Revista de Estudios Empresariales. Segunda época.
Número: 1 (2009). Páginas: 63 - 76

SISTEMAS DE PAGO SEGURO. SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Martínez López, Luis (Universidad de Jaén) (martin@ujaen.es)
Mata Mata, Francisco (Universidad de Jaén) (fmata@ujaen.es)
Rodríguez Domínguez, Rosa Mª (Universidad de Jaén) (rmrd0001@estudiante.ujaen.es)

RESUMEN

El comercio electrónico en Internet irrumpió con gran fuerza a finales de los 90, prometiendo ser un elemento transformador de la sociedad en el s. XXI. Aunque su evolución ha sido importante, no ha alcanzado las estimaciones iniciales. Uno de los principales problemas para este retraso ha sido la falta de herramientas que proporcionasen confianza a los usuarios en el uso del modelo de comercio a través de redes de ordenadores. Afortunadamente con el tiempo han ido surgiendo tecnologías y sistemas de pago electrónico que ofrecen garantías de seguridad e integridad para realizar estas transacciones de una forma fiable y de este modo, dar confianza a los usuarios. No obstante, este sigue siendo el mayor obstáculo (no tanto técnico como psicológico) a vencer para que se produzca el uso e implantación masivo del comercio electrónico. En este trabajo hacemos una revisión de los tres protocolos de pago más utilizados en el comercio electrónico, SSL (Secure Sockets Layer), SET (Secure Electronic Transaction) y 3D Secure, con el propósito de disipar las posibles dudas en cuanto a la falta de seguridad en las transacciones electrónicas a través de Internet.

Palabras claves: Comercio electrónico**,** seguridad, protocolos de pago seguro. **JEL:** 033

ABSTRACT

The electronic commerce (e-commerce) in Internet arose at the end of the 90s as a transforming element of the society in the 21st century. Even though the evolution of the electronic commerce has been important, it has not reached the initial expectations. The lack of tools to support the users' confidence about the new model of commerce through computer networks has been an important problem for its growth. Fortunately, the appearance of technologies and electronic payment systems offer users security and integrity guarantees to carry out electronic transactions. Nevertheless, the lack of confidence keeps being the main barrier (not technical but psychological) to achieve the success of the e-commerce. In this paper, we review the three main secure payment protocols in e-commerce, SSL (Secure Sockets Layer), SET (Secure Electronic Transaction) and 3D Secure, with the aim of removing any doubt about the lack of security in the electronic commercial transactions.

Key words: Electronic commerce**,** security, secure payment. **JEL:** 033

1. INTRODUCCIÓN

A pesar del crecimiento de las cifras económicas relacionadas con el comercio electrónico en los últimos tiempos (Laudon, 2006; Schneider, 2006; Aspatore, 2001), éste no ha cumplido las expectativas que se abrieron en el segundo lustro de los 90. La razón de mayor peso por la que no se han cumplido tales expectativas ha sido la desconfianza e inseguridad que causa en los usuarios la utilización de redes de ordenadores para llevar a cabo transacciones electrónicas a través de Internet, en las que la información que viaja por la red es de carácter personal y susceptible de ser utilizada en contra de los propios usuarios (Tsiakis, 2005). Esta desconfianza se debe principalmente a la falta de formación tecnológica

en general y al desconocimiento de la existencia y funcionamiento de sistemas de pago seguros que facilitan la compra-venta online en particular. Dichos sistemas permiten la realización de transacciones de forma segura mediante la autenticación de los actores y facilitan procesos como la devolución de los productos no satisfactorios. El factor de desconfianza existente en el comercio electrónico está relacionado con los problemas de seguridad propios de las redes de ordenadores como son:

a) *Privacidad:* trata de evitar que la información sea accedida por personas ajenas a la organización o simplemente no autorizadas.
b) *Validación de la identificación (Autenticación o Autentificación):* identifica a la persona con la que se intercambia información antes de realizar dicho intercambio.
c) *Irrefutabilidad* (No Repudio)*:* identifica a los usuarios comprobando sus firmas digitales, es decir, asegura la validez de la firma existente en un documento electrónico.
d) *Control de Integridad:* asegura que la información transmitida a través de una red de comunicación no se modifica a lo largo del trayecto que ha recorrido por el canal.

Además el usuario del comercio electrónico se enfrenta a otros problemas como pueden ser: la incertidumbre que supone la caída del sistema de comunicación por fallos del hardware o del software, o el excesivo tiempo transcurrido en obtener respuestas a sus peticiones. Esto ocasiona que al comprar un producto en Internet, aparezcan mensajes como: "no se ha encontrado la página", o a veces nos quede la duda de si hemos comprado realmente el producto deseado o lo que es peor, si nos cargarán el importe real de la compra en la tarjeta de crédito. Por lo tanto, el éxito de una tienda virtual dependerá entre otras cosas de que ésta transmita sensación de seguridad en sus transacciones comerciales.

Para evitar estos problemas se han desarrollado diferentes herramientas y protocolos de pago seguro que garantizan la seguridad de las transacciones electrónicas y mejoran la confianza de los usuarios en el comercio electrónico. El primer protocolo en desarrollarse fue el SSL (Secure Sockets Layer), al que sucedió la propuesta del SET (Secure Electronic Transactions) que aseguraba la confidencialidad e integridad de los datos de la transacción. Más recientemente se ha propuesto el protocolo 3D Secure que permite verificar que el comprador está autorizado a utilizar la tarjeta de crédito que le proporciona al vendedor.

