentra en un ambiente seguro. Si está usando Explorer, le aparecerá un candado en la parte inferior de la barra de información. Si está usando Netscape, el candado en la parte de herramientas se activará.

PAG 97