CAPÍTULO 4

SISTEMAS DE PAGO SEGURO

4.1 CARACTERÍSTICAS

Desde sus inicios, el Internet se utilizó básicamente como una herramienta de búsqueda de información, sin embargo, el incremento en el número de usuarios ocasionó que empresas comerciales lo utilicen como un medio de mercado para vender productos y servicios. En general, el comercio electrónico a través del Internet se puede implementar utilizando los sistemas de pago tradicionales, como son el pago por teléfono (out-of-band), transferencia de números de tarjeta de crédito, entre otros, sin embargo el nivel de seguridad no es el adecuado.

La razón principal por la cual el comercio electrónico no ha sido explotado en todo su potencial es porque, hasta recientemente, no existia una forma de operación segura que previniera los fraudes y robos de información financiera

confidencial. Esto involucra tres aspectos, (a) que los consumidores y vendedores deben ser capaces de identificarse mutuamente, a fin de confiar uno en el otro, (b) evitar que la información que se transmite sea monitoreada, y (c) que las operaciones comerciales se puedan realizar fácilmente con cualquier cliente o empresa. Para lograr esto, se deben cumplir los siguientes requisitos [1,26,27]:

- Confidencialidad de la información.
- Integridad de la información transmitida a través de una red pública.
- Verificación de que un usuario esté utilizando una cuenta legítima.
- Verificación de que un vendedor puede tener acceso a la cuenta del usuario.
- Interoperatibilidad entre distintos programas y redes de datos.

La *confidencialidad de la información* se refiere al hecho de que la información debe de poder ser transmitida de manera segura a través del Internet, libre de cualquier tipo de monitoreo en cualquier instante de la transmisión (servidor, ruteador, canal de comunicación ,etc). Para logralo, la información debe ser encriptada utilizando distintos algoritmos, como los descritos en el Capítulo 3. El objetivo de la Criptografía es la protección de información confidencial mediante algoritmos numéricos parametrizados en claves (cadenas de bits). El resultado de la encriptación es un encriptexto que es transmitido en forma segura y descrifrado utilizando una clave para obtener el mensaje original. Los

hurtados para ser utilizados en transacciones no autorizadas por el propietario. En este caso, se establece una conexión entre un número de cuenta y la firma digital de un usuario; esta conexión se realiza a través de un tercer usuario que se encarga de validar la clave del usuario y su número de cuenta. Este tercer usuario debe estar certificado para realizar esta función (reciben el nombre de autoridades certificadoras), y actualmente existen diversas organizaciones que realizan esta tarea, en dependencia del tipo de información que se transmita. La forma de validación consiste en permitir que el vendedor descifre la clave pública del usuario utilizando la clave pública de la autoridad certificadora, a fin de validar la autenticidad del comprador.

En el caso de la *verificación de que un vendedor puede tener acceso a la cuenta del usuario*, se trata del mismo problema, pero en este caso el objetivo es evitar que un usuario sin autorización simule vender productos o servicios para obtener los números de cuenta de los usuarios. En este caso, la autoridad certificadora utiliza el mismo mecanismo que se utilizó para validar que un usuario realmente esta utilizando una cuenta legítima.

Finalmente, la *interoperatibilidad entre distintos programas y redes de datos* se refiere a la posibilidad de realizar cualquier tipo de transacción entre dos usuarios (vendedor y comprador) conectados al Internet. Por esta razón, los estándares de seguridad y procedimientos deben ser soportados por cualquier plataforma de hardware y software que un usuario pueda estar utilizando, a fin

de que exista una interoperatibilidad completa. Esto se logra utilizando algoritmos y procedimientos de carácter público.

4.2 DESCRIPCIÓN GENERAL DE UN SISTEMA DE PAGO SEGURO

En muchos aspectos, los sistemas de comercio electrónico están sustentados en sistemas de pago electrónico. En general, un pago electrónico es un intercambio financiero que se realiza en línea entre compradores y vendedores. El contenido del pago electrónico es un tipo de instrumento financiero digital (tarjeta de crédito, cheques electrónicos o dinero digital) que es respaldado por un banco o institución financiera.

La incorporación de capacidades de pago electrónico conlleva una considerable complejidad para los sistemas de TI. Primero, los sistemas de pago seguro deben ser capaces de proteger las aplicaciones del sistema de TI. Segundo, el sistema debe proporcionar un alto grado de integridad para cualquier tipo de transacción; esto incluye que las comunicaciones entre el consumidor, el proveedor y la institución financiera estén libres de intercepciones y alteraciones. Tercero, el sistema debe admitir diversas opciones de pago de acuerdo a las preferencias de los consumidores (tarjeta de crédito, tarjeta de débito, transferencias, etc.).

En el caso de los sistemas de pago por Internet, existen diversos mecanismos tanto convencionales como especializados. Actualmente, los métodos de pago

convencionales como efectivo y cheques no son adecuados para sistemas de pago interactivo en tiempo real. Actualmente, la mayoría de los sistemas de pago por Internet utilizan dinero latente, como tarjetas de crédito, órdenes de compra con promesa de pago y transferencias de efectivo. También existen sistemas emergentes, algunos de los cuales basan sus operaciones en transacciones en dinero electrónico y micro pagos, que no tienen gran aceptación [16].

4.3 PROCESO DE PAGO Y COMPRA

Para que el proceso de pago y compra se pueda realizar como una transacción electrónico a través del Internet con las características descritas en la sección 4.1, se deben cumplir las siguientes etapas [1,11]:

1. Registro de la cuenta del usuario.
2. Registro del vendedor o compañía que ofrece el producto/servicio.
3. Envío de la orden de compra de parte del usuario.
4. Autorización del pago.

El *registro de la cuenta del usuario* consiste en que el usuario se registre con sus datos y número de cuenta (o tarjeta de crédito) ante una autoridad certificadora (AC) antes de realizar cualquier transacción con un vendedor. Para ello, el usuario debe contar con la clave pública de la AC, la cual puede ser

enviada a través de correo electrónico. Los pasos que sigue el software del usuario para realizar el registro son los siguientes (Fig. 4.1):

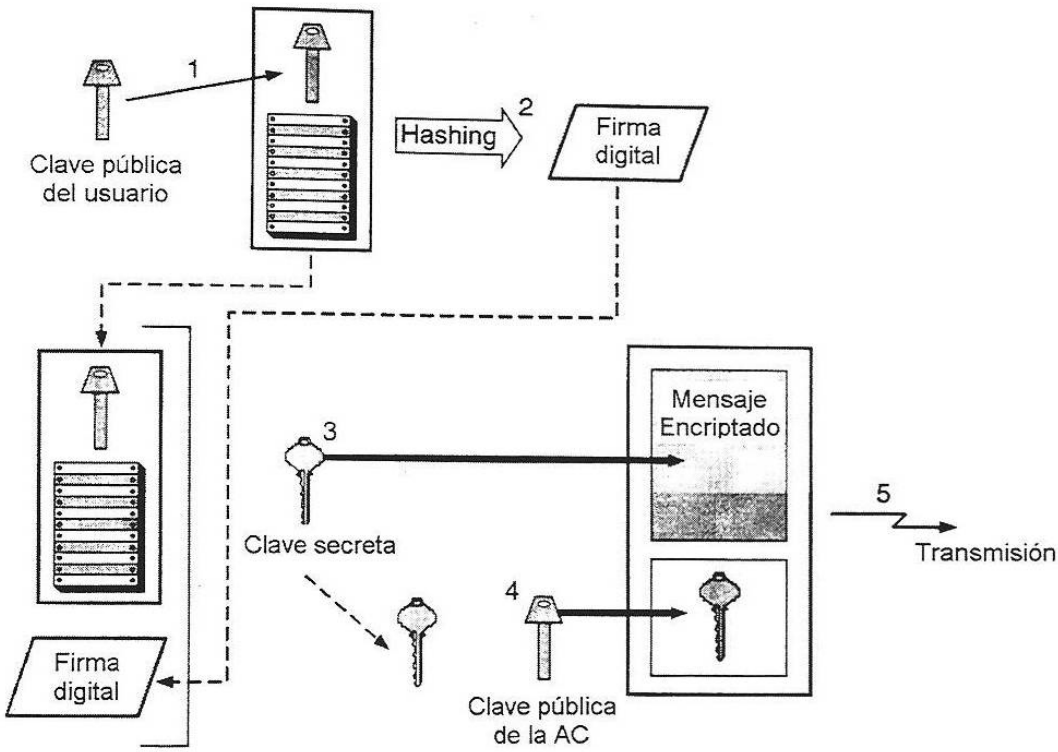

Fig. 4.1. Proceso de registro de la cuenta del usuario [1].