A lo largo de este trabajo presentaremos los conceptos necesarios para entender los protocolos de pago seguro y presentaremos su funcionamiento con el objetivo de despejar las posibles dudas respecto a problemas de seguridad en los mismos.

2. PRELIMINARES

En esta sección revisamos mecanismos generales que mejoran la seguridad en las redes de ordenadores como son: los sistemas de autenticación y de encriptación. Tales mecanismos se aplicarán posteriormente en el desarrollo de los distintos protocolos de pago en Internet.

Sistemas de autenticación

Este tipo de sistemas son una parte importante del diseño de las políticas de seguridad de cualquier sistema de redes de ordenadores.

La autenticación es el proceso que comprueba y verifica la identidad de la persona que se conecta al sistema. El usuario autenticado puede ser: una persona que usa un ordenador, un ordenador por sí mismo o un programa informático. En una red de ordenadores la

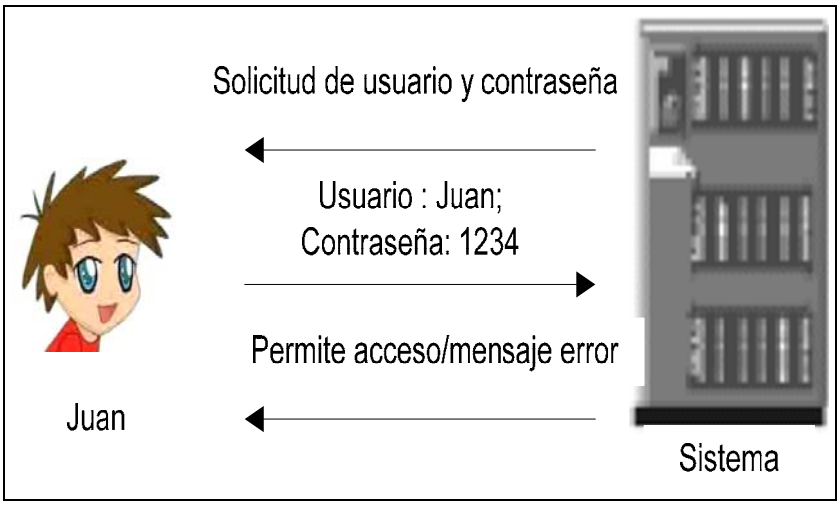
"autenticación" es una forma de asegurar que los usuarios son quienes dicen ser, es decir, que el usuario que intenta operar con el sistema es un usuario autorizado para hacerlo.

Cualquier sistema de autenticación ha de poseer unas determinadas características para ser implantado, como pueden ser: el nivel de fiabilidad, económicamente viable para la organización y capaz de soportar con éxito ataques de seguridad. Aparte de estas características técnicas tenemos también que destacar que un sistema de autenticación ha de ser aceptado por los usuarios sin demasiadas reticencias (Tanenbaum, 2006). Por ejemplo, un sistema que vulnerase o invadiese la intimidad de los usuarios sería inmediatamente rechazado por los mismos.

Los métodos de autenticación se dividen en tres grandes categorías en función de la información y tecnologías que utilizan para verificar la identidad (Wang, 2006; Everett, 1992):

a) Información que el usuario sabe, (*contraseña-password)*. Es el método más básico. Consiste en que cada usuario utiliza una contraseña o palabra clave (que sólo él conoce) para acceder al sistema. El sistema comprueba la validez de la contraseña y si ésta es correcta, permite el acceso del usuario, en caso contrario, mostrará un mensaje de error (gráfico 1).

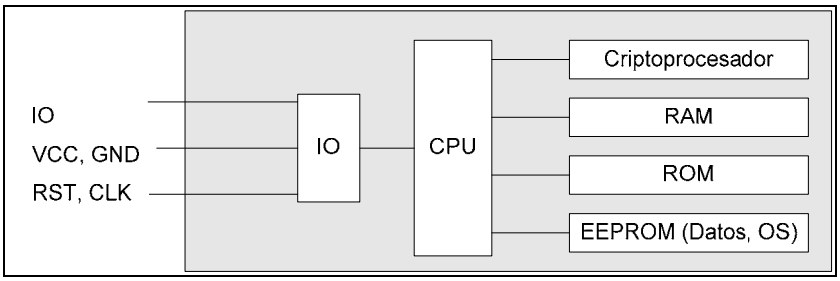
GRÁFICO 1: AUTENTICACIÓN DE CONTRASEÑA-PASSWORD



Fuente: Elaboración propia

b) Elementos que el usuario posee, (*hardware inteligente)*, como puede ser una tarjeta inteligente (o smartcard). Desde un punto de vista formal (Guillou, 1992), una tarjeta inteligente es un dispositivo de seguridad del tamaño de una tarjeta de crédito, que ofrece funciones para un almacenamiento seguro de información y para el procesamiento de la misma. En la práctica, las tarjetas inteligentes poseen un chip empotrado en la propia tarjeta que puede implementar un sistema de ficheros cifrado y funciones criptográficas. Además, puede detectar activamente intentos no válidos de acceso a la información almacenada. Este chip inteligente marca la diferencia respecto a simples tarjetas de crédito que solamente incorporan una banda magnética donde va almacenada cierta información del propietario de la tarjeta (gráfico 2).

