



SEGURIDAD EN COMERCIO ELECTRÓNICO

Manuel Pons Martorell
Departament de Telecomunicacions
Escola Universitària Politècnica de Mataró



Índice

1.	INTRODUCCIÓN AL COMERCIO ELECTRÓNICO.....	4
1.1.	ARQUITECTURA.....	4
1.2.	REQUISITOS DEL COMERCIO ELECTRÓNICO	5
1.3.	DINERO ELECTRÓNICO	6
1.4.	SISTEMAS DE CRÉDITO Y DÉBITO	6
1.5.	TARJETAS DE CRÉDITO O DÉBITO.....	6
1.6.	SISTEMAS DE MICROPAGOS	7
2.	SSL (SECURE SOCKETS LAYER) Y TLS (TRANSPORT LAYER SECURITY)	9
2.1.	CARACTERÍSTICAS DEL SSL.....	9
2.2.	PROTOCOLO SSL.....	10
2.3.	PROTOCOLO DE REGISTRO EN SSL	11
2.4.	PROTOCOLO HANDSHAKE EN SSL.....	12
2.5.	PROTOCOLO TLS.....	14
3.	SET (SECURE ELECTRONIC TRANSACTION)	15
3.1.	CARACTERÍSTICAS	15
3.2.	AGENTES DEL COMERCIO ELECTRÓNICO DE SET.....	15
3.3.	MÓDULOS DE PROGRAMACIÓN	16
3.4.	FIRMA DUAL	16
3.5.	TRANSACCIÓN DE COMPRA.....	20



Índice de figuras

Figura 1.6.1: Arquitectura de un sistema de micropagos	7
Figura 2.1.1: Situación de SSL en la pila TCP/IP	9
Figura 2.2.1: Protocolos de SSL	10
Figura 2.3.1: Protocolo de registro de SSL.....	11
Figura 2.3.2: Integridad en el protocolo de registro de SSL.....	12
Figura 2.4.1: Protocolo Handshake de SSL.....	13
Figura 3.2.1: Agentes del SET	16
Figura 3.4.1: Firma dual en SET	17
Figura 3.4.2: Tratamiento de los mensajes PI y OI en SET.....	20
Figura 3.5.1: Transacción de compra en SET	22



1. Introducción al comercio electrónico

1.1. Arquitectura

El comercio electrónico abarca todos los conceptos relacionados con procesos de mercado entre entidades físicas o jurídicas a través de redes telemáticas. Por los tipos de usuarios se pueden diferenciar dos grandes grupos:

- **Comercio entre empresas.** Se caracteriza por tener un segmento de clientes posibles limitado, así permite utilizar tecnologías que no necesariamente han de ser estándares al alcance de cualquiera.
- **Comercio entre empresas y usuarios domésticos anónimos.** El segmento de clientes es toda la red, en la mayoría de casos Internet, y únicamente está limitado geográficamente por los servicios de transporte del producto. Es conveniente utilizar sistemas estándares y muy extendidos.

Como en todas las transacciones, en el comercio electrónico intervienen varios agentes que se deben comunicar. Los **agentes mínimos** en un sistema de comercio electrónico son:

- **Comprador.** Adquiere el producto o servicio.
- **Comerciante.** Vende el producto o servicio.
- **Entidades y servicios financieros.** Autorizan los pagos y realizan los movimientos de dinero entre comprador y comerciante.

Además las **entidades y servicios financieros** pueden ser diversos en la misma transacción:

- **Banco del comprador.**
- **Banco del vendedor.**
- **Pasarela entre bancos.**
- **Marca de la tarjeta de crédito o débito si se utiliza.**
- **Broker para micropagos.**

También puede haber entidades implicadas en la seguridad como una **autoridad de certificación**, o en la logística como las **empresas de transportes**.

Todos los agentes de la transacción han de estar comunicados mediante la red o físicamente, aunque un sistema ideal sólo utilizaría la red. Dependiendo del medio de pago y del sistema de seguridad se utilizarán unos agentes o otros.

Una transacción siempre se realiza con estas cuatro fases:

1. El comprador obtiene los datos del producto o servicio del vendedor.
2. Se solicita la autorización de pago del comprador.
3. Se confirma la autorización y se paga al vendedor (en algunos sistemas el pago puede realizarse después de la cuarta fase).
4. Se entrega el producto o servicio mediante un transporte físico o por la red.



Existen diversas **formas de pago** en el comercio electrónico que se pueden agrupar en cuatro familias:

- **Dinero electrónico.**
- **Sistemas de crédito y débito.**
- **Tarjetas de crédito y débito.**
- **Sistemas de micropagos.**

Los **protocolos de seguridad** más utilizados actualmente son:

- **SSL/TLS.** Es un protocolo de seguridad para cualquier aplicación de Internet y, por lo tanto, se puede utilizar en el comercio electrónico. Está muy extendido y actualmente todos los navegadores comerciales lo implementan (Ver capítulo 2).
- **SET.** Es un protocolo especialmente diseñado para el comercio electrónico con tarjetas de crédito. Actualmente se encuentra en su fase de desarrollo (Ver capítulo 3).

Un caso particular del comercio electrónico es cuando la cantidad a pagar es más pequeña que los costes de transacción, en estos casos se deben utilizar sistemas especiales denominados de **micropagos**.

1.2. Requisitos del comercio electrónico

El **principal requisito** en una transacción de comercio electrónico es la **seguridad**, como en todas las transacciones que implican el manejo de dinero.

Pero hay otros **requisitos aconsejables** para que los sistemas de comercio electrónico sean comparables a los de monedas y billetes, sino no se aplican puede que el comercio electrónico no sea atractivo para los usuarios. Estos son:

- **Anonimato.** Con monedas o billetes la identidad del comprador no es conocida por los vendedores. Para poder mantener también en el comercio electrónico el derecho propio de los humanos a la intimidad, nadie excepto el banco propio deberían conocer la identidad del comprador y éste no debería conocer la naturaleza de la compra.
- **Flexibilidad.** Poder aceptar diferentes medios de pago para todas las situaciones posibles de usuarios de Internet.
- **Convertibilidad.** Poder transformar los diferentes sistemas de pago sin necesidad de realizar una compra, como pasa con las divisas y las cuentas de los bancos.
- **Eficiencia.** El coste del sistema de comercio no debe ser mayor que el precio del producto o servicio.
- **Ser divisible.** Como las monedas o billetes poder dividir la posibilidad de compra en fracciones más pequeñas.
- **Transferible.** Poder pasar el poder de compra de una persona a otra sin necesidad de realizar una transacción, igual que se puede prestar o regalar el dinero tradicional.

El único sistema de pago que cumple todos los requisitos es el dinero electrónico.



1.3. *Dinero electrónico*

Estos sistemas **deben cumplir todos los requisitos** comentados en el apartado 1.2, por lo tanto tienen exactamente las mismas funciones que las monedas y los billetes.