- Se completa una forma de solicitud, y se adjunta la clave pública del usuario.
- Se genera una firma digital a partir de la información anterior.
- El mensaje y la firma digital son encriptadas utilizando la clave secreta del usuario.
- Se encripta la clave secreta del usuario utilizando la clave pública de la AC.
- Se transmite la información a la AC.

Una vez que la AC recibe la información de la solicitud del usuario, se siguen los siguientes pasos (Fig. 4.2):

- Se descifra la clave secreta.
- Se descifra la información, la firma digital y la clave pública del usuario.
- Se calculan y comparan las firmas digitales.

Si la información del registro es verificada, la AC certifica la clave pública del usuario y la información de su cuenta a través de una firma digital utilizando la clave secreta de la AC. Entonces, un documento de certificación (DC) es transmitido al usuario (el cual es validado por el software del usuario en forma similar) para su uso en transacciones electrónicas.

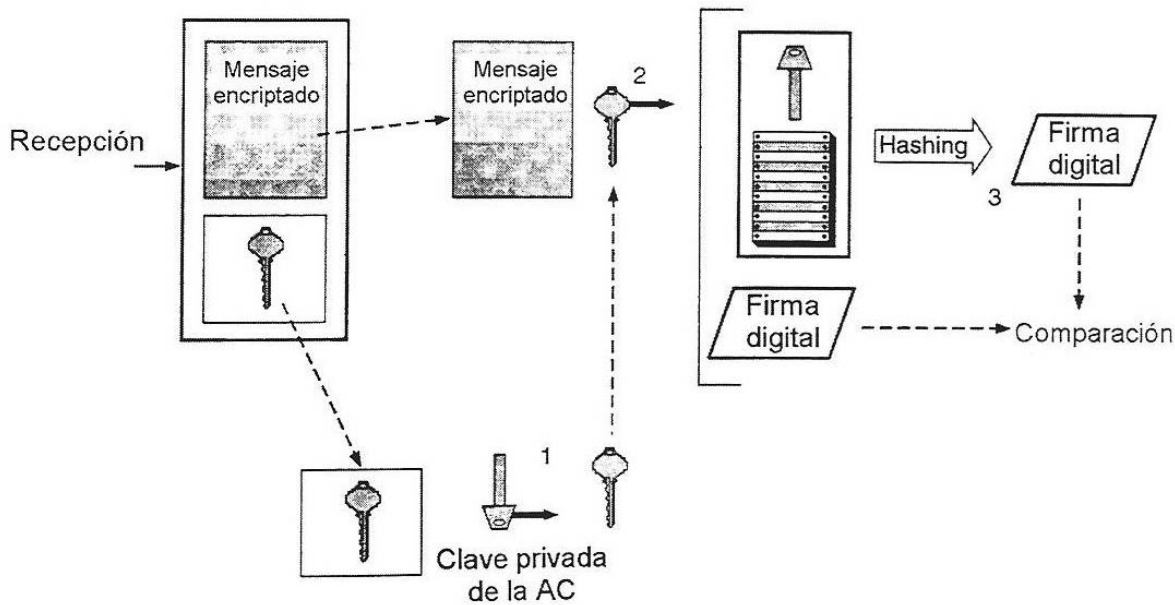

Fig. 4.2. Conformación de la AC del registro de la cuenta del usuario [1].

El *registro del vendedor o compañía que ofrece el producto/servicio* es similar al registro de un usuario ante una AC descrito en los párrafos anteriores. Sin embargo, a diferencia del usuario, el vendedor debe registrarse ante una o más AC en dependencia del tipo de sistema de pago que desea manejar.

El *envío de la orden de compra de parte del usuario* requiere que éste cuente con una copia de la clave pública del vendedor y una copia de la clave pública de la AC de acuerdo a la forma de pago que el usuario le haya informado previamente al vendedor. Para tener acceso a una compra en línea, el usuario solicita el DC del vendedor, el cual verifica con la clave pública de la AC y verificando la firma digital de la AC. En este punto el usuario esta en la posibilidad de realizar una compra ; una vez que la orden esta lista, el software del usuario realiza los siguientes pasos (Fig. 4.3):

- Se encripta la información de la cuenta con la clave pública de la AC.
- Se anexa esta información a la orden de compra.
- Se crea una firma digital de la orden de compra, y se firma digitalmente utilizando la clave privada del usuario.
- La orden de compra (con la información de la cuenta encriptada), la firma digital y el DC del usuario son encriptados con la clave secreta.
- Se encripta la clave secreta con la clave pública del vendedor obtenida de su DC.

- El mensaje encriptado con la clave secreta y la clave secreta encriptada son transmitidos al vendedor.

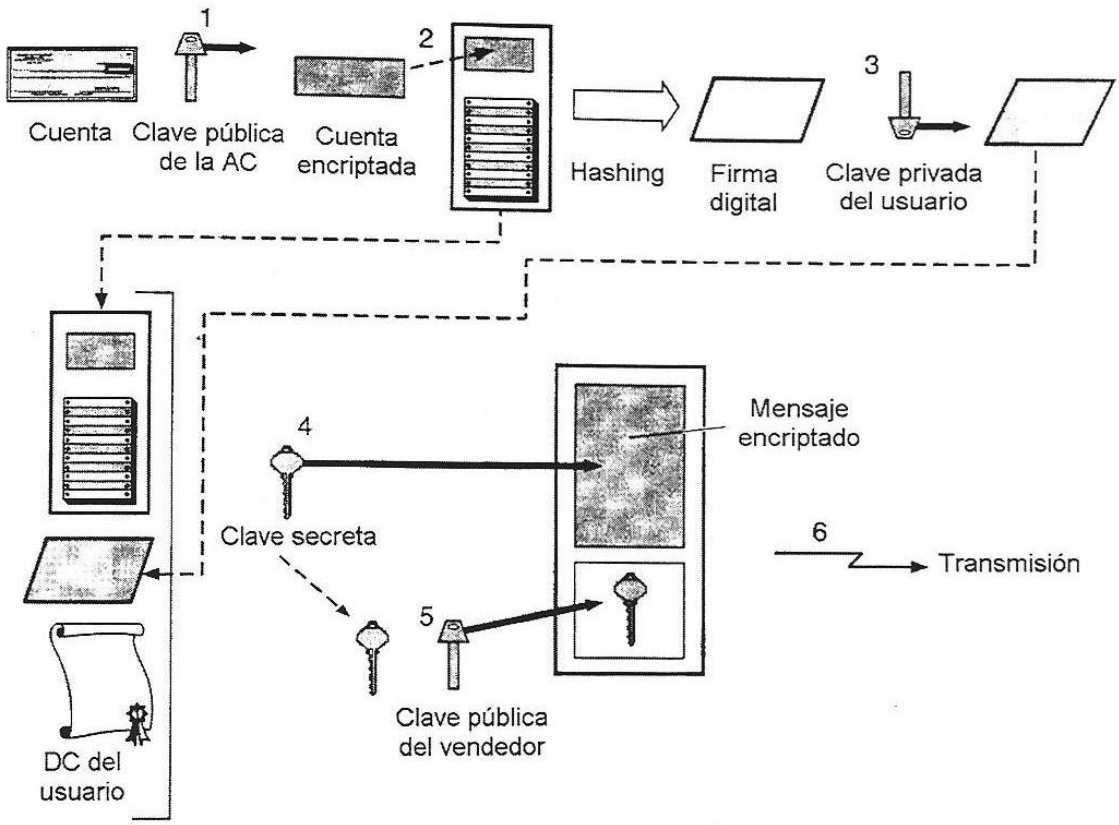

Fig. 4.3. Proceso de orden de compra: usuario [1].

Una vez que el vendedor recibe esta información, su sistema realiza el siguiente proceso (Fig. 4.4):

- Se descifra la clave secreta utilizando la clave privada del vendedor.
- Se descifra la orden de compra, la firma digital y el DC del usuario utilizando la clave secreta.

- Se descifra la firma digital utilizando la clave pública del usuario obtenida de su DC (esto verifica la firma digital del usuario).
- Se determina la firma digital de la orden y se compara con la enviada por el usuario.

