# SEGURIDAD EN EL CONTEXTO DEL COMERCIO ELECTRÓNICO E INTERNET
# LOS PROTOCOLOS SSL Y SET

*Joaquín Peña, Antonio Ruiz y Francisco Ferrer*
*Informe Técnico*
*Dpto. Lenguajes y Sistemas Informáticos de la Universidad de Sevilla*
*Avda. de la Reina Mercedes, s/n. Sevilla, 41.012*
*E-mail: jpena@lsi.us.es*

# Índice

## 1.- Introducción

Es un hecho de todos conocido que Internet constituye un canal de comunicaciones inseguro, debido a que la información que circula a través de esta red es fácilmente accesible en cualquier punto intermedio por un posible atacante. Los datos transmitidos entre dos nodos de Internet (por ejemplo una máquina y el servidor web desde el que quiere descargar una página) se segmentan en pequeños paquetes que son encaminados a través de un número variable de nodos intermedios hasta que alcanzan su destino. En cualquiera de ellos es posible leer el contenido de los paquetes, destruirlo e incluso modificarlo, posibilitando todo tipo de ataques contra la confidencialidad y la integridad de sus datos.

En los últimos cinco años ha ido surgiendo un número considerable de tecnologías y sistemas de pago electrónico que ofrecen las garantías de seguridad e integridad necesarias para realizar las compras en línea de una manera fiable y sin sorpresas. La piedra angular de todas ellas es la criptografía, que proporciona los mecanismos necesarios para asegurar la confidencialidad e integridad de las transacciones.

En este trabajo veremos en que consisten y como proporcionan la seguridad dos de los protocolos más importantes que existen en la actualidad: uno es el **SSL** (Secure Sockets Layer) que es la solución más adoptada en la actualidad, y otro, el protocolo **SET** (Secure Electronic Transaction) que sin duda será el nuevo estándar dentro de Internet en muy poco tiempo.
Antes de estudiar los protocolos de seguridad para Internet veremos una introducción a los certificados, autentificación y criptografía, ya que son necesarias para comprender el funcionamiento de los protocolos SSL y SET.

## 2.- Criptografía, autentificación y certificación

La introducción a los certificados y la autentificación trata de los certificados digitales y cómo se utilizan para la autentificación. Se incluye una explicación de los sistemas de seguridad de software y cifrado para proporcionar información fundamental sobre este tema.

En una red de acceso público como Internet, la información puede caer en manos de usuarios con intenciones desconocidas. Si la información tiene poco valor o ninguno, las medidas de seguridad pueden resultar innecesarias. Si la información es importante o confidencial, se deben tomar las medidas de seguridad adecuadas para asegurar la información.

Esto significa asegurar que sólo las personas con las que se desea compartir información podrán entenderla y que los usuarios con los que se comparte la información son realmente las personas elegidas para compartirla. Estas son las dos ideas expresadas por los términos *privacidad* y *autentificación*.

En este contexto, la *privacidad* depende de la capacidad de impedir que alguien, excepto el destinatario indicado, pueda leer un mensaje, incluso si un usuario de la red es capaz de interceptarlo. También en este contexto, la *autentificación* es la comprobación de que la entidad con quien se está comunicando es, en realidad, quien dice ser, incluso si no tiene medios físicos directos para comprobarlo.

La necesidad de privacidad y autentificación en las redes no seguras requiere del cifrado y descifrado de datos como parte de un sistema de seguridad de software. Los protocolos de cifrado que utilizan los certificados están diseñados para cubrir estas necesidades.

## 2.1.- Criptografía

La criptografía proporciona un conjunto de técnicas para cifrar los datos y mensajes de forma que se almacenen y transmitan de forma segura. La criptografía puede lograr comunicaciones seguras incluso cuando el medio de transmisión (por ejemplo, Internet) no sea confiable. La criptografía también puede cifrar archivos confidenciales para que un intruso no pueda entenderlos.

La criptografía también proporciona técnicas para descifrar los datos y mensajes cifrados de forma que se pueda descubrir su estado original. Cuando las técnicas se implementan correctamente, es extremadamente difícil reconstruir el mensaje original sin conocer la clave criptográfica secreta necesaria para descifrar un mensaje. El ***sobre digital***, un método de cifrado donde sólo un destinatario específico puede descifrar un mensaje, es una técnica criptográfica importante.