Se utilizan diversas tecnologías para implementarlos:

- **Números firmados.** La entidad financiera emite unos números aleatorios y los firma con su clave privada. Estos números están registrados en la base de datos de la entidad. Su valúa depende de la longitud del número y se pueden fraccionar cambiándolos en la entidad. Los usuarios los piden por la red a la entidad a cambio de un cargo a su cuenta o tarjeta y los utilizan o dan cuando creen conveniente. El sistema DigiCash trabaja con este tipo de dinero electrónico.
- **Monederos electrónicos.** Son tarjetas con un chip donde se almacenan cantidades de dinero que previamente se han descontado de una cuenta. El poseedor de la tarjeta posee el dinero de forma anónima y los puede gastar cuando y de la forma que quiera, así como prestar. Estos sistemas ya se utilizan en las compras físicas, pero para Internet se deberían construir ordenadores con lectores adecuados.

1.4. *Sistemas de crédito y débito*

En estos sistemas el usuario **debe tener una cuenta con la entidad** que gestiona los pagos, esta cuenta puede recibir dinero real o estar conectada a una cuenta real de un banco y recibir cargos por las compras.

Pueden ser de:

- **Débito.** Se debe tener dinero en la cuenta para cubrir el gasto.
- **Crédito.** La entidad puede dar crédito hasta el día del pago completo o fraccionado.

Los usuarios se deben **dar de alta en el sistema** y abrir la cuenta, después reciben un **password** o otra manera de identificarse. Al realizar compras en las tiendas virtuales que permiten este forma de pago se debe indicar el password o identificador y entonces se comprueba si el pago está autorizado.

Utilizan este sistema entre otras las entidades: NetCheque, NetBill, FirstVirtual, InfoCommerce, [Virtu@lCash](#), etc... Probablemente cada vez se utilizarán menos debido a la tendencia hacia sistemas universales que no dependen de darse de alta en una entidad. Pueden servir para realizar micropagos.

1.5. *Tarjetas de crédito o débito*

Son los más utilizados y posiblemente los que se extiendan más en el futuro. Se trabaja con una tarjeta de crédito o débito cargando la compra como si se hubiera hecho en una tienda física. No cumple los requisitos de anonimato, aunque el sistema de seguridad



SET permite que el vendedor no conozca los datos de la tarjeta del comprador y el banco los datos del producto o servicio comprado.

1.6. Sistemas de micropagos

Los micropagos en comercio electrónico ocurren cuando **el precio del producto o servicio es muy pequeño** y puede ser menor que coste de la transacción realizada mediante los métodos habituales.

La característica fundamental de estos sistemas es **bajar mucho los costes de la transacción a costa de pérdida de seguridad**. Su principio se basa en que las transacciones son tan pequeñas que no resultan atractivas para realizar un ataque, así los esfuerzos realizados por el ladrón no compensan el valor del robo.

Se utilizan unos intermediarios llamados **Brokers**. Es normal que un comprador realice muchos micropagos a muchos vendedores diferentes y que un comerciante reciba muchas compras de poco valor de muchos compradores diferentes. Gestionar estas interacciones múltiples entre compradores y vendedores por muy poco margen de beneficio no interesa a ninguna de las partes. Así se utilizan brokers que **concentran todas las compras de un comprador y todas las ventas de un comerciante** y así simplifican el modelo (Ver Figura 1.6.1).

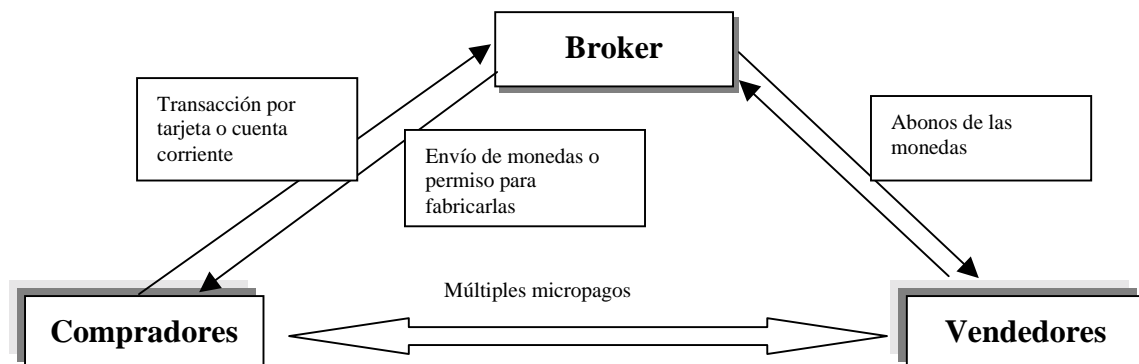


Figura 1.6.1: Arquitectura de un sistema de micropagos

Actualmente no existe un estándar para realizar micropagos sino que existen varios sistemas que compiten para ser el futuro estándar, algunos ya se están utilizando. Unas características comunes a la mayoría son:

- **Utilización de dinero electrónico.** Utilizan sistemas con características de dinero electrónico (ver apartado 1.3 *Dinero electrónico*). Las unidades de transacción se llaman **monedas electrónicas** y pueden ser generadas por el broker o por el comprador que posee un permiso firmado por el broker.
- **Cambio.** Los vendedores tienen la posibilidad de devolver cambio o las monedas se pueden fragmentar.
- **Detección de doble pago.** Para detectar la doble utilización de las monedas electrónicas los vendedores mantienen una base datos con los mensajes moneda recibidos, esto se debe mantener hasta la caducidad de estos mensajes. Esta



prestación obliga en la mayoría de sistemas a editar monedas específicas para un vendedor y, por lo tanto, se pierde la flexibilidad de sistema universal.

- **Cifrado débil.** Para aumentar la velocidad de proceso y facilitar la gestión de claves no se acostumbra a utilizar encriptación de clave pública, pero si se utiliza, se procura minimizar el número de ejecuciones del algoritmo. Normalmente la seguridad se implementa mediante funciones Hash con o sin clave.

Algunos de los sistemas más conocidos son:

- **Millicent.** Las monedas electrónicas se denominan *scrips*. La seguridad se basa en una clave secreta compartida entre el vendedor y el broker. No utiliza encriptación sólo funciones Hash con clave. Los *scrips* están marcados para un comprador y un vendedor determinados, se compran al Broker.
- **MicroMint.** Permite diferentes formas de monedas: anónimas (poca seguridad), marcadas para el comprador y marcadas para el vendedor. Como seguridad solamente utiliza la propiedad de resistencia a colisiones de las funciones Hash. Las monedas se compran al broker.
- **Payword.** Las monedas son cadenas de resúmenes realizados por funciones Hash, denominadas *Paywords*, cada elemento de la cadena es la función Hash del anterior y el primero es un número aleatorio. Los *Payword* son generados por el comprador y sirven para cualquier vendedor. Para generar *Paywords* se debe poseer un certificado de clave pública firmado por el broker, donde aparece la cantidad máxima que se puede gastar en una transacción. Es un sistema de crédito donde el broker responde del cliente (como las tarjetas). En cada compra se realiza una única encriptación de clave pública.
- **SubScrip.** Utiliza un mensaje llamado ticket que es específico para un vendedor y un comprador. El ticket se actualiza en el vendedor después de cada compra, restando la cantidad pagada del total. El vendedor mantiene una base de datos de los tickets y sus últimos valores. Los Brokers generan los tickets.

