

PROTOCOLO SET (SECURE ELECTRONIC TRANSACTION)

El protocolo SET (Transacción Electrónica Segura) está diseñado con el propósito de asegurar y otorgar autenticidad a la identidad de los participantes en las compras abonadas con tarjetas de crédito en cualquier tipo de red en línea.

Los objetivos que cumple SET son:

- Confidencialidad de la información transmitida.
- Autenticación de los titulares y comercios.
- Integridad de la información transmitida.
- No repudio de las operaciones realizadas.

Los certificados SET son el soporte electrónico mediante el cual se genera la firma digital y el encriptado de la información de acuerdo con el protocolo SET. Cada uno de los participantes en la transacción comercial electrónica debe disponer de su certificado SET.

PROTOCOLO SSL (Secure Sockets Layer)

El protocolo SSL proporciona seguridad mediante el cifrado del canal de comunicación establecido entre el consumidor y el comercio. Asimismo, el certificado de servidor permite garantizar la autenticidad del servidor frente a los posibles compradores. Sin embargo, el comercio no puede realizar la identificación de la persona que quiere realizar la compra salvo que éste sea titular de un certificado. Por otra parte, el pago no se realiza de una forma automática, sino que el titular tiene que introducir todos los datos personales y de tarjeta de crédito en una plantilla y enviarla a través de la comunicación segura establecida mediante SSL. Este proceso deberá repetirse cada vez que se quiera realizar una compra a no ser que el web disponga de alguna tecnología tipo "carro de compra". Para verificar si un comercio está utilizando SSL basta con comprobar la URL del comercio y ver que en vez de "http" aparece "https".

Este sistema plantea dos inconvenientes adicionales:

- Sólo pueden realizarse transacciones punto a punto: SSL únicamente maneja interacciones punto a punto mientras que las transacciones con tarjeta de crédito involucran como mínimo a tres partes: el titular, el comerciante y el Banco o Caja emisor de la tarjeta.
- Con SSL los datos de la tarjeta de crédito del cliente se mantienen en el servidor del comercio por lo que son vulnerables a un ataque externo. Por otra parte, los comerciantes no tienen asegurada la veracidad de los datos de la tarjeta enviados por el cliente.