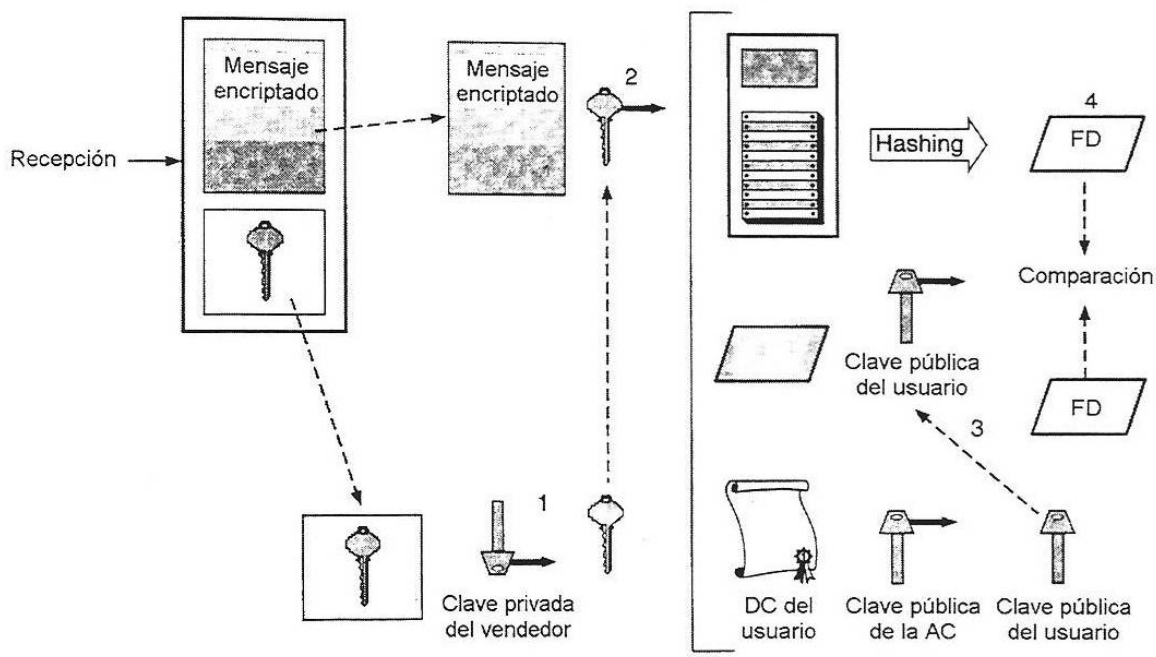

Fig. 4.4. Proceso de orden de compra: vendedor [1].

Si las firmas coinciden (la recibida y la calculada a partir de la orden de compra), el vendedor inicia el procesamiento de la orden de acuerdo a sus políticas internas. Una vez que la orden es procesada, el vendedor debe emitir una confirmación al usuario, notificándole que su orden ha sido procesada.

La *autorización del pago* consiste en que el vendedor debe obtener la autorización para realizar la transacción con la AC responsable de la cuenta del

usuario. Esta autorización asegura que la cuenta del usuario disponga de los fondos suficientes, o que el límite de crédito esta disponible, para cubrir el pago de la orden. Es importante resaltar que el vendedor en ningún momento tiene acceso a la información de la cuenta del usuario, ya que ésta fue encriptada con la clave pública de la AC

Por lo tanto, el sistema del vendedor debe transmitir la siguiente información a la AC: el DC del vendedor, datos de la orden de compra, el DC del usuario, y la información de la cuenta del usuario. Con esta información, la AC autoriza las acciones de transferencia de fondos de acuerdo a los mecanismos financieros establecidos. En todo momento, la información es encriptada y firmada digitalmente de acuerdo a como se describió anteriormente.

4.4 PROTOCOLOS DE TRANSPORTE SEGURO

Los protocolos de transporte seguro proporcionan un medio seguro para transferir información a través del Internet. A continuación se describen las características de los protocolos MIME, PEM-MOSS, SSL, S-HTTP e iKP [7].

4.4.1 MIME (Multipurpose Mail Enhancements)

MIME es un protocolo de intercambio de objetos a través de Internet. Cada objeto se encapsula en una especie de concha que especifica tanto su semántica como el medio de codificación utilizado. La caracterización

semántica permite asociar los datos con su mecanismo de transporte (codificación) y con su significado, de forma que el remitente y el destinatario utilicen coordinadamente los datos intercambiados. MIME se desarrolló inicialmente para intercambios de correo electrónico, habiéndose extendido a muchos otros protocolos.

4.4.2 PEM - MOSS (Privacy Enhanced Mail y MIME Object Security Objects)

PEM es un sistema similar a MIME y desarrollado en paralelo con éste para crear objetos de correo garantizados. Con el desarrollo de MIME, PEM es, de alguna forma, repetitivo, por lo que se verá probablemente desplazado por MOSS, que no es más que una extensión de MIME que aporta exclusivamente lo que le falta a éste para obtener las garantías deseadas: claves, firmas, certificados, etc.

4.4.3 SSL (Secure Sockets Layer)

Secure Sockets Layer es una tecnología diseñada por Netscape Communications, que proporciona un nivel seguro de transporte entre el servicio clásico de transporte en Internet (TCP) y las aplicaciones que se comunican a través de él.

Las comunicaciones tienen lugar en dos fases. En una primera fase se negocia entre el cliente y el servidor una clave simétrica sólo válida para esta sesión. En

la segunda fase, se transfieren datos cifrados con dicha clave. Este sistema es transparente para las aplicaciones finales, que simplemente saben que el canal se encarga de proporcionarles confidencialidad entre extremos.

La fase inicial se realiza muy cuidadosamente para evitar tanto la intromisión de terceras partes como para evitar suplantaciones de personalidad de parte del centro servidor. El cliente conoce de antemano las claves públicas de ciertos notarios electrónicos. Con esta información se pone en contacto con el servidor, el cual le envía su clave pública, rubricada por el notario. La identificación se completa enviando al servidor un mensaje aleatorio que éste debe firmar. De esta forma el cliente sabe que al otro lado está quien dice estar.

Verificada la identidad del servidor, el cliente genera una clave de sesión y la envía cifrada con la clave pública del servidor. Conociendo ambos la clave de sesión, se intercambian datos con seguridad. En ciertas circunstancias puede ser necesario ejecutar una fase adicional para descubrir y legitimar la identidad del cliente.

SSL se utiliza fundamentalmente en los productos de la propia Netscape, concretamente con el Netscape Commerce Server y en el Netscape Navigator. Aunque la especificación permite diferentes algoritmos, el browser de Netscape sólo se exporta de EE.UU. usando algoritmos RC4 de cifrado simétrico restringidos a 40 bits. Esto da un nivel muy discutible de seguridad frente a ataques criptográficos.

4.4.4 S-HTTP (Secure HTTP)

Secure HTTP es un protocolo propuesto por Enterprise Integration Technologies (EIT) y patrocinado por el consorcio CommerceNet. Constituye una extensión del protocolo HTTP, incorporando cabeceras MIME para aportar confidencialidad, autenticación, integridad e irrenunciabilidad de las transacciones.

S-HTTP utiliza un sistema inspirado en PEM, añadiendo las cabeceras suficientes a cada transacción para lograr cada uno de los objetivos propuestos. Las transacciones HTTP constan simplemente de una petición de parte del cliente que induce una respuesta del servidor. S-HTTP especifica que el cliente envíe directamente toda la información pertinente: claves, certificados, códigos de integridad, etc. (incluyendo la posibilidad de referenciar secretos compartidos obtenibles exteriormente: intercambios previos o bases de datos comunes). El servidor responde siguiendo la misma filosofía PEM.

A diferencia de SSL, S-HTTP sólo afecta a las transacciones HTTP, sin extender su cobertura a otros protocolos habituales en Internet. Por lo demás, S-HTTP y SSL pueden convivir, utilizándose uno u otro en diferentes instantes de una transacción comercial, o incluso utilizándose simultáneamente.

4.4.5 iKP (Internet Keyed Payment Protocols)

Los protocolos iKP han sido desarrollados en los Laboratorios de IBM en Zürich y tratan de proporcionar formas seguras de pago multiparte. Aunque tienen voluntad de no ligarse a instrumentos específicos de pago, están implementados para usarse sobre tarjetas de crédito, confiando en las redes financieras preexistentes para realizar la transferencia de dinero.

Están basados en criptografía de clave pública RSA para asegurar la privacidad de los números de tarjeta de crédito y de los PIN, proporcionando características de no repudiación. iKP tiene tres opciones. Dependiendo de los requerimientos, iKP implica una clave pública (pagador, 1KP), dos claves (pagador y vendedor, 2KP) y tres (pagador, vendedor y consumidor, 3KP).

La criptografía nos proporciona funciones matemáticas para dotar a los datos de ciertas propiedades interesantes. Su utilización sólo involucra a las partes que intercambian información, si bien en ciertas situaciones se puede requerir la presencia de una tercera parte confiable que avale la transacción.

Además de las funciones matemáticas, que encriptan la información, ésta hay que transportarla. Para ello MIME proporciona un formato normalizado que se usa sobre objetos individuales (MOSS), sobre sesiones cliente-servidor (SSL) o sobre transferencias WWW (S-HTTP). No son técnicas incompatibles entre sí, sino más bien diferentes opciones de integración en un entorno transaccional.