La Tabla 1.6.1 compara los 4 sistemas.

	Millicent	MicroMint	Payword	SubScrip
Encriptación	No	No	Sí	No
Hashing	Sí, con clave.	Sí	Sí	No
Monedas específicas de vendedor	Sí	Depende	No	Sí
Monedas específicas de comprador	Sí	Depende	Sí	Sí
Genera las monedas	Broker	Broker	Comprador	Broker

Tabla 1.6.1



2. SSL (Secure Sockets Layer) y TLS (Transport Layer Security)

2.1. Características del SSL

El SSL es un protocolo seguro de Internet inventado por la empresa Netscape. No es exclusivo del comercio electrónico sino que sirve para cualquier comunicación vía Internet y, por lo tanto, también para transacciones económicas. Está implementado por defecto en todos los navegadores de Netscape para Webs, o sea, para el protocolo HTTP, aunque se espera que pronto salgan versiones para Mail, FTP, etc...

Sustituye los sockets del sistema operativo. Los sockets son el interficie entre las aplicaciones y el protocolo TCP/IP del sistema operativo (Ver Figura 2.1.1). Así puede servir para cualquier aplicación que utilice TCP/IP: Mail, Webs, FTP, News, etc... Aunque las aplicaciones de los programas actuales sólo permiten HTTP (Webs).

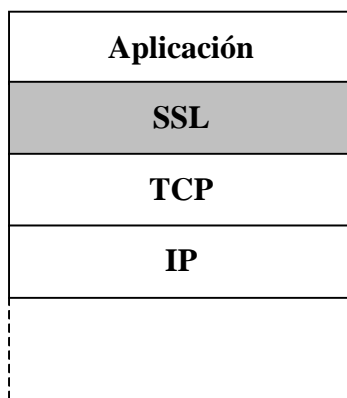


Figura 2.1.1: Situación de SSL en la pila TCP/IP

Para diferenciar las páginas dentro de una zona de servidor SSL, Netscape utiliza la denominación https y se conecta mediante el puerto 443.

El SSL puede realizar las **funciones**:

- **Fragmentación.** En el emisor se fragmentan los bloques mayores que 2^{14} octetos y en el receptor se vuelven a reensamblar.
- **Compresión.** Se puede aplicar un algoritmo de compresión a los mensajes.
- **Autenticación.** Permite autenticar el cliente y el servidor mediante certificados. Este proceso se realiza durante la fase de Handshake. Durante la transmisión los mensajes autentican al emisor mediante un resumen con clave, llamado **MAC**, en cada mensaje.
- **Integridad.** En todos los mensajes se protege la integridad mediante el MAC.
- **Confidencialidad.** Todos los mensajes se envían encriptados.

Se utilizan **certificados X.509v3** para la transmisión de las claves públicas.



2.2. Protocolo SSL

El protocolo SSL se divide en dos capas complementarias (ver Figura 2.2.1):

- **Protocolo Handshake.** Realiza las siguientes funciones:
 - Autenticación de usuario y servidor.
 - Selección de los parámetros de la sesión y de la conexión.
 - Establece la conexión segura.
- **Protocolo de registro** (Record protocol). Se utiliza para la encriptación de los protocolos de las capas más altas: Handshake y aplicaciones.

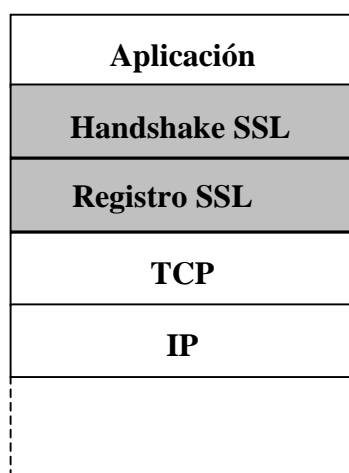


Figura 2.2.1: Protocolos de SSL

El protocolo SSL se comporta como una máquina de estados, durante el intercambio de información siempre hay un estado de escritura activo y otro pendiente y un estado de lectura activo y otro pendiente. Para cambiar del estado activo al pendiente se utiliza un subprotocolo del Handshake llamado **Change Cipher Spec**.

Entre dos entidades cliente y servidor se pueden abrir varias sesiones SSL, aunque no es habitual, y dentro de cada sesión se pueden mantener varias conexiones SSL. Las conexiones se abren o cierran a través del protocolo de Handshake.

Un **estado de sesión** incluye los siguientes elementos:

- **Identificador de sesión.** Un número arbitrario elegido por el servidor para identificar la sesión.
- **Certificado.** El certificado X.509v3 del otro.
- **Método de compresión.** Algoritmo de compresión.
- **Algoritmo de encriptación.** Especifica el algoritmo simétrico de encriptación para confidencialidad y la función Hash de resumen para integridad. También se definen atributos de Hash o encriptación.
- **Clave maestra.** Un número de 48 bytes secreto entre el servidor y el cliente.
- **Flag de nuevas conexiones.** Indica si desde esta sesión se pueden iniciar nuevas conexiones.



Un **estado de conexión** incluye los siguientes elementos:

- **Números aleatorios del servidor y el cliente.** Números de inicio de la secuencia elegidos por el cliente y el servidor.
- **Número secreto del cliente para MAC.** Número secreto utilizado por el cliente para calcular los MAC de sus mensajes.
- **Número secreto del servidor para MAC.** Número secreto utilizado por el servidor para calcular los MAC de sus mensajes.
- **Clave secreta del cliente.** Clave secreta utilizada por el cliente para encriptar sus mensajes.
- **Clave secreta del servidor.** Clave secreta utilizada por el servidor para encriptar sus mensajes.
- **Vectores iniciales (IV).** Si se utiliza encriptación con modo CBC (Cipher Block Chaining) se necesita un vector inicial para cada clave.
- **Números de secuencia.** Cada parte actualiza números de secuencia en cada mensaje, estos son puestos a cero cuando se recibe un mensaje change cipher spec.

2.3. Protocolo de registro en SSL

El protocolo de registro realiza las funciones de seguridad sobre los mensajes que llegan de la capa de Handshake o de las aplicaciones (HTTP, FTP,...). Para ello utiliza los parámetros de conexión que se han negociado antes mediante la capa de Handshake. En la Figura 2.3.1 se pueden ver las funciones realizadas por orden de actuación en el emisor.