GRÁFICO 2: ESTRUCTURA GENÉRICA DE UN SMARTCARD



Fuente: Elaboración propia

Cuando el usuario poseedor de una tarjeta inteligente desea autenticarse, necesita introducir la tarjeta en un hardware lector, los dos dispositivos se identifican entre sí. Tras identificarse las dos partes, se lee la identificación personal (PID) de la tarjeta y el usuario teclea su número de identificación (PIN). Seguidamente se inicia un protocolo en el que la máquina lee el PID y solicita al usuario una clave personal. Si la respuesta es correcta, la tarjeta y usuario son identificados y obtienen acceso al recurso solicitado.

c) Características físicas del usuario, *(autenticación biométrica).* El reconocimiento de patrones, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos.

Aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y medible del individuo (esto incluye desde el reconocimiento del iris o huellas dactilares hasta el olor corporal), tradicionalmente ha estado basada en cinco grandes grupos (Everett, 1992). En el cuadro 1 se muestra una comparativa de sus rasgos más generales (Jain, 2004).

CUADRO 1: COMPARACIÓN DE MÉTODOS BIOMÉTRICOS, (I: IRIS; R: RETINA; D: HUELLAS DACTILARES; G: GEOMETRÍA DE LA MANO; E: ESCRITURA; V: VOZ; MA: MUY ALTA; A: ALTA; M: MEDIA; B: BAJA; S: SI; N: NO)

	I	**R**	**D**	**G**	**E**	**V**
Fiabilidad	Ma	Ma	A	A	A	A
Facilidad de uso	M	B	A	A	A	A
Prevención de ataques	Ma	Ma	A	A	M	M
Aceptación	M	M	M	A	Ma	A
Estabilidad	A	A	A	M	M	M
Identificación	S	S	S	N	S	N
Autenticación	S	S	S	S	S	S

Fuente: Elaboración propia

Los dispositivos biométricos tienen dos partes principales. Por un lado, disponen de un mecanismo automático que lee la característica a analizar y la digitaliza. Por otro lado disponen de un software capaz de almacenar y comparar los datos capturados con los guardados en una base de datos (que son considerados válidos). El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: i) captura o lectura de los rasgos fisiológicos que se pretenden validar, ii) extracción de las características de la muestra (por ejemplo, los rasgos de una huella dactilar), iii) comparación de tales características con las guardadas en una base de datos. El resultado final de este proceso es la identificación o no del usuario en cuestión. Los métodos biométricos más utilizados son:

1. Verificación de voz.
2. Verificación de escritura.
3. Verificación de huellas.
4. Verificación de patrones oculares (analizan la retina o el iris).
5. Verificación de la geometría de la mano.

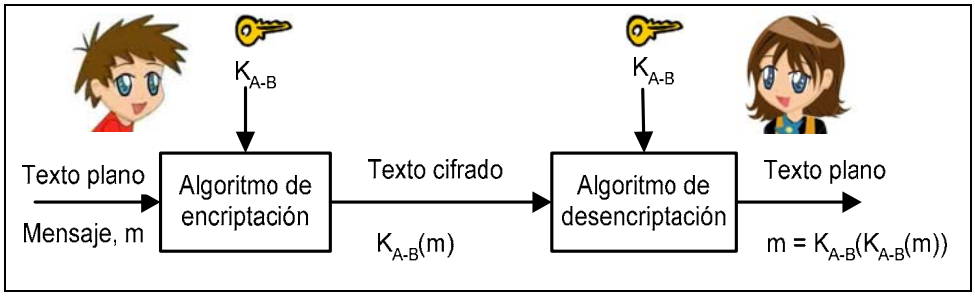
Sistemas de encriptación

La encriptación o codificación (Caballero, 2002) es un proceso que consiste en transformar una información expresada en un lenguaje determinado a otro lenguaje con reglas sintácticas y semánticas distintas, pero que no puede entenderse a no ser que se conozca el proceso que realiza la función inversa, es decir, la desencriptación o descodificación. Este proceso se lleva a cabo mediante un conjunto de fórmulas matemáticas complejas denominados algoritmos de encriptación.

Existen distintos métodos de encriptación o codificación (Chou, 2002; Weaver, 2006):

i. *Encriptación simétrica*. Este tipo de encriptación utiliza un algoritmo para codificar y descodificar la información utilizando una única clave de cifrado (Diffiehellman, 1976). Si alguien codifica un mensaje, sólo otra persona que conozca la clave de cifrado podrá descifrarlo (gráfico 3). El tamaño de la clave es la característica crítica de los sistemas de encriptación simétricos, dicho tamaño se cuenta en bits (e.g, 64, 128, 256 bits).