4.5 ESQUEMAS DE PAGO ELECTRÓNICO

A continuación se describen las principales características de los sistemas de pago electrónico más utilizados en transacciones de comercio electrónico y las compañías que los han implementado [1,13,16,29].

4.5.1 Netscape

El sistema de Netscape, Secure Courier Electronic Payment Scheme, ha sido utilizado como sistema de pago seguro para los usuarios de programas de banco en su casa y los bancos; éste se basa en el protocolo SEPP, antecesor del SET. Compañías que trabajan con Mastercard, incluyendo Netscape Navigator, estan planeando incluir el Secure Courier, el cual encripta los datos y autentica a los individuos y comerciantes durante las transacciones de Internet.

4.5.2 Microsoft

El STT de Microsoft es similar a SEPP/SET en que provee firmas digitales y autenticación de usuarios para pagos electrónicos seguros. STT es una mejora de la versión de herramienta de seguridad SSL de Netscape. STT conserva las características básicas de SSL pero incluye un proceso más robusto de autenticación para la exportación de datos y mejora la eficiencia del protocolo de comunicaciones reduciendo el número de llamadas para comenzar la sesión

de comunicaciones. STT es una tecnología de propósito general para afianzar las transacciones financieras con aplicaciones más allá del Internet.

4.5.3 Checkfree

Checkfree Corporation provee servicios de procesamiento de pagos en línea para clientes mayores, incluyendo CompuServe, Genie, Cellular One, Delphi International Services Corporation, y Sky-Tel. Checkfree emplea una variedad de mecanismos para la manipulación de estos servicios, incluyendo Microsoft's STT, CyberCash, Netscape's SSL, and VeriSign's Digital ID. Checkfree también ha anunciado sus intenciones para soportar todos los métodos de seguridad para lograr destacar en el mercado.

4.5.4 CyberCash

CyberCash combina las características de los cheques y el efectivo. CyberCash es un sistema de software de dinero digital el cual es usado como una orden de dinero, garantizando el pago de la mercancía antes de que los bienes sean enviados. CyberCash provee una solución segura (cercana) para enviar información de tarjetas de crédito a través del Internet usando técnicas de encriptación que codifiquen la información de la tarjeta (ver Fig. 4.5).

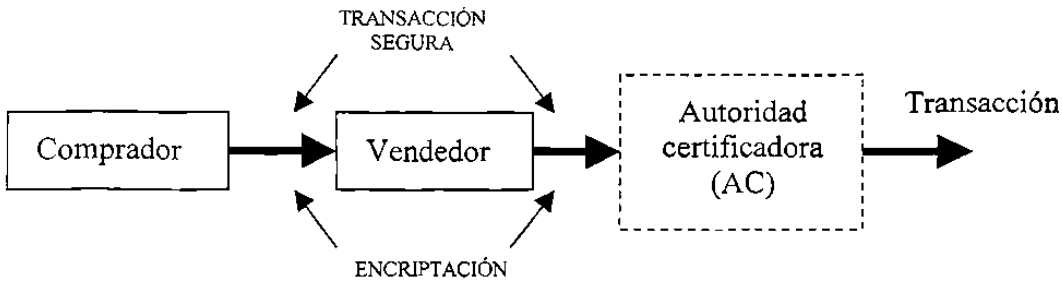

Fig. 4.5. Proceso de transacción electrónica de CyberCash.

4.5.5 VeriSign

VeriSign ofrece tecnología de firmas digitales para la autenticación de los usuarios como un componente separado de la encriptación, lo cual permite aumentar la confianza del proceso de autenticación. Como el gobierno de los Estados Unidos tiene (a la fecha) prohibido exportar los mecanismos de encriptación fuera del país, muchas compañías que tienen divisiones en otros continentes incrementan su seguridad usando tecnologías de autenticación de VeriSign's Digital ID.

4.5.6 DigiCash

DigiCash es una compañía de software cuyos productos permiten a los usuarios comprar bienes a través de Internet sin usar una tarjeta de crédito. La amenaza de pérdida de privacidad se resuelve a través del concepto de dinero electrónico anónimo, que es un almacenamiento electrónico para el manejo de fondos, el cual puede ser en una tarjeta para realizar compras electrónicas; este sistema es conocido como "monedero electrónico". La ventaja de DigiCash es

que proporciona el anonimato al comprador ya que el banco utiliza su propia firma digital en lugar de utilizar la del usuario.

En realidad, DigiCash es un sistema de pago electrónico basado en software que proporciona una total privacidad para el usuario. El principal beneficio del modelo utilizado por DigiCash es su habilidad de administrar grandes cantidades de dinero en comparación con los sistemas que manejan tarjetas de crédito.

Para que un usuario haga uso del servicio de DigiCash, debe contar con el software de encriptación de DigiCash (disponible en *www.digicash.com*) . Posteriormente, el usuario debe depositar el dinero en una cuenta de banco de DigiCash, a través de un cheque personal o por tarjeta de crédito, recibiendo a cambio monedas electrónicas. Durante la compra de un bien, el usuario debe enviar su solicitud de compra al banco de DigiCash. El banco verifica la firma digital del usuario para validar que se trata de un usuario registrado; una vez hecho esto, el banco reemplaza la firma digital del usuario por la del banco y retorna el dinero al usuario. Entonces, el usuario envia el dinero electrónico al vendedor del bien, el cual lo acepta basado en el hecho de que está respaldado por la firma digital del banco. Como sucede en otros sistemas, DigiCash no es completamente seguro, ya que es posible que un usuario no autorizado obtenga la clave de encriptación digital de un usuario registrado y la utilice para compras fraudulentas.

4.5.7 First Virtual

First Virtual es un sistema enfocado a individuos o pequeñas empresas que desean realizar transacciones comerciales por Internet pero que no cuentas con la infraestructura para operaciones en linea. Utilizando una cuenta de correo electrónico de First Virtual y su servidor para rastrear y almacenar la información de productos y órdenes de pago, es posible que el comprador y el vendedor interactuen a través del Internet para la compra/venta de bienes y servicios sin la necesidad de transmitir información financera, como son los datos de tarjeta de crédito. Todo este tipo de información se intercambia por teléfono (ver Fig. 4.6).

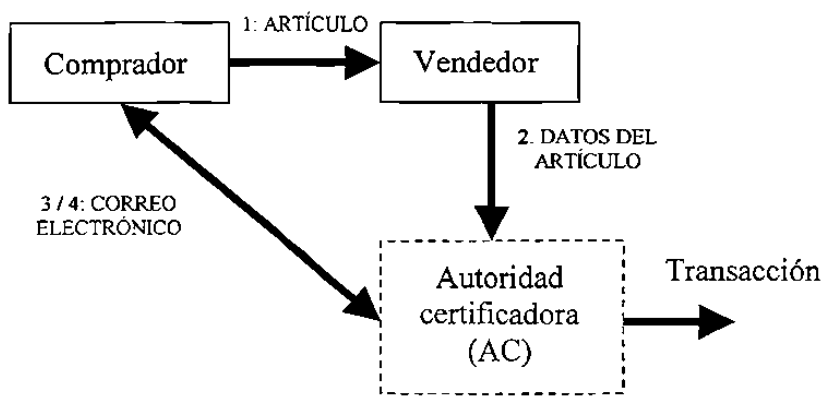

Fig. 4.6. Proceso de transacción electrónica de First Virtual.

Utilizando el sistema de First Virtual, el comprador dispone de una cuenta en el sistema, que al momento de registarse recibe un password a cambio de un número válido de tarjeta de crédito. El password no es encriptado durante su transferencia por Internet, ya que First Virtual solicita al comprador la

confirmación de cada pago por medio no electrónico. La seguridad del sistema se basa en el hecho de que los compradores están en la posibilidad de rechazar un pago durante un lapso de tiempo posterior a la transacción.

4.5.8 NetCash

NetCash es una opción para los cheques de viajeros. Para utilizar este sistema, el usuario debe registrar su número de cuenta de cheques o tarjeta de crédito; esto habilita al usuario a adquirir cupones electrónicos de NetCash, cada uno de los cuales está registrado con un número de serie. Para comprar un bien, el usuario accesa la lista de vendedores disponibles en NetCash y selecciona los productos que desea adquirir. Para ello, el usuario envia los cupones electrónicos al vendedor, quien los remite de nueva cuenta a NetCash para hacerlos efectivos. EL sistema no es completamente seguro, por lo que se impone un límite de 100 dólares americanos por cada transacción. Adicionalmente, el sistema de NetCash no permite a los vendedores ofrecer productos que deban ser enviados por servicio postal.