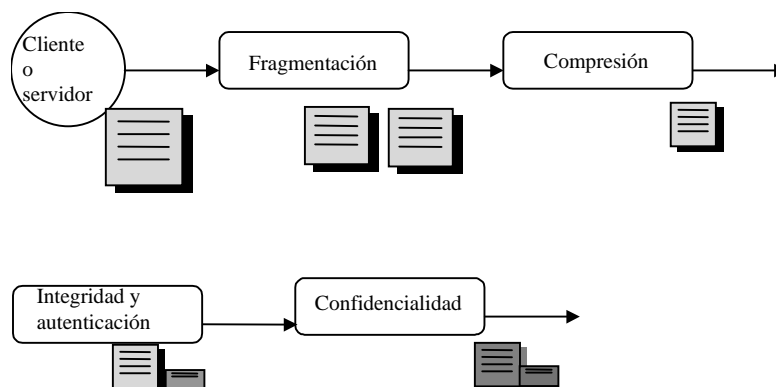


Figura 2.3.1: Protocolo de registro de SSL

La **fragmentación** divide los mensajes mayores de 2^{14} bytes en bloques más pequeños.

La **compresión** se realiza utilizando el algoritmo que se ha negociado en la fase inicial, puede ser algoritmo nulo (Null) si no se comprimen los mensajes.

La **autenticación e integridad** se realiza calculando un resumen del mensaje concatenado con un número secreto y el número de secuencia (Ver Figura 2.3.2). El resultado de este resumen es el MAC y se añade al mensaje. La autenticación se puede comprobar con el número secreto, que sólo comparten el cliente y el servidor, y

mediante el número de secuencia que nunca viaja en claro. La integridad se realiza mediante la función Hash.

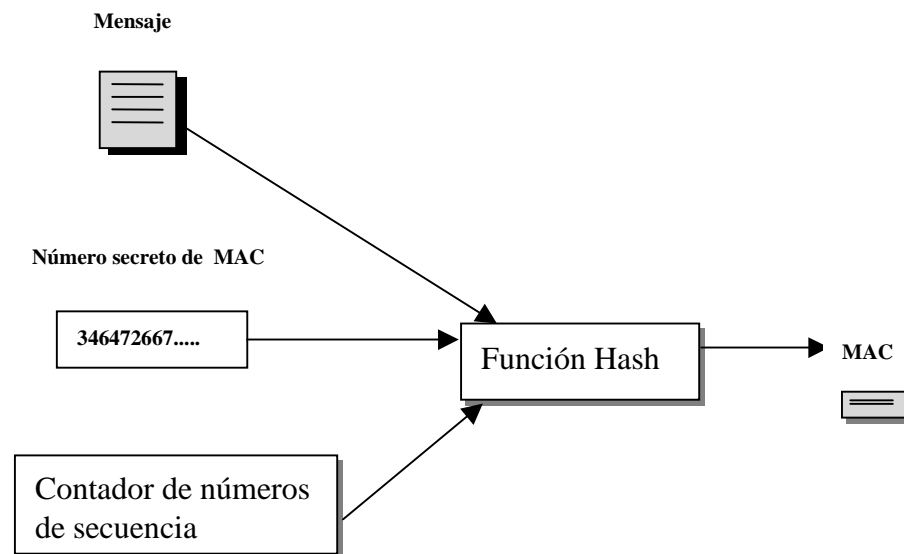


Figura 2.3.2: Integridad en el protocolo de registro de SSL

La **confidencialidad** se realiza encriptando con un algoritmo simétrico mediante la clave secreta negociada en el Handshake. Las encriptaciones pueden ser de:

- **Bloque.** Se encripta en bloques de 64 bits. Si el mensaje no es múltiplo de 64 se añaden bits de relleno y se indica en el formato del mensaje. Los algoritmos utilizados son RC2 y DES en forma CBC, para la forma CBC se utiliza un vector inicial (IV) previamente pactado.
- **Stream.** Se encripta realizando la OR-Exclusiva entre los bytes y un generador pseudoaleatorio, este generador es el algoritmo RC4.

2.4. Protocolo Handshake en SSL

Se encarga de establecer, finalizar y mantener las conexiones SSL. Durante el Handshake se negocian los parámetros generales de la sesión y los particulares de cada conexión. Hay dos subprotocolos anexos:

- **Change Cipher Spec.** Es un único mensaje que sirve para pasar de los estados activos a los pendientes.
- **Alerta.** Son mensajes que avisan de problemas ocurridos durante la conexión, pueden obligar a una terminación brusca de la sesión.

En la Figura 2.4.1 se puede ver el esquema del protocolo.