GRÁFICO 3: CRIPTOGRAFÍA DE CLAVE SIMÉTRICA



Fuente: Elaboración propia

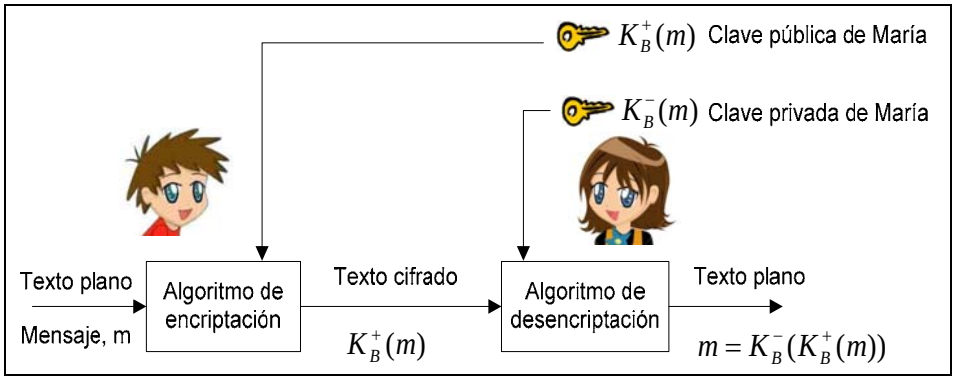
En un método basado en encriptación simétrica existen varios aspectos a tener en cuenta como son, la complejidad del algoritmo de encriptación así como el mecanismo utilizado por los usuarios para intercambiar dicho algoritmo (canales de comunicación inseguros).

El sistema DES (Estándar de Encriptación de Datos) es el sistema más usual de encriptación simétrica. Posee una clave de entrada con una longitud de 64 bits, lo que significa que es posible aunque costoso deducir la clave de codificación mediante un ataque de fuerza bruta[1]. Vemos que, es posible obtener la clave del sistema DES, por lo que podría no ser apropiado para encriptar información que consideremos de alta seguridad.

ii. *Encriptación asimétrica*. Es un método de encriptación basado en un par de claves complementarias y relacionadas entre sí: una clave pública y una clave privada. Cada parte de la comunicación (emisor, receptor) tiene sus propias claves, una pública y otra privada. La clave pública está disponible libremente mientras que la clave privada debe ser conocida únicamente por el usuario propietario. Cada clave abre el código que produce su complementaria. La clave pública debe hacerse accesible a aquellos usuarios con quien se desee comunicarse de forma segura. Esta transferencia puede hacerse a través de canales no seguros o estar disponible en algún servidor de acceso público.

El funcionamiento del cifrado es el siguiente: supongamos una comunicación entre los usuarios ***A*** y ***B***, de forma que ***A*** va enviar a ***B*** un mensaje seguro utilizando codificación asimétrica. ***A*** encriptará el mensaje para ***B*** utilizando la clave pública de ***B*** que éste le transfirió o encontró en un servidor público que contiene este tipo de información. Sólo ***B*** puede desencriptar el mensaje con su clave privada ya que es el único que la conoce (gráfico 4).

GRÁFICO 4: CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA



Fuente: Elaboración propia

Autenticación y Encriptación en los problemas de seguridad en las redes

El uso de los sistemas de autenticación y encriptación pueden ayudar a aliviar los problemas de seguridad en las redes de ordenadores tal y como vemos a continuación:

Privacidad: en esta área se utilizan los sistemas de autenticación para controlar el acceso al sistema y la encriptación simétrica para guardar las palabras clave de los distintos usuarios de la red.

Validación de la identificación: pueden utilizarse tanto sistemas de encriptación simétricos como asimétricos para constatar la identidad de un interlocutor, aunque siempre son más seguros los sistemas asimétricos.

[1] Forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Irrefutabilidad (No Repudio): para garantizar la autenticidad de las firmas electrónicas se utiliza la encriptación asimétrica de forma que el emisor firma un mensaje utilizando su clave privada. El receptor del mensaje debe conocer la clave pública del emisor. Si la firma es correcta el receptor descifrará la firma con la clave pública del emisor.

Integridad de la información: para asegurar la integridad de los mensajes no es suficiente con la encriptación asimétrica, ya que un intermediario podría interceptar el mensaje, conseguir la clave pública del receptor y crear un nuevo mensaje con el mismo nombre que el mensaje original. En este caso, el receptor desencripta el mensaje utilizando su clave privada y no le es posible saber que el mensaje no es el original. Para resolver este problema se utilizan las denominadas funciones MAC (Message Authentication Codes) y MDC (Modification Detection Codes) [ISO 9731, rfc2104]. Los MDC aplican una función hash[2] que se envía con el propio mensaje, de forma que al recibirlo el receptor aplica la función hash al mensaje y comprueba que sea igual al hash que se envió antes.

3. SEGURIDAD Y SISTEMAS DE PAGO

Una vez introducidos los principales conceptos y herramientas para mejorar la seguridad en las redes de ordenadores, en esta sección revisamos su aplicación a protocolos de pago en Internet (cuadro 2) desarrollados para realizar transacciones de comercio electrónico de forma segura. Presentaremos sus funcionalidades, ventajas y desventajas con el propósito de hacer ver que el uso de estas herramientas facilita la realización de transacciones de comercio electrónico de forma al menos, tan simple y segura como en el comercio tradicional.

CUADRO 2: COMPARACIÓN DE LOS TRES PROTOCOLOS

	SSL	SET	3D SECURE
Confidencialidad	X	X	X
Integridad	X	X	X
Autentifica los titulares de las tarjetas de crédito	X	X	X
Autentifica los comerciantes	X	X	X
Autentifica los bancos		X	X
Verifica que el comprador está autorizado a utilizar la tarjeta de crédito que le proporciona al vendedor			X

Fuente: Elaboración propia

[2] Es una función o método para generar un resumen que representen de manera casi unívoca a un documento, registro, archivo.