4.5.9 CommerceNet

Más que un sistema de pago electrónico, CommerceNet es un consorcio industrial que tiene por objetivo facilitar las actividades de comercio electrónico por Internet y crear oportunidades de negocios para su miembros. Entre las actividades que realiza están (a) la definición de marcos legales regulatorios

para fomentar el comercio global, (b) asesorías especializadas para asistir a los miembros en el desarrollo de estrategias comerciales por Internet, (c) definición de soluciones industriales verticales para la identificación de oportunidades de negocios y (d) desarrollo de un estándar de comercio electrónico, denominado E-co, a través de la definición de protocolos que aseguren la interoperatividad entre sistemas.

CommerceNet nació en 1994, agrupando a 20 empresas de Silicon Valley, entre las que se encuentran Apple Computer, Bank of America, Pacific Bell, Wells Fargo y Xerox entre otras.

4.5.10 JEPI

JEPI no es un sistema de pago que representa un intento por fusionar las tecnologías de los sistemas de pago bajo una misma especificación. JEPI, Joint Electronic Payment Initiative representa un esfuerzo del consorcio World Wide Web (W3C) y CommerceNet para alcanzar la interoperatividad de los sistemas de comercio electrónico. Aunque JEPI no es un sistema de pago, considera los procesos de pago y compra descritos en la sección 4.3 (ver Fig. 4.7, tomada de [1]). Apoyandose en el soporte del estándar SET (sección 4.6), JEPI se compone de dos partes. La primera es una capa de extensión denominada PEP (Protocol Extension Protocol) que se situa en la parte superior del servidor básico de Web HTTP. La segunda parte es el UPP (Universal Payment Preamble) que es una capa de protocolo de negociación que tiene la función de

identificar en forma apropiada la metodología de pago de cada vendedor. Actualmente, la segunda fase de desarrollo de JEPI esta en proceso, donde se está considerando la inclusión de los más recientes sistemas de pago, como son los micropagos [7]. En cierta forma, JEPI puede ser considerado un competidor directo del estándar SET [30].

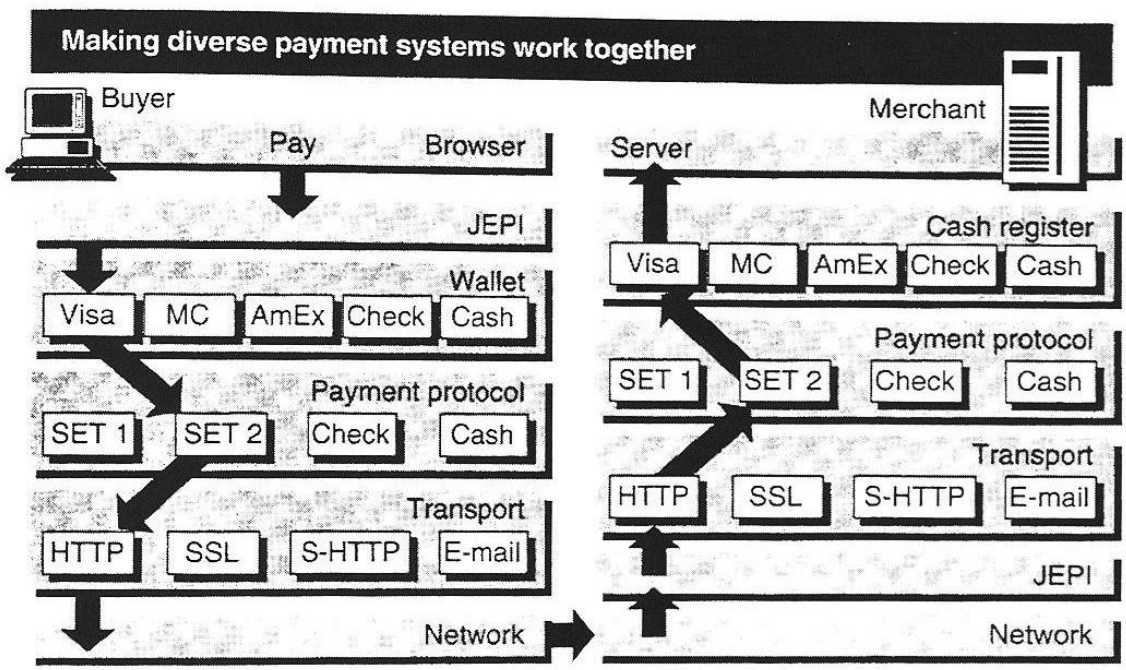

Fig. 4.7. Modo de operación de JEPI [1].

4.5.11 Otros

Recientemente han aparecido nuevos sistemas de pago basados en la misma tecnología que los sistemas descritos, pero que incorporan distintos procedimientos para la verificación de los usuarios y verificación de la

autenticidad de las transacciones. Algunos de estos sistemas son Mondex, Netmarket, OpenMarket, Global On-line, NetBill, entre otros [1,7].

4.6 ESTÁNDAR SET

La especificación SET, Secure Electronic Transactions, en español, Transacción Electrónica Segura, está diseñada con el propósito de asegurar y autenticar la identidad de los participantes en las compras abonadas con tarjetas de pago en cualquier tipo de red en linea, incluyendo la Red Internet [6,30]. La especificación SET es la manera más segura de realizar una compra vía Internet, ya que la información de pago al usar SET viaja encriptada, es decir, sólo el receptor legítimo la puede descifrar y además, se utiliza un esquema de certificados digitales que permite garantizar la identidad de las entidades que participan en la transacción. En pocas palabras, el usuario puede verificar la legitimidad del comercio y el comercio puede tener la confianza de que el usuario posee una relación bancaria legítima y por ende, recibirá su pago. El proceso subyacente en una transacción SET típica funciona de forma muy parecida a una transacción convencional con tarjeta de crédito:

1) Decisión de compra del cliente. El cliente está navegando por el sitio Web del comerciante y decide comprar un artículo. Para ello llenará algún formulario al efecto y posiblemente hará uso de alguna aplicación tipo carrito de la compra, para ir almacenando diversos artículos y

pagarlos todos al final. El protocolo SET se inicia cuando el comprador pulsa el botón de Pagar o equivalente.

2) Arranque de la cartera. El servidor del comerciante envía una descripción del pedido que despierta a la aplicación cartera del cliente (vea el recuadro "La cartera safeWallet").

3) Transmisión cifrada de la orden de pago. El cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante. La aplicación cartera crea dos mensajes que envía al comerciante. El primero, la información del pedido, contiene los datos del pedido, mientras que el segundo contiene las instrucciones de pago del cliente (número de tarjeta de crédito, banco emisor, etc.) para el banco adquiriente. En este momento, el software cartera del cliente genera un firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el comerciante puede acceder a la información del pedido, pero no a las instrucciones de pago, mientras que el banco puede acceder a las instrucciones de pago, pero no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso, ya que ni el comerciante llega a conocer el número de tarjeta de crédito empleado por el comprador, ni el banco se entera de los hábitos de compra de su cliente.

4) Envío de la petición de pago al banco del comerciante. El software SET en el servidor del comerciante crea una petición de autorización que envía a la pasarela de pagos, incluyendo el importe a ser autorizado, el identificador de la transacción y otra información relevante acerca de la misma, todo ello convenientemente cifrado y firmado. Entonces se envían al banco adquiriente la petición de autorización junto con las instrucciones de pago (que el comerciante no puede examinar, ya que van cifradas con la clave pública del adquiriente).

5) Validación del cliente y del comerciante por el banco adquiriente. El banco del comerciante descifra y verifica la petición de autorización. Si el proceso tiene éxito, obtiene a continuación las instrucciones de pago del cliente, que verifica a su vez, para asegurarse de la identidad del titular de la tarjeta y de la integridad de los datos. Se comprueban los identificadores de la transacción en curso (el enviado por el comerciante y el codificado en las instrucciones de pago) y, si todo es correcto, se formatea y envía una petición de autorización al banco emisor del cliente a través de la red de medios de pago convencional.

6) Autorización del pago por el banco emisor del cliente. El banco emisor verifica todos los datos de la petición y si todo está en orden y el titular de la tarjeta posee crédito, autoriza la transacción.

7) Envío al comerciante de un testigo de transferencia de fondos. En cuanto el banco del comerciante recibe una respuesta de autorización del banco emisor, genera y firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, la cual se la hace llegar al comerciante.

8) Envío de un recibo a la cartera del cliente. Cuando el comerciante recibe la respuesta de autorización de su banco, verifica las firmas digitales y la información para asegurarse de que todo está en orden. El software del servidor almacena la autorización y el testigo de transferencia de fondos. A continuación completa el procesamiento del pedido del titular de la tarjeta, enviando la mercancía o suministrando los servicios pagados. Además, se le entrega a la aplicación cartera del cliente un recibo de la compra para su propio control de gastos y como justificante de compra.