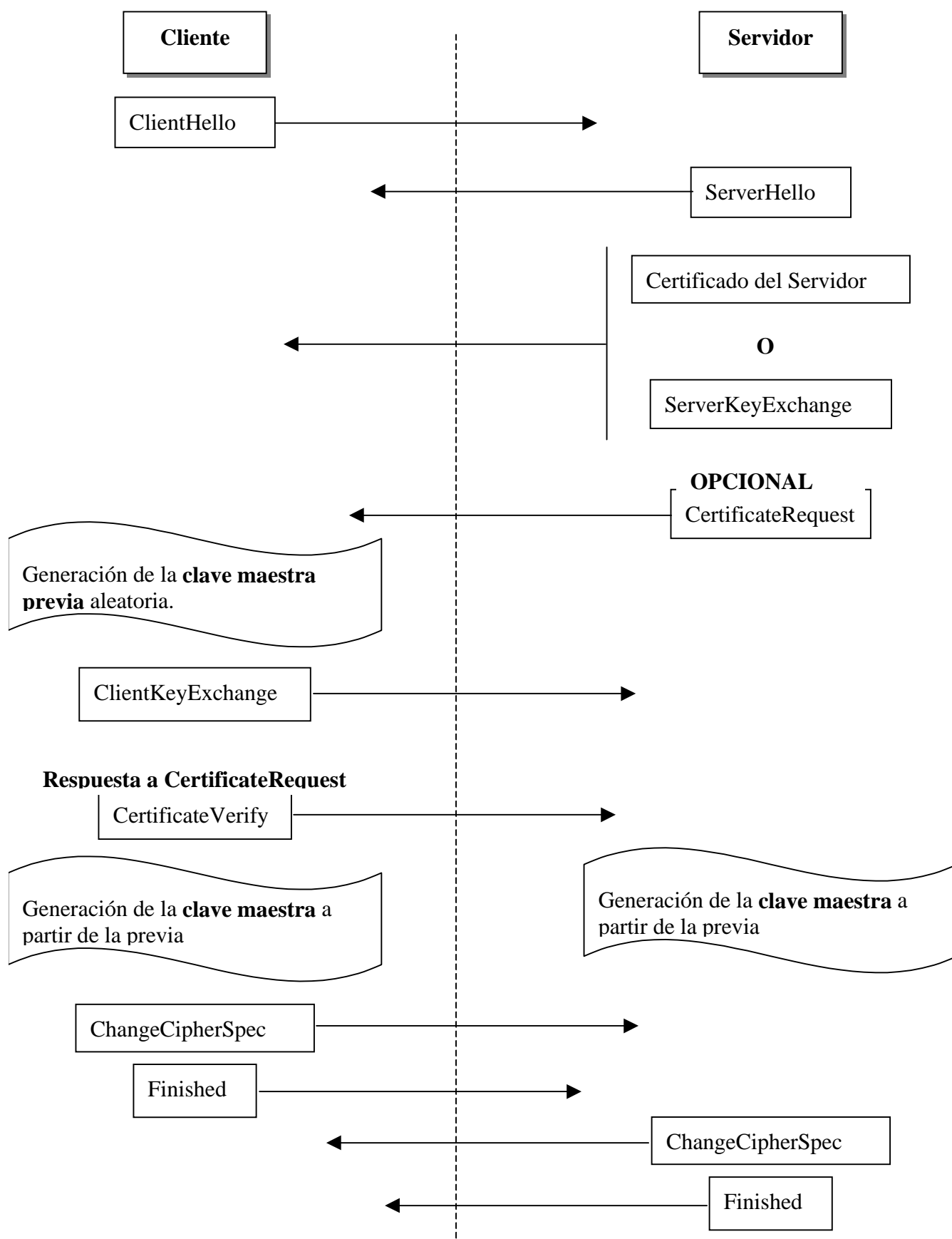


Figura 2.4.1: Protocolo Handshake de SSL



Los mensajes llevan la siguiente información:

- **ClientHello.** Es el mensaje que envía el cliente cuando establece contacto con un servidor seguro. Describe los parámetros que quiere utilizar durante la sesión:
 - **Hora y fecha.**
 - **Identificador de sesión.**
 - **Algoritmos de encriptación.** Consecutivamente envía los algoritmos por orden de preferencia de intercambio de claves, encriptación de mensajes y MAC.
 - **Algoritmos de compresión.** Se envían los algoritmos que acepta por orden de preferencia.
- **ServerHello.** Se envían los algoritmos elegidos para la conexión, siempre deben ser alguno de los propuestos en el mensaje de ClientHello. Si no hay acuerdo con los algoritmos se envía un mensaje de error.
- **Certificado o ServerKeyExchange.** Si el servidor tiene certificado X.509v3 se envía, sino no tiene se puede utilizar el mensaje ServerKeyExchange para enviar la clave pública sin certificado. El cliente puede elegir si acepta una clave sin certificado.
- **CertificateRequest.** Los servidores pueden pedir certificados a los clientes utilizando este mensaje.
- **CertificateVerify.** Si el cliente recibe una petición de certificado debe enviar su certificado mediante este mensaje.
- **ClientKeyExchange.** Se envía un número aleatorio que sirve para calcular la clave maestra, esta clave sirve para generar todas las claves y números secretos utilizados en SSL. Se envía encriptada con la clave pública del servidor.
- **ChangeCipherSpec.** Inicia la sesión segura.
- **Finished.** Termina la fase de Handshake. Sirve para comprobar que la negociación de parámetros y claves ha funcionado correctamente.

2.5. Protocolo TLS

El TLS es un protocolo estandarizado por el IETF, por lo tanto, es un estándar de facto de Internet. Su origen es el SSL versión 3 pero se aparta de éste para mejorar algunas cosas y, sobre todo, porque SSL es propiedad de una empresa privada: Netscape. Así el **TLS** puede ser el **estándar mundial** para todo el software de cliente y servidor. El TLS permite **compatibilidad con SSLv3**, el cliente y el servidor definen el protocolo utilizado durante el Handshake.

Las **diferencias** más importantes son sobre los siguientes aspectos:

- **Alerta de certificado.** En respuesta al mensaje CertificateRequest los clientes que no tienen certificado sólo contestan con un mensaje de alerta si son SSL.
- **Claves de sesión.** Se calculan de forma diferente.
- **Algoritmos de intercambio de claves.** El TLS no soporta el algoritmo Fortezza Kea del SSL, un algoritmo secreto y de propiedad privada muy similar al Diffie Hellman.
- **Campos incluidos en el MAC.** En TLS se utilizan dos campos más del mensaje que en SSL para el cálculo del MAC. Es más seguro.



3. SET (Secure Electronic Transaction)

3.1. Características

El SET es un protocolo inventado **exclusivamente para realizar comercio electrónico con tarjetas de crédito**. Fue impulsado por las empresas de tarjetas de crédito Visa y MasterCard, las más extendidas e importantes del mundo. Han colaborado en su desarrollo las empresas más significativas del mundo de la telemática: GTE, IBM, Microsoft, SAIC, Terisa, Verisign, etc... La participación de estas empresas tan importantes y especialmente el impulso de las marcas de tarjetas Visa y MasterCard hacen que este protocolo tenga muchas posibilidades de convertirse en el futuro sistema de comercio electrónico seguro.

Es un **sistema abierto y multiplataforma**, donde se especifican protocolos, formatos de mensaje, certificados, etc... sin limitación de lenguaje de programación, sistema operativo o máquina. El **formato de mensajes** está basado en el estándar definido por la empresa RSA Data Security Inc. **PKCS-7**, como los protocolos S-MIME y SSL.

La especificación del SET v1.0 está contenida en 3 volúmenes publicados en mayo de 1997 y es de libre distribución en la web www.setco.org. El organismo SETco homologa los módulos de programación y los certificados desarrollados por empresas privadas, después de pasar unos tests técnicos y pagar unos derechos. El software homologado por SETco tiene derecho a llevar el logotipo de SET.

El protocolo SET se puede transportar directamente en TCP, mediante correo electrónico con SMTP o MIME y en Webs con HTTP.

3.2. Agentes del comercio electrónico de SET

En SET se definen **5 agentes** que pueden intervenir en transacciones comerciales:

- **Comprador.** Adquiere un producto utilizando la tarjeta de crédito de su propiedad.
- **Banco o entidad financiera (Issuer).** Emite la tarjeta de crédito del comprador.
- **Comerciante (Merchant).** Vende los productos.
- **Banco del comerciante (Acquirer).** Banco donde el comerciante tiene la cuenta.
- **Pasarela de pagos (Payment gateway).** Gestiona la interacción con los bancos. Puede ser una entidad independiente o el mismo banco del comerciante.

Dos agentes relacionados pero que no actúan directamente en las transacciones son:

- **Propietario de la marca de la tarjeta.** Avalan las tarjetas: Visa, MasterCard, American Expres, etc...
- **Autoridad de certificación.** Crea los certificados que se utilizan en las transacciones de la pasarela, el vendedor y el comprador. Pueden ser los bancos, los propietarios de la marca de la tarjeta o entidades independientes.

Se relacionan entre ellos como marca la Figura 3.2.1.