SSL (Secure Sockets Layer)

Es el protocolo de seguridad más extendido en la Red (Chou, 2002; Freier, 1996; Rescorla, 2000; Viega, 2002). Se trata de una tecnología diseñada por Netscape Communications Inc. con el propósito de conseguir un sistema de intercambio de información seguro tanto en el transporte de la información como en la autenticación del servidor de comercio electrónico. El protocolo SSL combina sistemas de encriptación simétrica con sistemas de encriptación asimétrica.

El intercambio de información tiene lugar en dos fases: (i) se negocia entre el cliente y el servidor una clave simétrica sólo válida para esa sesión, (ii) se transfieren los datos cifrados con dicha clave. Estas fases son transparentes para los usuarios finales que sólo saben que el canal de transmisión de la información es seguro y proporciona confidencialidad entre los extremos, haciéndolo simple de usar. Veamos en mayor detalle las fases del protocolo:

i. El sistema se basa en la utilización de un mecanismo de claves públicas. Así, los navegadores incluyen a priori las claves públicas de ciertos "notarios electrónicos" o Entidades Certificadoras Autorizadas (ECA). De esta forma, el cliente contacta con el servidor seguro y éste le envía su clave pública rubricada por la ECA. La identificación se completa para que el cliente sepa que al otro lado está quien dice ser.

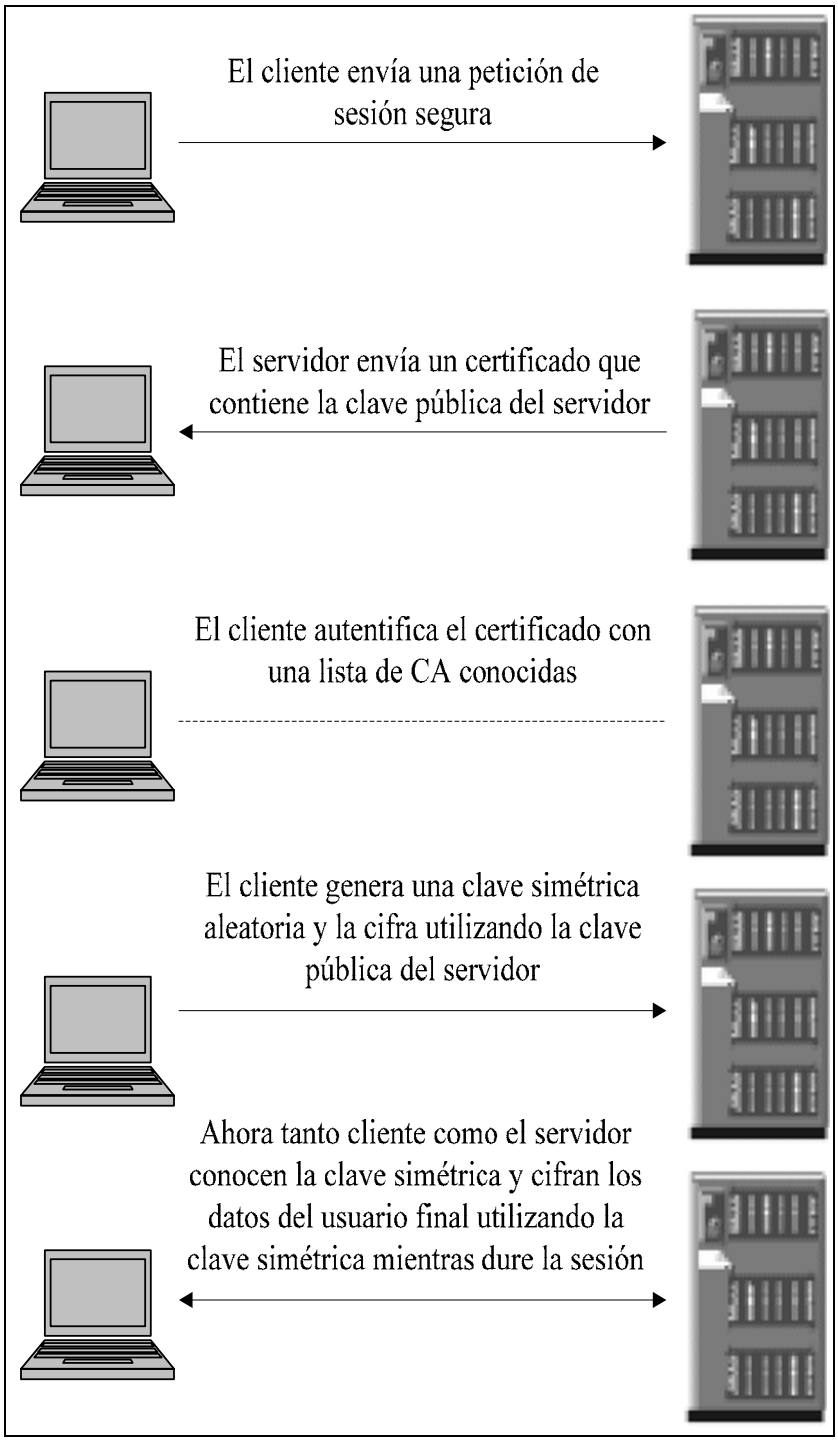
ii. Verificada la identidad del servidor, el cliente genera una clave de sesión y la envía cifrada con la clave pública del servidor. Conociendo ambos la clave simétrica de sesión, se intercambian los datos cifrados por el algoritmo de clave simétrica (gráfico 5).