9) Entrega del testigo de transferencia de fondos para cobrar el importe de la transacción. Después de haber completado el procesamiento del pedido del titular de la tarjeta, el software del comerciante genera una petición de transferencia a su banco, confirmando la realización con éxito de la venta. Como consecuencia, se produce el abono en la cuenta del comerciante.

10) Cargo en la cuenta del cliente. A su debido tiempo, la transacción se hace efectiva sobre la cuenta corriente del cliente.

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

En su estado actual SET solamente soporta transacciones con tarjeta de crédito/débito, y no con tarjetas monedero [31,32]. Se está trabajando en esta linea para extender el estándar de manera que acepte nuevas formas de pago. Al mismo tiempo se están desarrollando proyectos para incluir los certificados SET en las tarjetas inteligentes, de tal forma que el futuro cambio de tarjetas de crédito a tarjetas inteligentes pueda incorporar el estándar SET.

4.7 CONCLUSIONES DEL CAPÍTULO

El comercio electrónico puede ser analizado en su conjunto como un sistema de pago seguro, donde los usuarios y ofrecedores de bienes y servicios realizan transacciones a través del Internet. Para ello, los sistemas de pago deben asegurar la confidencialidad de la información, verificar la integridad de la información que se transmite, verificar la autenticidad de las cuentas de los usuarios y su acceso por parte del vendedor, y asegurar la interoperabilidad entre las plataformas de cómputo del usuario y del vendedor.

CAPÍTULO 5

COMPARACIÓN DE SISTEMAS DE SEGURIDAD PARA EL COMERCIO ELECTRÓNICO

5.1 INTRODUCCIÓN

En el Capítulo 4 se realizó una descripción de los sistemas de pago electrónico que actualmente dominan las transacciones a través del Internet. Cada uno de estos sistemas tienen distintas características en cuanto al tipo de transacción que se puede realizar y el nivel de seguridad que ofrecen a sus usuarios.

En el caso de los sistemas de pago por Internet, existen diversos mecanismos tanto convencionales como especializados. Actualmente, los métodos de pago convencionales como efectivo y cheques no son adecuados para sistemas de pago interactivo en tiempo real. Actualmente, la mayoría de los sistemas de pago por Internet utilizan dinero latente, como tarjetas de crédito, órdenes de compra con promesa de pago y transferencias de efectivo. También existen

sistemas emergentes, algunos de los cuales basan sus operaciones en transacciones en dinero electrónico y micro pagos, que no tienen gran aceptación.

En las siguientes secciones se describen los resultados de un estudio comparativo de los sistemas de seguridad utilizados en los sistemas de pago electrónico que sirven de base para el comercio electrónico.

5.2 CRITERIOS DE COMPARACIÓN

Existen diversos factores que pueden ser considerados para evaluar un sistema de seguridad para pago electrónico, desde el medio de comunicación que se utiliza con el usuario, hasta los aspectos técnicos de los protocolos de transporte seguro utilizados para realizar las transacciones por Internet.

Los tres aspectos que tienen mayor influencia para la selección de un determinado sistema son la disponibilidad, los costos iniciales de inversión y la seguridad. Los sistemas basados en llamadas telefónicas son frecuentemente utilizados por los usuarios debido a su ubicuidad, su bajo costo y alto nivel de seguridad. En contraste, el uso de Internet tiene menos penetración, así como costos de inversión mayores; sin embargo, esto empieza a cambiar a medida que más usuarios tienen acceso al Internet para otro tipo de actividades (correo electrónico, videoconferencias, etc.). En cuanto a la seguridad, ésta ha sido

mejorada sustancialmente con el desarrollo de nuevos protocolos (SSL, SET, etc.) y sistemas de procesamiento de datos.

5.3 RESULTADOS

Actualmente existe una amplia diversidad de mecanismos de pago electrónico, cada uno con sus ventajas e inconvenientes. Por tanto, en ausencia de un único estándar, se hace necesario que las empresas que se dediquen al comercio electrónico ofrezcan al cliente la posibilidad de elegir el método de pago. Aunque, lógicamente, el costo de la plataforma aumenta, cliente y proveedor se benefician de la diversidad de posibilidades. Tanto la Unión Europea como Estados Unidos favorecen los acuerdos de la industria como mejor forma de incrementar la interoperabilidad, aunque sin descartar la necesidad de introducir normas generales. La iniciativa JEPI (Joint Electronic Payment Initiative) del Consorcio W3 y la asociación CommerceNet definen un protocolo que permite negociar automáticamente cuál de los múltiples métodos de pago aceptables para el comprador y el vendedor se deben utilizar en una transacción particular.

Desde este punto de vista, el pago con tarjeta de crédito, el uso de cheques y órdenes de pago electrónicas y la utilización de dinero electrónico son los métodos de pago más utilizados a través del Internet. En el caso de las tarjetas de crédito, el protocolo SET (Secure Electronic Transaction) regula la mayor parte de las transacciones con tarjeta de crédito en Internet. Definido por MasterCard y Visa con la colaboración de otras importantes compañías como

IBM, Microsoft y Netscape, SET permite un alto nivel de seguridad en las transacciones. Para ello utiliza procedimientos de cifrado simétrico y asimétrico, firmas digitales y certificados de seguridad. SET funciona desde 1997 y supone una garantía inestimable de seguridad y eficacia para el cliente y el proveedor. Existen otros sistemas de pago electrónico basado en tarjetas, como son CyberCash y FirstVirtual.

En el caso de los cheques y órdenes de pago electrónicas, el pago con tarjeta es menos habitual. En las transacciones entre empresas es más frecuente la utilización de cheques y pagos electrónicos. Un ejemplo es el sistema eCheck, basado en un "talonario de cheques electrónicos" que permite a las empresas realizar sus compras y ventas de forma fiable y segura. Otro ejemplo es el sistema NetCheque, desarrollado por la Universidad del Sur de California, que básicamente reproduce en la Red el sistema usual de emisión de cheques y compensación entre bancos.

Los sistemas de pago citados anteriormente sirven para realizar transacciones electrónicas sobre dinero no electrónico. Existe otro grupo de sistemas en los que se maneja directamente dinero "virtual", por ejemplo almacenado en una tarjeta inteligente que hace de monedero electrónico. Estos sistemas se basan en el prepago, es decir la conversión previa de dinero real en dinero electrónico. Por comparación, los sistemas de cheque electrónico serían sistemas de tipo "pague ahora" y los de pago electrónico con tarjeta serían de tipo "pague después".

Los sistemas de dinero electrónico suelen caracterizarse por un bajo costo de cada operación de pago, lo que los hace muy apropiados para realizar micropagos. Por micropagos se entiende cantidades pequeñas, por ejemplo unos pocos dólares, y que en ocasiones pueden llegar a ser del orden de un dólar o incluso menores. Los micropagos son muy importantes para hacer posible el comercio electrónico de fotografías, imágenes, noticias, pequeños programas y otros elementos que pueden tener un valor unitario bajo, así como para poner en práctica esquemas de pagar por ver páginas Web, pagar por jugar a un juego a través del Internet, etc.

En la actualidad existen diversas empresas que ofrecen servicios de comercio electrónico para que otras compañías ofrezcan sus productos y servicios a través del Internet. Estos servicios se instalan en servidores de las empresas para crean un centro de ventas virtual, con el soporte necesario para realizar transacciones electrónicas con cualquier potencial usuario a través del Internet. Netscape and OpenMarket fueron los primeros en ofrecer este servicio, basados principalmente en los protocolos SSL y S-HTTP para asegurar la confidencialidad de las transacciones. Por otra parte, Microsoft ha planeado utilizar los productos VeriFone como parte de su Merchant System, un servidor de comercio electrónico basado en tecnología Windows-NT. Recientemente, Netscape y Oracle han anunciado su intención de incorporar vPOS, una herramienta de VeriFone, como parte de sus sistemas de comercio electrónico [33,34].

Considerando lo anterior, se realizó un estudio para analizar las características de los sistemas de seguridad para pago electrónico que ofrecen diversas empresas para actividades de comercio electrónico. Los resultados de este estudio se resumen en la Tabla 5.1. Estos resultados demuestran la tendencia hacía la estandarización de los sistemas de pago a nivel internacional, siendo JEPI uno de los primeros intentos.

Tabla 5.1. Resultados de la evaluación.