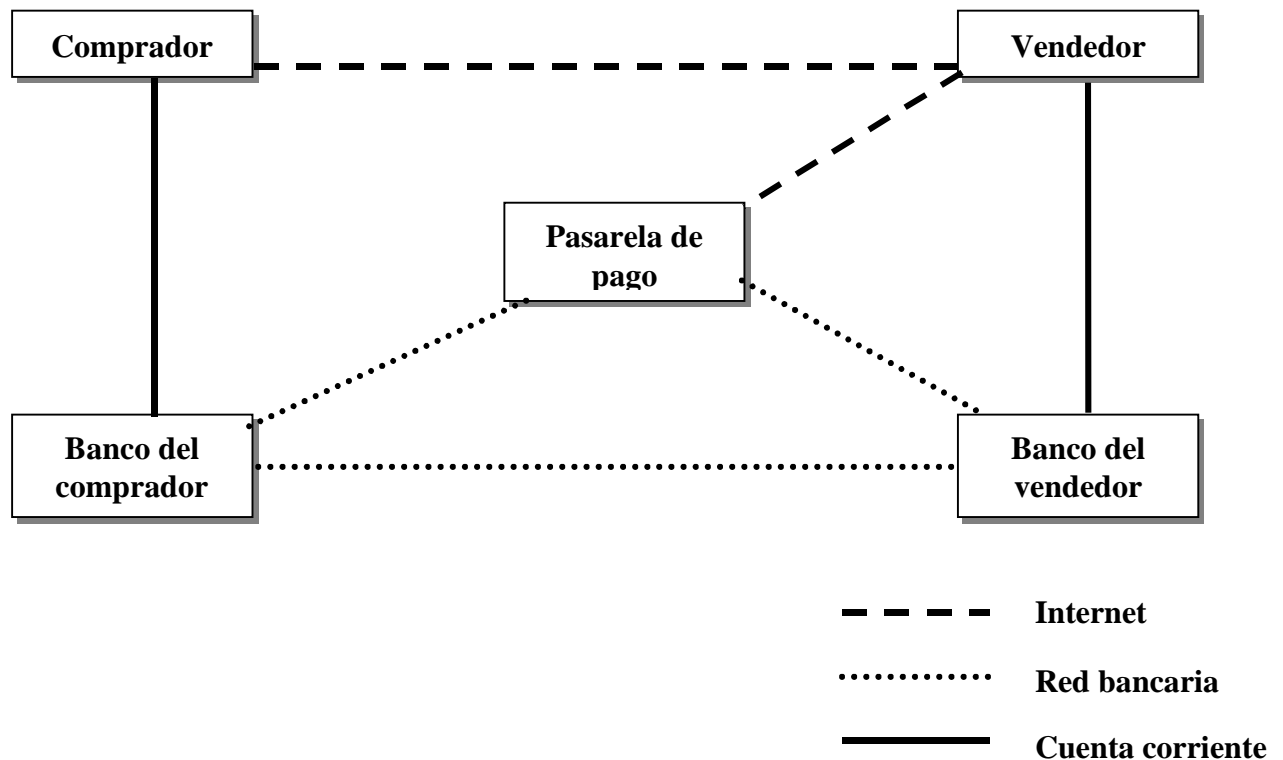


Figura 3.2.1: Agentes del SET

3.3. Módulos de programación

Para poder utilizar el SET se deben incorporar unos módulos de software que adaptan los programas existentes al protocolo. Se han definido 4 **módulos**:

- **Cartera** (Wallet). Es una aplicación que se instala en el navegador del comprador como plug-in.
- **De venta** (merchant). Se conecta a la Web del vendedor. Como se parece mucho a los actuales terminales punto de venta para tarjetas se le llama también TPV.
- **Pasarela de pagos** (payment gateway). Cumple las funciones de este agente.
- **Autoridad de certificación** (CA). Crea certificados de clave pública adaptados al estándar SET.

Los 4 módulos se pueden **homologar** por separado en la entidad **SETco**, actualmente ya hay varias empresas que ofrecen productos comerciales de alguno de los módulos con sello SET.

3.4. Firma dual

La firma dual es un concepto nuevo de firma inventado por el SET, para dos documentos relacionados resuelve el compromiso entre su privacidad mutua frente a la necesidad de demostrar que están relacionados comercialmente.



En una transacci3n SET:

- El vendedor no debe saber los datos bancarios del comprador.
- El banco no debe saber la informaci3n del producto vendido.

Pero los documentos con la informaci3n bancaria y la del producto **deben estar ligados por la misma firma**, de manera que se pueda comprobar que han sido generados por la misma persona y para el mismo fin. En las transacciones del SET el comprador genera dos documentos:

- **Informaci3n de pedido (OI).** Donde se describen los datos del producto, el precio y todas las informaciones necesarias para realizar la compra. Este documento s3lo puede ser visto por el vendedor.
- **Instrucciones de pago (PI).** Donde se describen los datos bancarios del comprador y se dan instrucciones para el pago de la cantidad de venta. Este documento s3lo puede ser visto por la pasarela de pago.

La firma dual del OI y el PI se realiza concatenando los res3menes de los dos y despu3s encriptandolos con la clave privada del comprador (ver Figura 3.4.1).

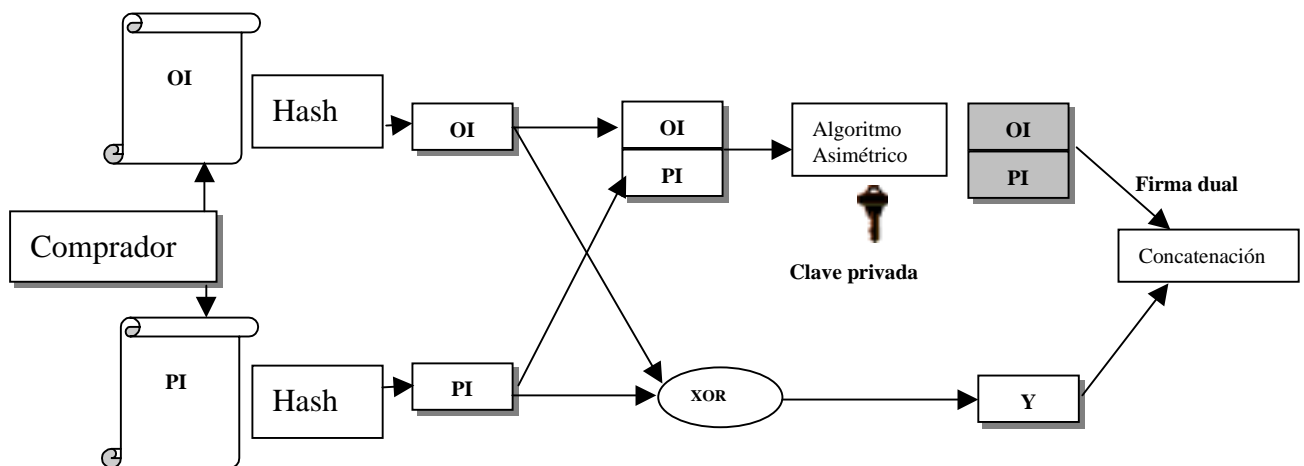


Figura 3.4.1: Firma dual en SET

Cada parte recibe uno de los mensajes y la firma dual:

$$M_1 \mid FD = M_1 \mid X \mid Y = M_1 \mid E_{KP}[H(M_1) \mid H(M_2)] \mid H(M_1) \mid H(M_2)$$

Para comprobar la firma dual se realizan las operaciones:

- $H_1 = H(M_1)$
- $H_2 = H_1 \text{ XOR } Y$
- Se comprueba si $\checkmark D_{KU} [X] = H_1 \mid H_2$?