Las versiones 1 y 2 del protocolo SSL sólo proporcionaban autenticación de servidor y usaban claves simétricas de 40-bits como máximo. Esta limitación de longitud, se dio solamente en EE.UU debido a intereses de su gobierno que imponía restricciones sobre la exportación de tecnología criptográfica, ya que en realidad, el protocolo soportaba longitudes mayores de claves (128-bits). Estas versiones presentaban algunas debilidades por lo que Netscape continuó trabajando y desarrolló la versión 3 (Chou, 2002; Freier, 1996). Esta versión soluciona los problemas de las anteriores versiones y agrega la autenticación del cliente, utilizando los certificados digitales de cliente y de servidor. Además utiliza claves simétricas de 128-bits (o más) (cuadro 3).

Para la mayoría de las transacciones, este protocolo es válido, práctico y fácil de implantar además de asegurar las transacciones de una forma similar al comercio tradicional. Sin embargo, SSL deja de lado ciertos aspectos como para ser considerado una solución definitiva:

- 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 no tenga saldo.

GRÁFICO 5: FUNCIONAMIENTO DEL PROTOCOLO SSL



Fuente: Elaboración propia

CUADRO 3: CARACTERÍSTICAS DE LAS VERSIONES DE SSL, (V1: VERSIÓN 1; V2: VERSIÓN 2; V3: VERSIÓN 3)

	V1	V2	V3
Confidencialidad	X	X	X
Integridad	X	X	X
Autenticación del cliente			X
Autenticación del servidor	X	X	X
Clave simétrica (bit)	128	128	128 ó más

Fuente: Elaboración propia

SET (Secure Electronic Transaction)

Como complemento al protocolo SSL, Mastercard y Visa desarrollaron SEPP (Secure Electronic Payment Protocol) y STT (Secure Transaction Technology) para asegurar las transacciones económicas exclusivamente utilizando tarjetas de crédito como medio de pago, aunque más tarde ambas entidades, junto con American Express, convinieron en aunar esfuerzos para elaborar un único protocolo para el pago electrónico con tarjetas, denominado SET (Drew, 1999; Agnew, 2003; Merkow, 1998).

El protocolo SET (Transacción Electrónica Segura) es un conjunto de normas o especificaciones de seguridad que constituyen una forma estándar para la realización de transacciones de pago a través de Internet.

Este protocolo fue desarrollado para:

- Proteger el sistema de tarjetas de crédito cuando es utilizado a través de Internet.
- Generar en la mente del consumidor una opinión de confianza respecto al nuevo concepto de Internet como mercado.
- Generar nuevos tipos de transacciones financieras seguras.

Se basa en el uso de una firma electrónica del comprador y una transacción que involucra, no sólo al comprador y al vendedor, sino también a sus respectivos bancos.

Cuando se realiza una transacción segura por medio de SET, los datos del cliente son enviados al servidor del vendedor, pero dicho vendedor sólo recibe la orden. Los números de la tarjeta del banco se envían directamente al banco del vendedor, quien podrá leer los detalles de la cuenta bancaria del comprador y contactar con su banco para verificarlos en tiempo real (gráfico 6).

El uso del protocolo SET aporta una serie de beneficios de carácter inmediato:

- Autentica los titulares de las tarjetas de crédito, los comerciantes y los bancos que intervienen en las operaciones comerciales por Internet.
- Garantiza la máxima confidencialidad de la información del pago.

- Asegura que los mensajes financieros no serán manipulados dentro del circuito del proceso de pago.
- Proporciona interoperatividad entre distintas plataformas hardware y software.

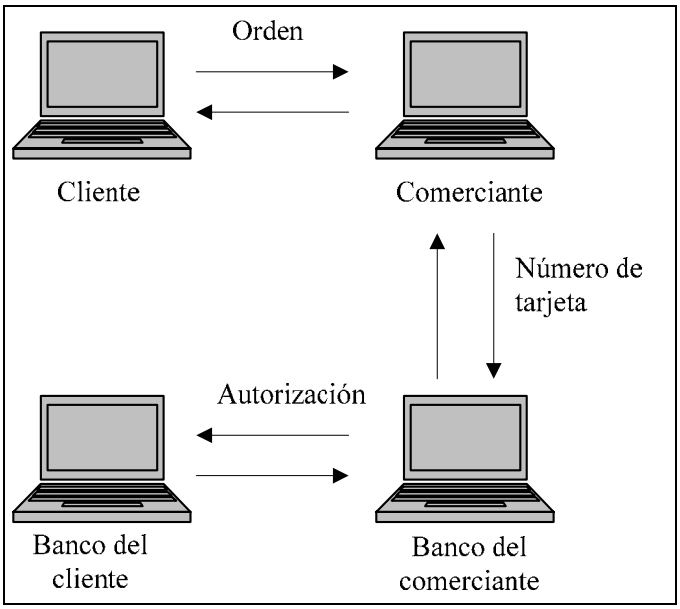
Con ello, el nuevo protocolo evita:

- El pago de compras mediante tarjetas de crédito no autorizadas.
- El robo de información financiera del comprador.