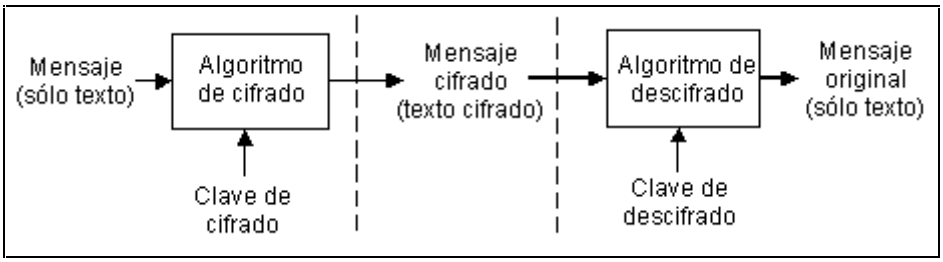
Además, la criptografía proporciona un conjunto de técnicas para comprobar el origen de los datos y mensajes mediante las ***firmas digitales***.

Cuando utiliza la criptografía, la única parte que debe mantener en secreto son las claves criptográficas, con la excepción de las claves conocidas como *claves públicas*. Los algoritmos, los tamaños de las claves y los formatos de archivo se pueden hacer públicos sin comprometer la seguridad.

### 2.1.1.- Cifrado de datos

Al utilizar el cifrado de datos, un mensaje de *texto normal* se puede alterar de forma que parezca un galimatías aleatorio y sea difícil de descifrar sin una clave secreta. Aquí, el término *mensaje* hace referencia a cualquier parte de datos que se deben cifrar. Este mensaje puede ser un texto en formato ASCII, un archivo de base de datos o cualquier tipo de datos destinado a una transmisión segura. El término *texto normal* hace referencia a datos no cifrados y *texto cifrado* hace referencia a datos cifrados.

Después de cifrar un mensaje, se puede almacenar en un medio poco seguro o se puede transmitir a través de una red no segura, y aún así permanecerá secreto. Más tarde, se puede descifrar el mensaje para devolverlo a su formato original. Este proceso se muestra en la siguiente ilustración.



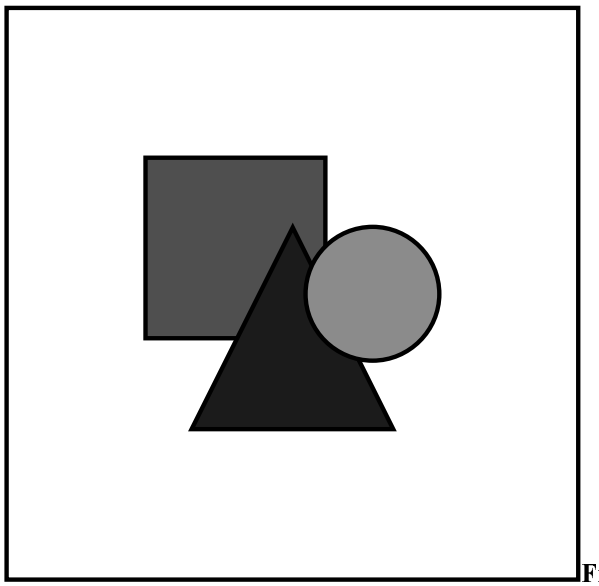


**Figura 1: Cifrado de un mensaje**

Cuando se cifra un mensaje, se utiliza una *clave de cifrado*. Esta clave es análoga a la llave que se utiliza para cerrar un candado. Para descifrar el mensaje, se debe utilizar la *clave de descifrado* correspondiente. Es muy importante restringir correctamente el acceso a la clave de descifrado porque quien la tenga podrá descifrar todos los mensajes cifrados con esa clave de cifrado.

Los algoritmos simétricos son los tipos de algoritmos de cifrado más comunes. Los algoritmos simétricos utilizan la misma clave para el cifrado y el descifrado. Para comunicarse mediante algoritmos simétricos, ambas partes deben compartir una clave secreta.