En el **SET**:

el vendedor recibe del comprador:

- OI.
- Firma dual.

Comprueba la autenticación del comprador y la integridad del OI. (Ver Figura 3.4.2)

La pasarela de pagos recibe del comprador:

- PI.
- Firma dual.

Del vendedor:

- Resumen del OI.

Con el mensaje del comprador comprueba la autenticación del comprador y la integridad del PI. Con el mensaje del vendedor comprueba la relación entre el OI enviado al vendedor y el utilizado para la firma dual recibida. (Ver Figura 3.4.2)

El **comprador no se conecta directamente con la pasarela de pagos**, envía al vendedor todos los documentos pero **la información para la pasarela se encripta con la clave pública de la pasarela**. Cuando el vendedor ha comprobado la información dirigida a él, envía la parte encriptada a la pasarela.

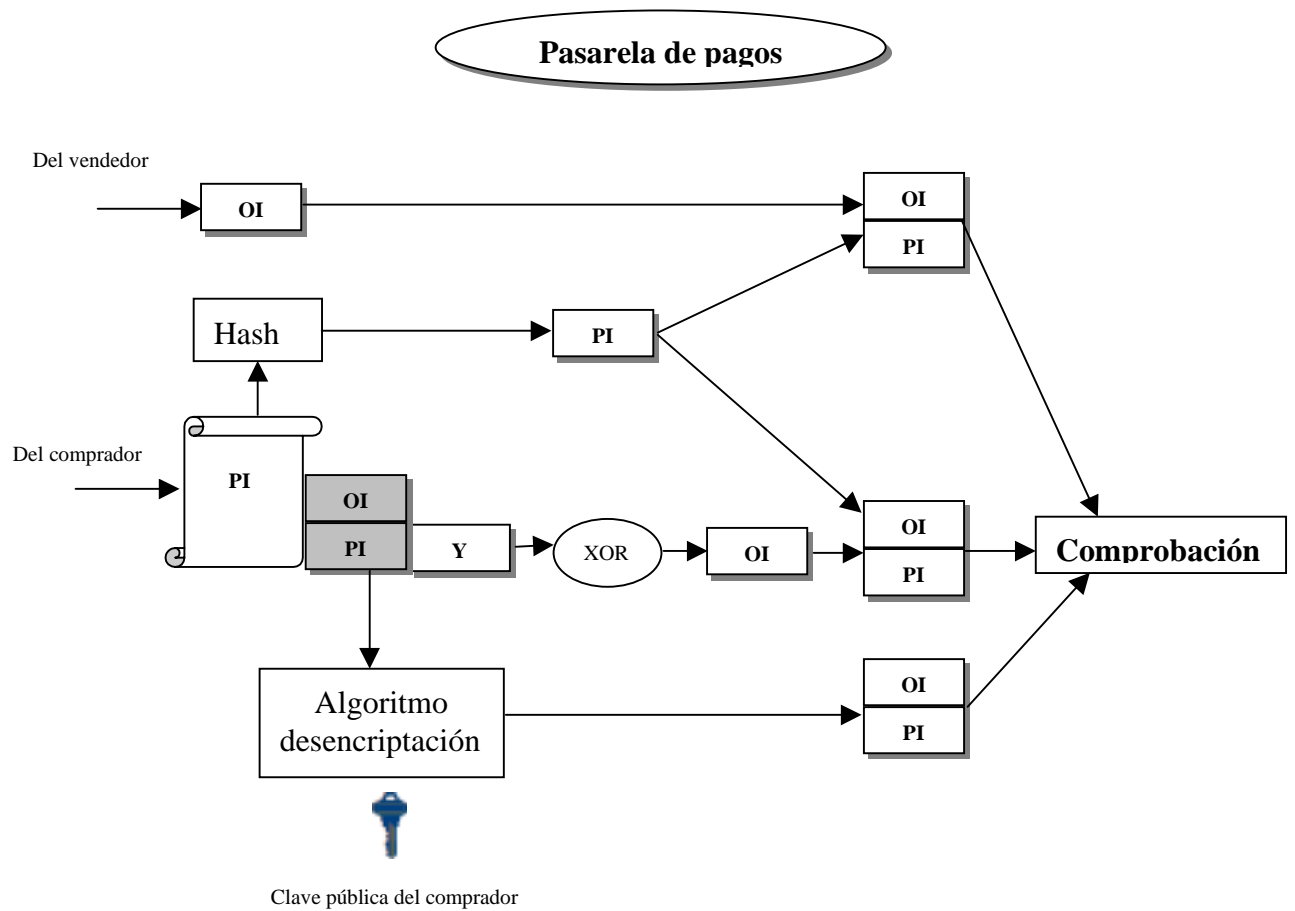
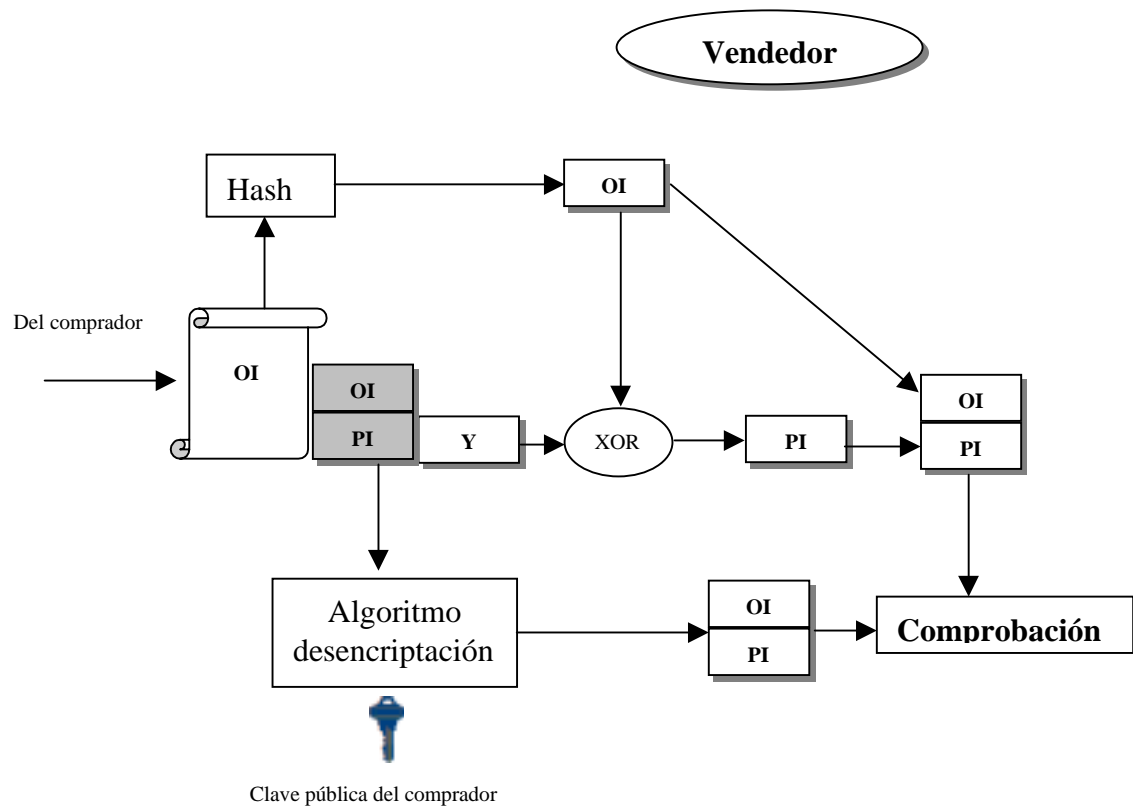