Las ventajas que aporta el protocolo SET son:

- Los compradores, los comerciantes, los intermediarios financieros y los bancos tendrán la confianza de saber que cada transacción está protegida por un protocolo de validación aceptado.
- La principal aportación del protocolo SET es la garantía de la confidencialidad y la no manipulación de la información financiera personal.

GRÁFICO 6: FUNCIONAMIENTO DEL PROTOCOLO SET



Fuente: Elaboración propia

Sin embargo, SET no goza de la popularidad de SSL y no termina de implantarse. Esto se debe, en primer lugar, a que su despliegue es muy lento y exige software especial, tanto para el comprador como para el comerciante. En segundo lugar, aunque varios productos cumplan con el estándar SET, esto no significa necesariamente que sean compatibles.

3D SECURE (3 Domain Secure)

El tercer protocolo, denominado 3D Secure o 3 Domain Secure, ha sido desarrollado por Visa para verificar que el comprador está autorizado a utilizar la tarjeta de crédito que le proporciona al vendedor y proveer mayor seguridad a las transacciones de comercio electrónico. Su nombre comercial es *Verified by Visa*.

Este protocolo trabaja utilizando seguridad en 3 dominios:

- Dominio Emisor: emisor o entidad financiera que emite la tarjeta de crédito. Los emisores participantes en Verified by Visa deben tener un servidor que atienda las solicitudes de autenticación de pago.
- Dominio Adquirente: comercios virtuales y físicos junto a sus respectivas entidades financieras que se encargarán de solicitar los pagos al dominio emisor a través del dominio de interoperabilidad.
- Dominio de Interoperabilidad: dispone de toda la infraestructura necesaria para permitir las transacciones electrónicas entre el dominio emisor y el dominio adquirente. Este dominio es administrado directamente por Visa Internacional.

Su funcionamiento es bastante sencillo. 3-D Secure solicita al usuario una contraseña que éste previamente habrá tramitado con su banco emisor. Si la clave es correcta y la tarjeta tiene crédito disponible, el sistema autoriza el cierre de la compra. Para garantizar la integridad de los mensajes intercambiados entre todos los involucrados en la transacción (Comprador, Vendedor, Banco Emisor, Banco del Vendedor) 3-D Secure se apoya en el protocolo SSL.

Veamos con más detalle los pasos que ocurren en toda autenticación de pagos utilizando el protocolo 3-D Secure (gráfico 7):

- El tarjetahabiente selecciona los productos y servicios a comprar y hace clic en el botón comprar.
- El comercio a través del *Merchant Plug-in*[3] *(MPI)*[4] *Server* envía esta petición al *Directorio de Visa* para verificar que el comercio que hizo la petición de autenticación es un comercio válido para VISA y participa en Verified by Visa. Además de esto, el *Directorio de Visa* verifica que el número de la tarjeta de crédito se encuentra entre el rango de tarjetas participantes en Verified by VISA. Seguidamente el *Directorio de Visa* consulta al *Control de Acceso* del banco correspondiente la participación de la tarjeta de crédito en Verified by Visa y envía esta respuesta al *MPI Server*.
- El *MPI Server* envía un pedido de autenticación al *Control de Acceso* haciendo uso del navegador web del tarjetahabiente.
- El *Control de Acceso* del banco emisor de la tarjeta de crédito, solicita la clave de autenticación del tarjetahabiente y valida que esta tarjeta sea la correcta.
- El *Control de Acceso* responde al pedido de autenticación que le hizo el *MPI Server* a través del navegador web del tarjetahabiente.
- El *MPI Server* recibe y valida la respuesta del *Control de Acceso*.
- Una vez culminado el proceso de autenticación de pagos se procede con el habitual proceso de autorización de pagos.

Este protocolo evita el uso fraudulento de las tarjetas de crédito a través de Internet, el cual puede generar grandes pérdidas a los comerciantes y molestias a los usuarios cuyas tarjetas son utilizadas de forma ilegítima.

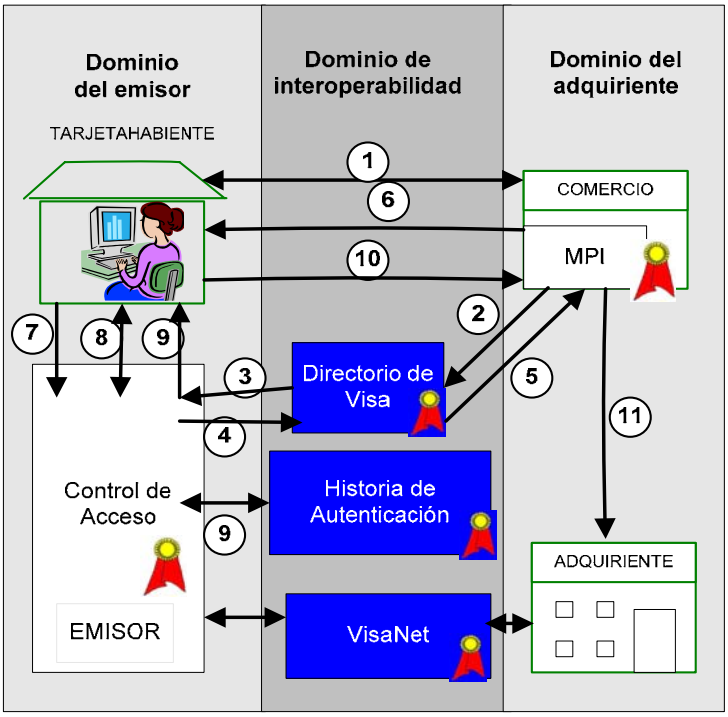
[3] Un plug-in es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy especifica.