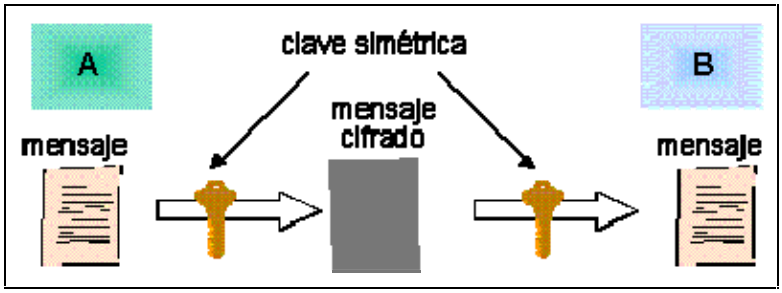



**Figura 2: Cifrado/descifrado simétrico**

Los algoritmos de clave pública (asimétrica) utilizan dos tipos de claves diferentes: una *clave pública* y una *clave privada*. La clave privada permanece privada para el propietario de la pareja de claves y la clave pública se puede distribuir a cualquiera que la solicite (normalmente mediante un certificado digital). Si se utiliza una clave para cifrar un mensaje, se requiere la otra clave para descifrarlo.

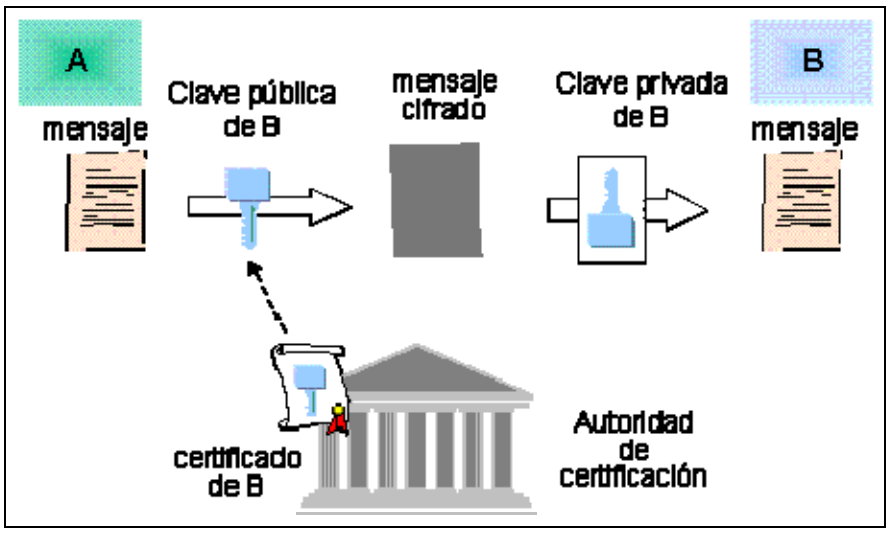



**Figura 3: Cifrado/descifrado asimétrico**

Los algoritmos simétricos son en algunos casos más rápidos que los algoritmos de clave pública y se usan fundamentales para el cifrado de grandes cantidades de datos. Sin embargo, puesto que las claves deben ser secretas, no es práctico distribuirlas a un gran número de personas. Los algoritmos de clave pública solucionan este problema y se pueden utilizar con los algoritmos simétricos para lograr un rendimiento óptimo cuando se trabaja con un gran volumen de datos.

### 2.1.2.- Firmas digitales

Las firmas digitales se pueden utilizar cuando se distribuye un mensaje con formato de texto normal y los destinatarios deben ser capaces de comprobar que el mensaje no ha sido manipulado por un usuario no autorizado. Firmar un mensaje no lo altera, simplemente genera una cadena de firma digital que se empaqueta con el mensaje o se transmite por separado.

Las firmas digitales se pueden generar con algoritmos de firma de clave pública donde la clave privada de quien transmite el mensaje, utilizada para generar la firma, se envía en un mensaje de correo electrónico. Al recibir el mensaje, el destinatario utiliza la clave pública para validar la firma. Como para validar la firma sólo se puede utilizar la clave pública del firmante (recibida por el destinatario en un mensaje de correo electrónico anterior), la firma digital es la prueba de que la identidad del remitente del mensaje es auténtica. Este proceso se muestra en la siguiente ilustración.

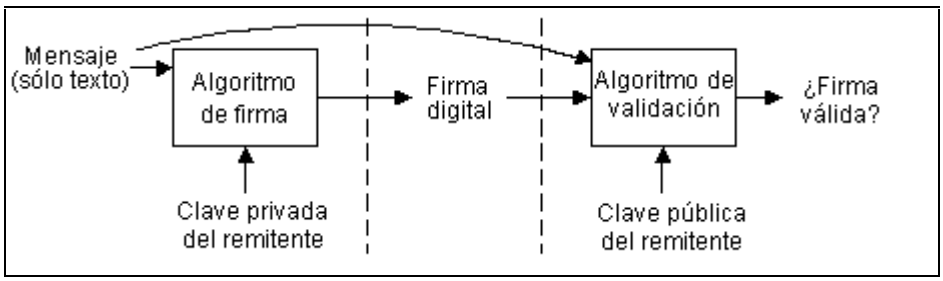



**Figura 3: Firma Digital**

### 2.1.3.- Sobres digitales

Los sobres digitales se utilizan para enviar mensajes privados que sólo un destinatario específico puede entender. El mensaje sólo se puede descifrar mediante la clave privada del destinatario, para que sólo éste sea capaz de entenderlo.