PRODUCTO	TIPO DE PRODUCTO	COMPATIBILIDAD	USUARIOS	SEGURIDAD
BroadVission One-Two-One (Broadvision Inc.)	Herramienta Web	HP-UX SunOS Sun Solaris Sun Net Windows NT Irix	Windows Windows NT	CGI support API Secure server SSL support HTTP support EDI support SET support Multithreaded processing Forms processing Intermerchant trade
OneServer (Connect Inc.)	Aplicación interactive	AT&T Unix HP-UX HP OpenView IBM RS/6000 NFS	Windows X Windows Visual Basic	CGI support API Secure server SSL support EDI support

		SunOS Sun Solaris Windows NT		SET support Multithreaded processing Forms processing Intermerchant trade
Secure Internet payment service (CyberCash)	Programa de pagos y servicios por Internet	SunOS Sun Solaris Windows NT Irix SCO Unix	Windows Visual Basic	CGI support API SET support
CyberCat (Evergreen Internet Inc.)	Programa commercial en línea	SunOS Sistemas Unix Windows NT	Programas de navegación por Internet	CGI support Secure server SSL support HTTP support EDI support Multithreaded processing Forms processing Intermerchant trade
Tango Merchant (EveryWare Development Corp.)	Aplicación comercial	Windows NT Apple	Windows MAC	CGI support SSL support Multithreaded processing Forms processing
CyberStream (Geac SmartStream)	Aplicación administrativa	SunOS Sun Solaris HP-UX	Windows Estaciones de trabajo	CGI support

		Windows NT	Sun	
PC-Charge (Go Software)	Programa de procesamiento de tarjetaas de crédito	Windows 3.x Windows 9x Windows NT	Windows	- - -
PC-Charge interfase (Go Software)	Herramienta de integración	Windows 3.x Windows 9x Windows NT	Windows	API
PC-Charge Web (Go Software)	Herramienta de desarrollo	AT&T Unix Windows 3.x Windows 9x Windows NT SCO Unix	- - -	CGI Support

5.4 OBSERVACIONES SOBRE LA SITUACIÓN DEL COMERCIO ELECTRÓNICO EN MÉXICO

El primer proyecto interoperable de comercio electrónico seguro usando SET se dió el 23 de abril de 1999 [35]. Banorte, Banco Bilbao-Vizcaya y Citibank realizaron la primera transacción interoperable de comercio electrónico seguro en México, con el apoyo de Visa, VeriFone y Prosa. Esto representó un claro avance en el impulso a la utilización de Internet en nuestro país para operaciones de compra-venta de manera segura.

La operación fue realizada con una tarjeta de Banorte y un comercio afiliado por el Banco Bilbao-Vizcaya, y demostró las enormes ventajas que ofrece la utilización del estándar SET (Secure Electronic Transaction), ya que permitió que la transacción se realizara de manera segura entre una institución afiliada a un banco y un tarjetahabiente de otra institución. Por su parte, Citibank presentó las perspectivas de las instituciones financieras respecto al comercio electrónico y las ventajas de la interoperabilidad.

De los esfuerzos que se han realizado en México por parte de particulares de alcanzar un esquema ordenado, seguro y actualizado para el ejercicio del comercio electrónico, en 1986 se conformó la Asociación Mexicana de Estándares para el Comercio Electrónico (AMECE), la cual promueve el uso de normas y sus beneficios para el desarrollo del Comercio Electrónico [36]. Ésta se encuentra respaldada por organizaciones internacionales como *Uniform Code Counc*il (UCC) de los Estados Unidos de Norteamérica y, *International Article Numering Association* (EAN). Esta asociación civil, promueve principalmente estándares como Código de Barras o Código de Producto, Número de Localización EAN e Intercambio Electrónico de Datos, EDI. Actualmente AMECE agrupa a poco más de 15 mil empresas en contraparte con las 27 que la fundaron hace ya casi catorce años.

5.5 TENDENCIAS

Actualmente, el sistema de pago electrónico que mayor dominio del mercano tiene es DigiCash. Este sistema proporciona un alto nivel de seguridad a sus usuarios, y posee la ventaja de ofrecer el anonimato al comprador. Aunque el sistema puede ser monitoreado, y sus transacciones objetos de fraudes, el sistema tiene un buen desempeño. Sin embargo, este liderazgo puede representar su mayor desventaja a largo plazo, ya que en un futuro sistemas de pago con diferentes esquemas de operación deberán coexistir para asegurar la interoperabilidad en beneficio de los usuarios. Esta es la visión del proyecto JEPI, encabezado por W3C y CommerceNet.

En el caso de México, el comercio electrónico no ha desarrollado su máximo potencial, debido principalmente al rezago en los sistemas de comunicación y a la desconfianza de los usuarios. Actualmente, el protocolo SSL es el más utilizado para transacciones a través del Internet, sin embargo, estas transacciones son mayoritariamente consultas de saldos y transferencias de fondos entre cuentas bancarias.

5.6 CONCLUSIONES DEL CAPÍTULO

Cada uno de los sistemas de seguridad para el pago electrónico a través de Internet ofrecen distintas ventajas a sus usuarios, desde esquemas de seguridad para el uso de tarjetas de crédito, hasta el anonimato en cualquier

tipo de transacción. Los niveles de seguridad de cada tipo de sistema está en dependencia del tipo de protocolo que utilice, y del proceso de manejo de información que se realice a través de las autoridades certificadoras, por lo cual no es posible determinar cual sistema es mejor que otro. Los resultados de este estudio ponen de manifiesto que la tendencia en el desarrollo de estos sistemas no es la creación de nuevos esquemas y procedimientos, sino la integración de los esquemas que actualmente están en operación.

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

El objetivo de este trabajo de tesis, fue estudiar los aspectos fundamentales del comercio electrónico y su implementación a través de sistemas de pago electrónico; las conclusiones derivadas de este estudio son las siguientes:

- El uso de Internet para el comercio electrónico se ha difundido rápidamente debido a sus características de una red de comunicación abierta con un procesamiento de información distribuido; además, el uso del Internet tiene la ventaja de poder conectar a los usuarios y vendedores de bienes y/o servicios en cualquier parte del mundo; sin embargo esta ventaja se convierte en la principal desventaja si es que no se toman las medidas de seguridad para proteger los datos que se transfieran por la red.

- El uso de Internet facilita la interoperabilidad entre distintas plataformas de cómputo facilitando la comunicación entre usuarios independientemente de las características de sus redes locales; sin embargo aún existen debilidades en el protocolo TCP/IP que permiten que los mensajes puedan ser fácilmente monitoreados y accesados durante una transmisión.

- El nivel de seguridad se ha incrementado con la aplicación de métodos de encriptación y tecnologías de acceso digital para asegurar la privacidad de los mensajes transmitidos a través de Internet. El objetivo es proporcionar los objetivos esenciales de seguridad, la confidencialidad, la autenticación, la integridad de los datos y la repudación sin perder la capacidad de interoperabilidad.

- Los algoritmos de encriptación de información están basados en algoritmos matemáticos, y tienen el objetivo de garantizar la confidencialidad de la información que se transmita a través de una red de datos restringiendo el acceso a usuarios no autorizados. En dependencia del tipo de clave que se utiliza para cifrar y descifrar un mensaje, los algoritmos de encriptación se dividen en simétricos y asimétricos.

- Los algoritmos simétricos son los más simples, ya que se utiliza una misma clave para cifrar y descifrar, lo que representa un bajo nivel de seguridad. Los algorimos asimétricos utilizan dos claves, una pública y una privada, de tal forma que lo que una cifra la otra descifra, donde la clave privada solo es conocida por su propietario; esto aumenta la seguridad ya que aunque un mensaje sea monitoreado, no puede ser descifrado.

- Las autoridades de certificación son empresas que tienen la función de monitorear la información entre dos usuarios a través del Internet con el objetivo de verificar su autenticidad y evitar el problema de usurpación de personalidad. Para ello, proporcionan un código de autenticidad para los usuarios que desean hacer una transacción, el cual se utiliza para firmar digitalmente los mensajes con datos personales de cada usuario.

- Las firmas digitales son un mecanismo de autenticidad de los usuarios para intercambiar mensajes de manera segura. La firma digital se forma mediante una función hash que genera un resumen único del mensaje (no reproducible), el cual es cifrado con la clave del usuario. La firma digital se incluye en el mensaje y se analiza por cada usuario para determinar su autenticidad; una autoridad certificadora también valida la firma digital con el fin de resolver conflictos entre usuarios.

- En el caso de redes privadas que se conectan a Internet, además de los algoritmos de encriptación, es necesario disponer de otros medios de seguridad. Los firewalls tienen el objetivo de monitorear el tráfico de información entre una red privada y una red pública, a fin de restringir el acceso a usuarios no autorizados. Adicionalmente, es necesario definir una política de seguridad para proteger los recursos y servicios con que cuenta la red.

- Los procesos de pago y compra involucran cuatro etapas, el registro de la cuenta del usuario, el registro del vendedor o compañía que ofrece el bien, el envío de la orden de compra y la autorización de pago. La confidencialidad de este proceso se asegura mediante el uso de firmas digitales, que son validadas por una autoridad certificadora, y que son cifradas como parte de todos los mensajes que forman parte de la transacción.

