1.1.2.Set.

Set (*Secure Electronic Transaction*) fue creado por Visa y MasterCard con la participación de IBM, Microsoft, Verisign, RSA, Netscape y otras empresas tecnológicas. Su intención fue presentar unas especificaciones que asegurarán y autenticarán la identidad de aquellos que utilizan tarjetas de crédito/débito en sus compras. Así SET asegura la integridad de los datos emitidos, autentifica a los compradores y vendedores, la confidencialidad de los datos suministrados y el no repudio de las operaciones realizadas.

En una transacción SET pueden definirse las distintas partes intervinientes: *titular* (*Cardholder*) , que es el cliente para el que se ha emitido la tarjeta de crédito/débito; *emisor*, es la entidad financiera emisora de la tarjeta; *comercio* (*Merchant*) es el que ofrece sus productos o servicios y acepta los pagos a través de una entidad financiera (adquiriente); el *adquiriente*, que es una entidad que contiene la cuenta bancaria del comercio y procesa las autorizaciones del pago con la tarjeta; la *pasarela de pagos*, que es un mecanismo mediante el cual se autorizan las transacciones del comercio pudiendo pertenecer al propio adquiriente o a otro operador de medios de pago que procese las transacciones de un conjunto de entidades.

Toda la información que se transmite a través de la red debe codificarse para evitar que sea leída o manipulada por el camino. El procedimiento a usar es la encriptación , mediante la cual un algoritmo matemático genera un nuevo mensaje ilegible salvo con unas claves que van a poseer tanto el cliente como el vendedor. La clave usada tradicionalmente era la llamada “Clave Simétrica” en donde emisor y receptor del mensaje se ponen de acuerdo en qué algoritmo usar para cifrar el mensaje, pero para el tema que nos ocupa (comercio con multitud de clientes), esto no es posible , ya que el vendedor tendría que negociar una clave distinta con cada cliente que tuviese, lo cual sería operativamente muy costoso. De esta forma aparece la “Clave Pública” o “Clave Asimétrica” que incorpora un par de claves para el emisor (pública y privada) y otro par para el receptor. Mientras que todas las claves públicas deben aparecer en un sitio accesible para cualquiera, y poder realizar comunicaciones cifradas; la clave privada no puede ser leída salvo por el propio propietario manteniéndose en el propio sistema informático del mismo.

La criptología de clave pública puede ser utilizada tanto para la encriptación del mensaje consiguiéndose la confidencialidad del mismo, como para autenticación con la “Firma electrónica” (de la que se hablará después).

1.1.2.1.Certificados Set.

Cada participante en la transacción comercial debe poseer su certificado SET mediante el cual se genera su firma digital y el cifrado del mensaje que realice. Distinguimos varios certificados en el proceso:

- Certificado del titular. Es la representación electrónica de la tarjeta de crédito/débito y solo pueden ser emitidos a propuesta de una entidad financiera. En él aparece el número de la tarjeta y la caducidad de la misma, de una forma codificada. Este certificado será enviado al comercio junto con el mensaje que contiene el formulario de compra, que ha sido codificada mediante sotfware (llamado "*Electronic Wallet*") integrado en el navegador de Internet del titular.

- Certificado del comercio. Da prueba de que el comercio mantiene unas relaciones con una entidad financiera concreta que permite el pago mediante tarjeta. Este certificado debe ser aprobado por la entidad "adquiriente", y el comercio deberá tener tantos certificados como numero de marcas de tarjeta (VISA, MasterCard ...) acepte. El *software* que posee el comercio gestiona los certificados del comercio y todos los procesos de

encriptación, manejo de claves públicas y privadas, y las comunicaciones con la pasarela de pagos.

- Certificado de la pasarela de pagos (*Payment Gateway*). Son emitidos a los adquirientes o sus procesadores de transacciones y se aplican a los sistemas que procesan las autorizaciones y los mensaje. La clave de encriptación de la pasarela, recogida en la clave del titular, es utilizada para proteger la información sobre la tarjeta del mismo.

Todos estos certificados se basan en una jerarquía de certificación, esto es, cada entidad certificadora es a su vez certificada por otra de superior jerarquía. La clave raíz es distribuida a través de un certificado que es autofirmado. Esta clave va incluida en el sotfware distribuido por los proveedores de SET.

En España se crea en 1997 la Agencia de Certificación Electrónica (ACE) que es quién está encargada del procesamiento de las solicitudes de emisión de certificados de titular, comercio y pasarela de pagos realizadas por las entidades financieras y de la emisión de las mismas. Los certificados tienen validez anual y son renovables.