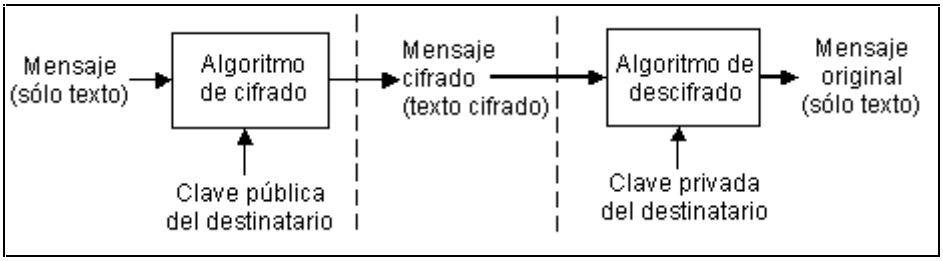



**Figura 4: Sobres digitales**

## 2.2.- Autentificación

En las secciones anteriores que tratan las firmas y los sobres digitales se ha supuesto que la identidad del propietario de la clave pública utilizada para cifrar o descifrar un mensaje se establece sin ninguna duda. Pero en la práctica, ¿cómo pueden los destinatarios de un mensaje supuestamente enviado por alguien llamado "Alicia", acompañado por una firma digital que se puede validar con una clave pública que supuestamente pertenece a Alicia, estar seguros de que realmente están utilizando la clave pública de Alicia? Y de forma similar, ¿cómo puede asegurarse un usuario que envía un mensaje en un sobre digital cifrado con una clave pública que supuestamente pertenece a un destinatario llamado "Juan" de que realmente se trata de la clave pública de Juan?

Durante mucho tiempo se han utilizado documentos físicos para lograr la autentificación en la vida diaria. Por ejemplo, cuando extiende un cheque para pagar una compra y el vendedor le pide un documento de identificación, este documento se utiliza para aumentar la confianza del vendedor en que quien extiende el cheque es usted. En este caso, el vendedor confía en que el organismo que emitió el documento de identificación realizó correctamente el trabajo de comprobar su identidad.

Para garantizar la autenticidad de las claves públicas, existen organismos encargados de proporcionar los ***certificados digitales*** (comúnmente conocidos como certificados) como un método seguro para el intercambio de claves públicas en redes no seguras.

## 2.3.- Certificados digitales

Un certificado es un conjunto de datos que identifican completamente una entidad y que una entidad emisora de certificados (CA) emite sólo después de haber comprobado la identidad de dicha entidad. El conjunto de datos incluye la clave criptográfica pública proporcionada a la entidad. Cuando el remitente *firma* un mensaje con su clave privada, el destinatario del mensaje puede utilizar la clave pública del remitente (recuperada del certificado enviado con el mensaje o disponible en cualquier parte del servicio de directorio) para comprobar que el remitente es quien afirma ser.

Los certificados digitales son documentos virtuales que autentican a las personas y a las entidades en la red. El uso de certificados en una red es más complejo que el uso de un documento físico porque la mayoría de las partes comunicantes no se conocen físicamente. Por tanto,

se necesita un método o protocolo para lograr un alto nivel de confianza a falta de una comprobación física. Además, en una red no segura es más fácil interceptar mensajes y presentar identidades falsas. Para evitar estos problemas, los protocolos de seguridad que utilizan las técnicas criptográficas hacen más difícil, si no imposible, que una persona falsifique un certificado y presente una identidad falsa.

### 2.3.1.- Certificación digital

Un primer objetivo de un certificado digital es confirmar que la clave pública contenida en un certificado es la clave pública que pertenece a la persona o entidad para la que se emitió el certificado. Por ejemplo, una entidad emisora de certificados (CA) puede firmar digitalmente un mensaje especial (conocido como información de certificado) que contiene el nombre de un usuario (en este caso "Alicia") y su clave pública, de forma que cualquier persona pueda comprobar que el mensaje de información del certificado fue firmado por la CA. Por tanto, se confirma la confianza en la clave pública diseñada para "Alicia".