- Un aspecto importante de este proceso es que el vendedor en ningún momento tiene acceso a la información de la cuenta del usuario; esto incluye a cualquier usuario no autorizado que estuviera monitoreando los mensajes de la transacción. Esto aumenta la confianza de los usuarios para realizar transacciones a través del Internet.

- Existen diversos sistemas de pago seguro que ofrecen sus servicios para la compra de bienes y servicios por Internet. Cada sistema utiliza un protocolo de transporte seguro de información (MIME, MOSS, SSL, S-http, etc.) y un procesamiento de información particular para asegurar el mayor nivel de seguridad para sus usuarios. Su evolución ha sido dictada por el desarrollo de las comunicaciones y el desarrollo de nuevos estándares de seguridad integrados en los protocolos de comunicación.

- En la actualidad el estándar SET, creado por las compañías VISA y Mastercard, posee los más altos estándares de seguridad, pero su uso esta restringido a transacciones con tarjetas de crédito/débito. Debido a ello, está en desarrollo el JEPI, un estándar para intercambio de información, que tiene la ventaja de interconectar cualquier sistema de pago independientemente de sus plataformas de cómputo, lo que asegura su interoperabilidad.

- Es importante mencionar que en México el comercio electrónico no ha desarrollado su máximo potencial, debido principalmente al rezago en los sistemas de comunicación y a la desconfianza de los usuarios. Actualmente, el protocolo SSL es el más utilizado para transacciones a través del Internet, sin embargo, estas transacciones son mayoritariamente consultas de saldos y transferencias de fondos entre cuentas bancarias.

6.2 APORTACIONES

Las principales aportaciones derivadas de la realización de este trabajo de tesis son las siguientes:

- Se proporciona una descripción de las características principales de los sistemas de comercio electrónico; estos sistemas se analizan como sistemas de pago electrónico en una red de comunicación, cuyo principal problema son las violaciones de seguridad asociadas a la transmisión de información privada a través de redes de acceso público, como Internet.

- Se analizaron los distintos algoritmos de encriptación de información utilizados para la transferencia de información por Internet, los cuales sirven de base para la definición de procedimientos de operación relacionados con el envío y recepción de mensajes en forma segura que se utilizan en los sistemas de pago electrónico.

- Se realizó un estudio comparativo entre los distintos sistemas de seguridad de pago electrónico que ofrecen diversas empresas para la implementación de servicios de comercio electrónico, utilizados por otras compañías para ofrecer sus bienes y servicios a través del Internet. Los resultados de este estudio ponen de manifiesto que la tendencia en el desarrollo de estos sistemas no es la creación de nuevos esquemas y

procedimientos, sino la integración de los esquemas que actualmente están en operación.

6.3 RECOMENDACIONES PARA TRABAJOS FUTUROS

En base a los resultados presentados en este trabajo de tesis, se recomienda continuar los trabajos de investigación en los siguientes tópicos:

- Estudiar los aspectos legales asociados a la realización de transacciones fraudulentas a través de los sistemas de pago electrónico.

- Estudiar las nuevas propuestas de integración de los sistemas de pago electrónico, como es el caso del proyecto JEPI, que busca establecer un estándar único que permita que cualquier usuario tenga acceso a los servicios de comercio electrónico independientemente de su plataforma de cómputo y tipo de esquema de pago.

BIBLIOGRAFÍA

[1] D. Minoli y E. Minoli, *Web Commerce Technology Handbook*, McGraw Hill, NewYork, 1998.

[2] J. Solinsky, *An Introduction to Electronic Commerce*, MIT, 1994.

[3] R. G. Saltman, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*, National Institute of Standards and Technology 800-9, Washington, 1993.

[4] National Electronic Authentication Council (NEAC), *The Integration of Business E-Commerce Systems*, Published by the National Office for the Information Economy, Canberra, 2000.

[5] R.Drummond, *"Safe and secure electronic commerce,"* Network Computing, December 1996, pp.116-118.

[6] J. Sandberg, "Visa, Mastercard to jointly develop internet pay plan," *The Wall Street Journal*, June, 1995, sec B5.

[7] M. A. González Sastre, Comercio Electrónico, Seguridad y Sistemas de Pago en la Red, http://personales.com/espana/leon/tristan

[8] M.S. Cronin, *Businesses and the Internet*, Van Nostrand Reinhold, NewYork, 1993.

[9] D.Minoli, *Internet and Intranet Engineering*, McGraw Hill, NewYork, 1997.

[10] M.Rose, *"Enabiling technologies for internet commerce,"* Network world & Interop Conference, September, 1995.

[11] F.B.Cohen *Protection and Security on the Information Superhighway*, John Wiley, NewYork, 1995.

[12] W.R. Cheswick, S.M. Belbuin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, Reading, Massachusetts, 1994.

[13] G.S. Howard, *Introduction to Internet Security: From Basics to Beyond*, Prima Publishing, 1995.

[14] R. Kalakota, M. Robinson, *Del E-Commerce al E-Business, el siguiente paso*, Pearson Education, Massachusetts, 2001.

[15] S. Y. Choi, D. O. Stahl and A. B. Whinston, *The Economics of Electronic Commerce*, MacMillan Technical Publishing, U.S.A., 1997.

[16] L. Martínez López, *"Sistema de pago seguro: Seguridad en el comercio electrónico,"* Revista ALI Base de la Asociación de Doctores, Licenciados e Ingenieros en Informática, no. 36, Junio 2000, pp. 58-60.

[17] J. R. Minor, *Hackers, Phrackers, and Crackers, The true story of Kevin Mitnick-World famous Computer Hacker*, Interzine, 1995.

[18] C. Kaufman, R.Perlmand, M.Speciner, *Network Security: Private Communication in a Public World*, Prentice Hall, Englewood cliffs, New Jersey, 1995.

[19] G. Brassard, *Modern Cryptology*, Springer-Verlag, NewYork, 1998.

[20] B.Schneier, *Applied Cryptography*, Second Edition, John Wiley, NewYork, 1996.

[21] W.Stallings, *Internet Security Handbook*, IDG Books, Foster City, California, 1995.

[22] RSA Laboratories, http://www.rsa.com.

[23] P.Fahn, *Answers to FAQs about Today's Cryptography*, RSA Labs, 1993.

[24] Public-Key Infrastructure (X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html.

[25] A.Saloma, *Public Key Cryptography*, Springer-Verlag, NewYork, 1990.

[26] M. Swanson, B. Guttman, *Generally Accepted principles and Practices for Securing Information Technology Systems*, National Institute of Standards and Technology 800-14, Washington, 1996.

[27] B. Guttman, R. Bagwill, *Internet Security Policy: A Technical Guide*, National Institute of Standards and Technology (DRAFT), Washington, 2000.

[28] RFC 1244 - Site Security Handbook, http://www.net.ohio-state.edu/hypertext/rfc1244/toc.html.

[29] NIST Computer Security Resource Clearinghouse, http://csrc.nist.gov.

[30] MasterCard, VISA, *SET Secure Electronic Transaction Specification version 1.0, Book 3: Formal Protocol Definition*, May 1997.

[31] VISA, http://www.visa.com.

[32] Mastercard, http://www.mastercard.com.

[33] London School of Economics Computer Security Research Centre, http://csrc.lse.ac.uk/csrc/csrchome.htm.

[34] Institute for Computer and Telecommunications Systems Policy, *http://wwwseas.gwu.edu:80/seas/ictsp*.

[35] Humberto Lagarde Moguel, "México: el comercio electrónico un reto," *Revista Electrónica Razón y Palabra*, No. 20, Año 4, Noviembre 2000 - Enero 2001.

[36] AMECE, *http://www.amece.com.mx*.

RESUMEN AUTOBIOGRÁFICO

Ma. MAGDALENA GARZA SÁNCHEZ

Candidato para el Grado de Maestro en Informática Administrativa

Tesis: ANÁLISIS Y EVALUACIÓN DE SISTEMAS DE SEGURIDAD PARA EL COMERCIO ELECTRÓNICO

Campo de Estudio: Informática

Biografía:

Datos Personales : Nacida en Monterrey, Nuevo León el 4 de Enero de 1971, hija de Eric Garza Garza y Hortencia Sánchez Guajardo.

Educación : Egresada de la Universidad del Norte, con los grados de Ingeniero Industrial y de Sistemas en 1991 y Licenciado en Informática Administrativa en 1992, y Diplomado en Information Technology Management en el verano-otoño 2000 por The University of Manitoba, Winnipeg, Canadá.

Experiencia Profesional : Coordinadora de Informática de la Universidad del Norte desde 1991, impartición de diversas cátedras tales como Estructura de Datos, Lenguajes de Programación y materias del área de Análisis y Diseño de Sistemas de Información.