Una vez presentadas las premisas, vamos a describir la operativa del comercio electrónico bajo SET:

1- El primer paso se da cuando el cliente conecta con la página web del vendedor mediante su navegador de Internet y selecciona un producto o servicio.

2- El cliente rellena el formulario que aparece en la página web indicando el medio de pago (tarjeta, contra reembolso...). Si selecciona el pago por tarjeta utilizando SET abrirá su Wallet (cartera electrónica) y seleccionará el certificado necesario según la marca de la tarjeta que van a utilizar.

3- Se produce una comunicación entre el navegador y el comercio intercambiándose certificados SET. El cliente mediante su Wallet envía dos sobres con información de su certificado, el pedido y una orden de pago firmados, y el *software* del comercio verifica la validez del certificado del titular y el pedido.

4- El comercio envía a la pasarela de pagos los datos de la transacción y el sobre encriptado con los datos de la tarjeta del titular.

5- La pasarela de pagos verifica los certificados de cliente y vendedor, sus firmas, descifra los datos de la tarjeta del cliente y la autorización enviada por el comercio vendedor. La pasarela de pagos procesa la petición de autorización al Medio de Pago. El Medio de Pago autoriza los pagos y manda un mensaje que contiene el número de autorización SET a la pasarela de pagos.

6- La pasarela de pagos envía el número de autorización al vendedor.

7- El vendedor envía sus productos al cliente o realiza los servicios demandados por el mismo.

8- El Medio de Pago realiza el cargo a la entidad emisora y el abono a la entidad adquiriente.

1.1.3.Firma electrónica.

Según el Real Decreto-Ley 14/1999 de 17 de Septiembre sobre firma electrónica, se define *firma electrónica* como: " Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados

funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge". Igualmente define *firma electrónica avanzada* como*: "* Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos". De esta forma pueden ser firmados cuantos tipos de documentos se quiera, salvo aquellos que estén sujetos a formas expresamente especificadas, como ocurre con licencias, licitaciones públicas, y otros en donde un notario no solo acredita la identidad de los contratantes, sino que también enjuicia su capacidad para realizar el contrato u obligación que se contrae.

La importancia del decreto anterior reside en que establece que la *firma electrónica avanzada* mantiene con el documento electrónico el mismo valor jurídico que la firma manuscrita con los consignatarios en papel, con lo que es una prueba válida para presentar en el caso de tener la necesidad de litigar en un juicio, y existe una presunción legal favorable cuando el Prestador de Servicios de Certificación que la ha proporcionado, está debidamente acreditado y el dispositivo de creación de la firma está certificado oficialmente. Para la firma electrónica normal, lo que se asegura es que no será rechazada su admisión previa.

La firma digital sería el procedimiento mediante el cual el comercio sabe que el titular es un usuario legítimo de la tarjeta que usa, autenticándolo de esta manera, pero a su vez, el cliente necesita confirmar que el comercio mantiene realmente una relación con una entidad financiera que acepta tarjetas de crédito/débito y poder autenticar al propio comercio. Así aparecen las “Autoridades de Certificación” que actúan como notarios que dan fe de que la empresa es quien dice ser. Con estas premisas, la autenticación en un entorno electrónico es un proceso en el cual el receptor de un mensaje puede estar seguro de la identidad del emisor y de la integridad del mensaje.

Específicamente la firma digital consta de una cadena de datos que van a probar que el mensaje corresponde a la persona que lo escribió y que su contenido no ha sido alterado en el camino recorrido hasta su destinatario. Además, la firma digital no puede ser repudiada, con lo que el firmante no puede alegar que el mensaje ha sido manipulado y que los datos enviados no son los que el proporcionó.

1.1.4. Autoridades de certificación.

La Autoridades de certificación (AC) son unas empresas, de carácter público o privado, o personas físicas o jurídicas que certifican

que el que firma un documento electrónico es realmente quien dice ser, por haber generado la AC sus claves pública y privada.

La AC debe estar debidamente acreditada ante la Administración, habiéndose comprobado técnicamente los procedimientos de generación de claves, la calidad y seguridad de la tecnología que emplea. Así se incluirá en el Registro de Prestadores de Certificación del Ministerio de Justicia con acceso público, siendo permanentemente actualizadas las condiciones y eficacia de la certificación.

Estas autoridades responden civilmente por daños y perjuicios que acarreen a sus usuarios o a terceros por negligencia en el mantenimiento y actualización de las condiciones del certificado que otorga, especialmente en el caso de extinción del mismo.