La implementación típica de la certificación digital comprende un algoritmo de firma para firmar el certificado. El proceso implica los pasos siguientes:

1. Alicia envía una petición de certificado que contiene su nombre y su clave pública a una CA.

2. La CA crea un mensaje especial *m* a partir de esta petición, que constituye la mayor parte de los datos del certificado. La CA firma el mensaje con su clave privada y obtiene una firma separada *sig*. La CA devuelve el mensaje *m* y la firma *sig* a Alicia. Ambas partes componen el certificado.
3. Alicia envía el certificado a Juan, que expresa su confianza en la clave pública.

4. Juan comprueba la firma *sig* mediante la clave pública de la CA. Si la firma se comprueba, se acepta la clave pública diseñada para Alicia.

Al igual que ocurre con una firma digital, cualquier persona puede comprobar, en cualquier momento, que la entidad emisora de certificados (CA) firmó el certificado, sin tener acceso a información privilegiada.

En este escenario se asume que Juan conoce la clave pública específica de la CA. La clave pública se puede obtener de una copia del certificado de la CA, que contiene la clave pública.

Puesto que los certificados tienen un período de validez, es posible que el certificado caduque y deje de ser válido. Un certificado sólo es válido durante el período de tiempo especificado por la CA que lo emitió. El certificado contiene información acerca de la fecha de comienzo y de caducidad. Si un usuario intenta obtener acceso a un servidor seguro mediante un certificado caducado, el software de autentificación del servidor rechazará automáticamente la petición de acceso. Los usuarios pueden renovar los certificados antes de la fecha de caducidad para evitar esta situación.

También es posible que la CA revoque los certificados por otras razones. Para controlar esta situación, la CA mantiene una lista de certificados revocados. Esta lista se llama lista de revocación de certificados (CRL) y está disponible para que los usuarios de la red determinen la validez de un certificado dado.

### 2.3.2.- Jerarquías de entidades emisoras de certificados

En las grandes empresas compuestas por múltiples unidades pequeñas es frecuente que cada unidad administre sus propios recursos en la intranet corporativa. Cada unidad debe hacer cumplir las directivas por las que se concede a los solicitantes el acceso a los recursos de la intranet.

Es posible proporcionar a estas unidades la capacidad de establecer directivas y emitir certificados por sí mismas al permitirles ser *entidad emisora de certificados*, cada una con su propio servidor de entidad emisora de certificados (CA). La organización principal debe supervisar atentamente la proliferación de múltiples CA en una intranet para que no se produzca un abuso de autoridad.

El abuso de autoridad se puede impedir mediante una *jerarquía de entidades emisoras de certificados (CA)*. La jerarquía de CA comienza con una entidad emisora de certificados definitiva llamada *raíz*. La entidad emisora de certificados raíz certifica los servidores de CA de la organización principal para hacer cumplir la seguridad y controlar todo el sistema. En las organizaciones grandes puede haber muchas capas de servidores CA para que la jerarquía se pueda desplegar por todas las unidades de la organización principal. Por ejemplo, la CA raíz certificaría la CA de primer nivel, que, a su vez certificaría la CA de segundo nivel, como se muestra en el diagrama siguiente.