[4] Un MPI es un módulo software diseñado para facilitar las verificaciones del protocolo 3D-Secure para prevenir fraudes con tarjetas de crédito

Adoptar 3-D Secure es fácil y sencillo para comerciantes y compradores. Los vendedores no tienen que modificar sus aplicaciones de venta, sólo instalar un plug-in en sus servidores de comercio electrónico y adquirir un certificado que les identifica como tienda confiable. Por su parte, los usuarios compradores no tienen la necesidad de instalar ningún software ni adquirir dispositivo alguno para disfrutar de las ventajas de 3-D Secure. Sólo deben tramitar su contraseña con el banco emisor de su tarjeta de crédito Visa que utilizan normalmente en cualquier mercado tradicional. Sin embargo, este protocolo no es totalmente infalible, ya que han aparecido algunas críticas respecto a su implantación. Una de ellas es la dificultad que encuentran los usuarios para distinguir entre una ventana emergente legítima de Verified by Visa y una fraudulenta de phising[5].

Las especificaciones actuales se encuentran en la versión 1.0.2, la cual también ha sido aceptada por MasterCard y JCB.

GRÁFICO 7: FUNCIONAMIENTO DEL PROTOCOLO 3D-SECURE



Fuente: Elaboración propia

4. CONCLUSIONES

En este trabajo se pretende dar una visión a los usuarios de comercio electrónico de las diversas herramientas existentes para llevar a cabo transacciones electrónicas de forma segura, con el objetivo de incrementar su confianza en este tipo de transacciones comerciales. Para ello hemos revisado los principales mecanismos utilizados para abordar los problemas de seguridad en las redes de ordenadores como son: los sistemas de autenticación y de encriptación de información. Posteriormente hemos presentado el funcionamiento, ventajas y problemas de los tres protocolos de pago electrónico más extendidos en la actualidad como

[5] Es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito,… Para después ser usados de forma fraudulenta.

son el SSL, el SET y el 3D Secure. Para así, mostrar que se pueden realizar transacciones electrónicas de forma al menos tan segura en Internet como en el comercio tradicional.

5. BIBLIOGRAFÍA

Agnew (2003): "Secure electronic transactions: Overview, capabilities and current status", *Payment Technologies for e-commerce,* Springer-Verlag, Berlin, pp. 211-226.

Aspatore, J.R. (2001): *Al Día en Comercio Electrónico,* MC Graw-Hill.

Caballero, P. (2002): *Introducción a la Criptografía,* 2ª Edición, Ra-Ma Editorial, Madrid.

Chou, W. (2002): "Inside SSL: the secure sockets layer protocol", *IEEE Computer Society,* vol. 4, p. 4, pp. 47-52.

Diffie, W. y Hellman, M. E. (1976): "New directions in cryptography", *IEEE Transactions on Information Theory,* IT-22, pp. 644-654.

Drew, G. N. (1999): *Using Set for Secure Electronic Commerce,* Prentice Hall, NJ.

Everett, D. (1992): "Identity verification and biometrics", In Keith M. Jackson and Jan Hruska, editors, *Computer Security Reference Book,* Butterworth- Heinemann.

Freier, A. O., Karlton, P. y Kocher, P. C. (1996): "The SSL protocol v3.0", *Internet Draft*.

Guillou, L.C., Ugon, M. y Quisquater, J.Q. (1992): "The smart card, a standardized security device dedicated to public cryptology", *Contemporary Cryptology- The Science of Information Integrity*, IEEE Press, pp. 561-614.

ISO 9731-1,2 (1987, 1992): "Banking – Approved algorithms for message authentication".

Jain, A.K., Ross, A. y Prabhakar, S. (2004): "An introduction to biometric recognition". *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, nº 1, pp. 4-20.

Laudon, K. y Traver, C. (2006): *E-Commerce: Business, Technology, Society,* 3ª Edición, Prentice-Hall, Inc.

Merkow, M.S. y Breithaupt, J. (1998): *Building SET Applications for Secure Transaction,* John Wiley & Sons.

Rescorla, *E.*, (2000): *SSL and TL. Designing and Building Secure Systems*, Addison-Wesley.

RFC 2104 (1997): "HMAC: keyed-Hashing for Message Authentication", Internet Request for Comments.

Schneider, G. (2006): *Commerce electronic,* 6ª Edición, Thomson Course Technology.

Tsiakis, T. y Sthephanides, G. (2005): "The concept of security and trust in electronic payments**"** *Computers & Security,* vol. 24, nº 1, pp. 10-15.

Tanenbaum. A. y Woodhull A. (2006): *Operating Systems: Design and Implementation*. 3ª Edición, Prentice Hall.

Viega, J., Messier, M. y Chandra, P. (2002): *Network Security with OpenSSL, Cryptography for Secure Communications.* O'Really.

Wang, J. (2006): *Computer Network Security: Theory and Practice,* Higher Education Press. Beijing.

Weaver, A.C. (2006): "Secure Sockets Layer", *IEEE Computer Society,* vol. 39, nº 4, pp. 88-90.