Figura 3.4.2: Tratamiento de los mensajes PI y OI en SET

3.5. Transacción de compra

En la transacción de compra actúan el comprador, el vendedor y la pasarela a través de Internet y la pasarela se comunica con los bancos por medio de la red bancaria. El comprador siempre se relaciona con la pasarela a través del vendedor, nunca directamente. La seguridad se gestiona de la siguiente manera:

- **Confidencialidad.** Se encripta utilizando claves de sesión encriptadas con las claves públicas de los receptores.
- **Firma electrónica.** Se utilizan firmas normales y duales encriptadas con las claves privadas de los firmantes.
- **Suplantación de personalidad.** Las claves públicas del vendedor, comprador y pasarela se deben enviar al principio mediante certificados avalados por una autoridad de certificación homologada por SET.

Los documentos utilizados son:

- **Información de pedido (OI).** Ver apartado 3.4 *Firma dual*..
- **Instrucciones de pago (PI).** Ver apartado 3.4 *Firma dual*.
- **Petición de autorización de pago.** El vendedor cuando ha comprobado que los datos enviados por el comprador son correctos envía este mensaje a la pasarela para que pida autorización de pago a los bancos. La pasarela cuando ha comprobado los datos que ha recibido del vendedor hace una petición de pago al banco del comprador.
- **Autorización de pago.** El banco envía una autorización de pago a la pasarela si la tarjeta del comprador es correcta y permite el cargo del importe.
- **Solicitud de pago.** Después de la entrega física del producto el vendedor pide cobrar a la pasarela el pago.
- **Solicitud de compensación.** La pasarela pide al banco del comprador la transferencia al banco del vendedor.

Todos los documentos llevan el identificador único de la transacción (ID).

La transacción puede realizarse con o sin firma dual, mediante un protocolo inicial los agentes deciden el tipo de transacción.

El esquema de la transacción con firma dual se puede ver en la Figura 3.5.1., los detalles se han omitido. El significado de los símbolos representados en la Figura 3.5.1 son:

ES_{KUX}[M]. M encriptado con una clave de sesión aleatoria k y un algoritmo simétrico y k encriptado con un algoritmo asimétrico con la clave pública de X.

FD. Firma dual del OI y el PI.

Firma. La firma calcula realizada con la encriptación del resumen con la clave privada del emisor.



Cx. Comprador de clave pública de X.

Vendedor

Pasarela de pagos

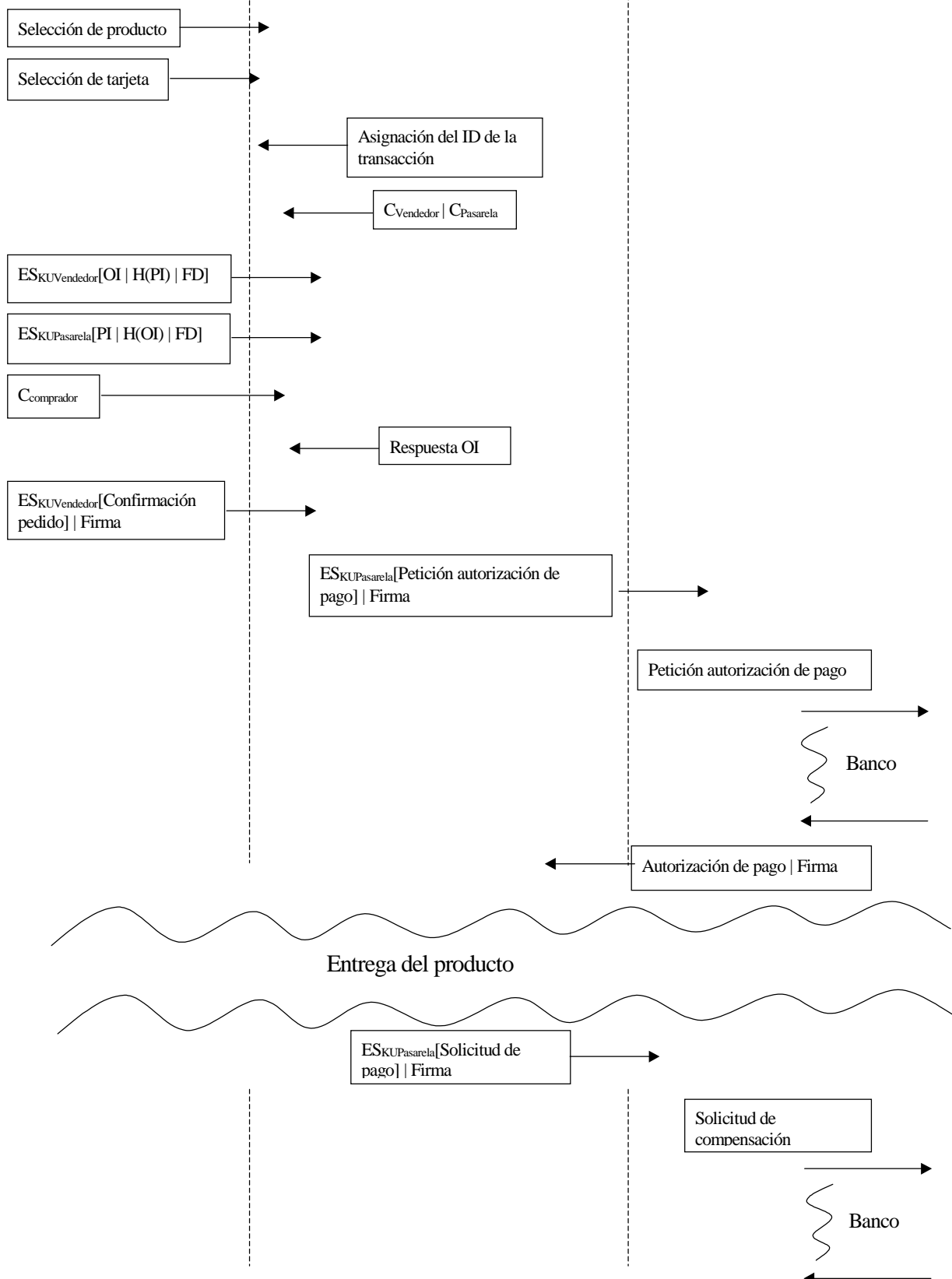


Figura 3.5.1: Transacción de compra en SET