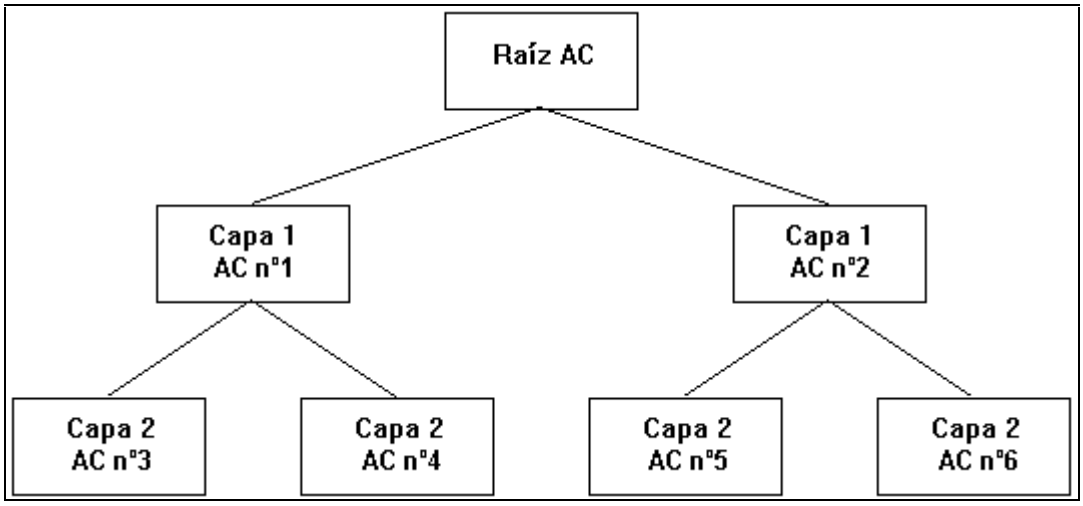



**Figura 5: Jerarquía de entidades emisoras de certificados**

El uso de una jerarquía de CA proporciona a las grandes empresas la flexibilidad necesaria para administrar las directivas y conceder certificados en todo el sistema de certificación compuesto por múltiples entidades emisoras de certificados. Una jerarquía de CA permite administrar un sistema de certificación desde un único punto de control. Por ejemplo, la entidad emisora de certificados raíz podría utilizar una administración de claves basada en hardware para que una CA subordinada específica se certifique con la mayor seguridad posible.

Cuando se transmite a través de una red un certificado emitido por una CA de Nivel 1 o de Nivel 2, el destinatario debe comprobar que el nivel superior ha certificado la emisión de la CA y que este nivel, a su vez, esté certificado por uno superior, hasta que exista una cadena de entidad emisora de certificados entre la CA de nivel más bajo y la CA raíz. Por ejemplo, en el diagrama anterior, se podría comprobar que cada CA #1 certificó cada CA #4 y que CA raíz certificó CA #1.

Si por alguna razón una CA de nivel más bajo administra mal la emisión de certificados, la entidad emisora de certificados raíz puede revocar el certificado del servidor pertinente. Esto deja sin validez efectiva a los certificados emitidos por la CA de nivel inferior sin que afecte a otros certificados emitidos en la organización principal.

# 3.- Protocolo SSL

## 3.1.- Qué es SSL

SSL (Secure Sockets Layer) fue diseñado y propuesto en 1994 por Netscape Corporation. La actual versión, SSL v3.0, se encuentra ampliamente extendido en Internet. En su estado actual proporciona cifrado de datos, autentificación de servidores, integridad de mensajes y, opcionalmente, autentificación de cliente para conexiones TCP/IP.

## 3.2.- Como funciona SSL

El rasgo que distingue a SSL de otros protocolos para comunicaciones seguras, como el S-HTTP, es que se ubica en la pila OSI entre los niveles de transporte (TCP/IP) y de aplicación (donde se encuentran los conocidos protocolos HTTP, FTP, SMTP, etc.). Gracias a esta característica, SSL resulta muy flexible, ya que puede servir para securizar potencialmente otros servicios además de HTTP para web.

SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple DES, RC2, RC4 o IDEA, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen de él y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea descubierta por un atacante en una transacción dada, no sirva para descifrar otras futuras. MD5 o SHA se pueden usar como algoritmos de resumen digital (hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad.

Durante el protocolo SSL, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes fases:

1. La **fase Saludo**, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autentificación. El navegador le informa al servidor de los algoritmos disponibles. Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.
2. La **fase de autentificación**, en la que el servidor envía al navegador su certificado x 509v3 que contiene su clave pública y solicita a su vez al cliente, su certificado X-509v3 (Sólo si la aplicación exige la autentificación de cliente).
3. La **fase de creación de clave de sesión,** en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la de sesión para cifrar los datos intercambiados. Posteriormente haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la pública del servidor que extrajo de su certificado

en la fase 2. Posteriormente ambos generarán idénticas claves de sesión a partir de la maestra generada por el navegador.

4. Por último, la **fase Fin**, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido una vez finalizada esta fase, ya se puede comenzar la sesión segura.


**Figura 6: Pasos seguidos por el protocolo SSL para crear un canal seguro**

De ahí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre los servidores web y los clientes (los navegadores) a través del cual se intercambiará cifrada la información relevante, como el URL y los contenidos del documento solicitado, los contenidos de cualquier formulario enviado desde el navegador, las cookies enviadas desde el navegador al servidor y viceversa y los contenidos de las cabeceras HTTP.

Existen una serie de desventajas al utilizar exclusivamente SSL para llevar adelante ventas por Internet:

- Por un lado, SSL ofrece un canal seguro para el envío de números de tarjeta de crédito, pero carece de capacidad para completar el resto del proceso comercial verificar la validez del número de tarjeta recibido, autorizar las transacciones con el banco del cliente, y procesar el resto de la operación con el banco adquiriente y emisor.
- Por otro lado, es importante recalcar que SSL sólo garantiza la confidencialidad e integridad de los datos en tránsito, ni antes ni después. Por lo tanto, si se envían datos personales al servidor, entre ellos el ya citado número de tarjeta de crédito, el número de la seguridad social, el DNI, etc., SSL, solamente asegura que mientras viajan desde el navegador hasta el servidor no serán modificados ni espiados. Lo que el servidor haga con ellos, está ya más allá de la competencia de este protocolo. Los datos podrían ser manipulados irresponsablemente o caer en manos de un atacante que asaltará el servidor con éxito.
- Además, SSL permite realizar ataques sobre servidores de comercio creados deficientemente con el fín de averiguar números de tarjeta reales.
- Por último, y quizá más importante, debido a la limitación de exportación del gobierno de los Estados Unidos sobre los productos criptográficos, las versiones de los navegadores distribuidas legalmente mas allá de sus fronteras operan con nada más que 40 bits de clave, frente a los 128 o 256 bits de las versiones fuertes. Claves tan cortas facilitan los ataques por búsqueda exhaustiva de claves, pudiéndose descifrar mensajes cifrados en estas condiciones tan desfavorables en cuestión de horas o días, dependiendo de los recursos informáticos disponibles.

Dado que SSL es un protocolo seguro de propósito general, que no fue diseñado para el comercio en particular, se hace necesaria la existencia de un protocolo específico para el pago. Éste existe y se conoce como SET.

# 4.- Protocolo SET

## 4.1.- Qué es SET

Secure Electronic Transaction (SET), en español, Transacción Electrónica Segura, es una especificación diseñada con el propósito de asegurar y autenticar la identidad de los participantes en las compras abonadas con tarjetas de crédito en cualquier tipo de red en línea incluyendo Internet.

El comercio electrónico en Internet y otras redes públicas pone de manifiesto algunos aspectos críticos:

1. La demanda de los consumidores para acceder de forma segura al comercio y otros servicios es muy alta.
2. Los comerciantes quieren métodos simples y de coste contenido para manejar las transacciones electrónicas.
3. Las instituciones financieras requieren de los suministradores de software soluciones competitivas en precio, manteniendo altos niveles de calidad.
4. Las sociedades de medios de pago, administradoras de tarjetas y propietarios de marca necesitan diferenciar el comercio electrónico sin afectar significativamente sus infraestructuras.

SET se desarrolla para dar respuesta a estos y otros factores críticos dentro de la estrategia de implantación del comercio electrónico en Internet.

El papel de las sociedades de medios de pago y sus instituciones financieras es crucial para establecer especificaciones abiertas que permitan:

- Proporcionar **confidencialidad** en las comunicaciones.
- **Autentificar** a las partes involucradas.
- Garantizar la **integridad** de las instrucciones de pago.
- **Autentificar** la identidad del usuario y el comerciante.

## 4.2.- Participantes en el sistema de pago SET

- **Comprador o Titular de la tarjeta** (cardholder): Es el poseedor de la tarjeta de crédito. Un comprador usa una tarjeta de pago que ha sido emitida por una entidad emisora.
- **Entidad Emisora** (Issuer): Es una institución financiera que emite una tarjeta para el cliente, extiende su crédito y es responsable de la facturación.
- **Comerciante** (merchant): El comerciante vende productos, servicios o información a cambio de un pago electrónico. Un comerciante que acepta tarjetas de pago debe tener una relación con una entidad receptora (banco adquiriente).

- **Entidad Receptora o banco adquiriente** (Acquirer): Es una entidad financiera que establece una cuenta con el comerciante y procesa los pagos con tarjetas autorizadas.
- **Pasarela de pagos** (Payment Gateway): Mecanismo mediante el cual se procesan y autorizan las transacciones del comerciante. La pasarela puede pertenecer a una entidad financiera (adquiriente) o a un operador de medio de pago.
- **Redes de medios de pago**: Proporciona servicios adicionales operando la infraestructura de telecomunicaciones sobre las que se realizan las transacciones.

### 4.3.- Criptografía y certificación en SET . Funcionamiento de SET

SET especifica la consecución de los objetivos antes expuestos por medio del empleo de la **criptografía**. Los procesos que afectan directamente a SET son:

- Envío de la orden de pedido al comerciante, junto con información sobre las instrucciones de pago.
- Solicitud de autorización del comerciante a la institución financiera del comprador.
- Confirmación de la orden por parte del comerciante.
- Solicitud de reembolso del comerciante a la institución financiera del comprador.

Esta es una secuencia de procesos que se distingue poco de la utilizada en el comercio convencional, lo que constituye una de las premisas para su desarrollo. La característica principal es la ausencia del *cara a cara* entre el comerciante y el comprador.

Por tanto, los procesos definidos en SET, dentro de los límites establecidos, son:

- Proporcionar la autentificación necesaria entre compradores, comerciantes e instituciones financieras.
- Garantizar la confidencialidad de la información sensible (número de tarjeta o cuenta, fecha de caducidad, etc...).
- Preservar la integridad de la información que contiene tanto la orden de pedido como las instrucciones de pago.
- Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

Aunque estos aspectos son importantes en cualquier red de transmisión de datos, su vulnerabilidad causa una preocupación mucho mayor cuando se relacionan con Internet, por la facilidad que se tiene para procesar automáticamente grandes volúmenes de información.

¿Cómo se implementan en SET todos los procesos de autentificación, confidencialidad e integridad enunciados anteriormente? Estas definiciones constituyen el núcleo de SET:

- La confidencialidad (no vulnerabilidad de la información conteniendo los datos necesarios para realizar el pago, tales como el número de cuenta o tarjeta y su fecha de caducidad) se alcanza mediante la **encriptación de los mensajes**.
- La integridad de los datos conteniendo las instrucciones de pago, garantizando que no han sido modificados a lo largo de su trayecto, se consigue mediante el uso de **firmas digitales**.

- La autentificación del comprador, como usuario legítimo de la tarjeta o cuenta sobre la que se instrumenta el pago del bien o servicio adquirido, se consigue mediante la emisión de **certificados** y la generación de **firmas digitales**.
- La autentificación del comerciante, garantizando que mantiene una relación comercial con una institución financiera que acepta el pago mediante tarjetas, se consigue mediante la emisión de **certificados** para el comerciante y las correspondientes **firmas digitales**.

Los algoritmos criptográficos empleados en SET para los procesos de encriptación, emisión de certificados y generación de firmas digitales son de doble naturaleza. Por un lado, se define un algoritmo de **clave privada**, de fortaleza contrastada y excelente rendimiento: DES (Data Encryption Standard), en uso desde 1977, aunque útilmamente se le han detectado problemas. Por otro lado, se hace imprescindible contar con un algoritmo que permita el intercambio de claves en una red pública, con total seguridad, entre múltiples participantes sin ninguna relación previa; un algoritmo como el descrito se define de **clave pública**, y el escogido para SET fue diseñado por Rivest, Shamir y Adleman, cuyas iniciales componen su nombre: RSA.

Esencialmente, cada algoritmo criptográfico empleado en SET permite la implementación de una función determinada. DES se emplea para garantizar la confidencialidad de los mensajes transmitidos; RSA se emplea para garantizar la integridad de los datos y la autenticidad de los participantes. RSA desempeña todavía una función adicional, posible gracias a su definición como algoritmo de clave pública (también se conoce como algoritmo asimétrico, por emplear dos claves diferentes, una para la encriptación y otra para la desencriptación): permite la distribución y utilización de una clave secreta entre participantes sin ninguna relación previa y, lo que es más importante, sobre canales no asegurados.

**Clave privada vs. clave pública**

DES, como algoritmo de clave privada (este tipo de algoritmos también recibe la denominación de algoritmos simétricos) requiere que las partes intervinientes en un proceso de encriptación/desencriptación compartan la misma clave. Esto plantea, como cabe suponer, problemas de distribución de claves en entornos no seguros, como es el caso de Internet. Nadie pensaría en distribuir una clave DES mediante un mensaje de correo electrónico. Incluso algunos canales "menos públicos" como puede ser el correo ordinario o el teléfono son sumamente vulnerables. Solo la entrega en mano garantiza que una clave no ha sido descubierta durante la distribución.

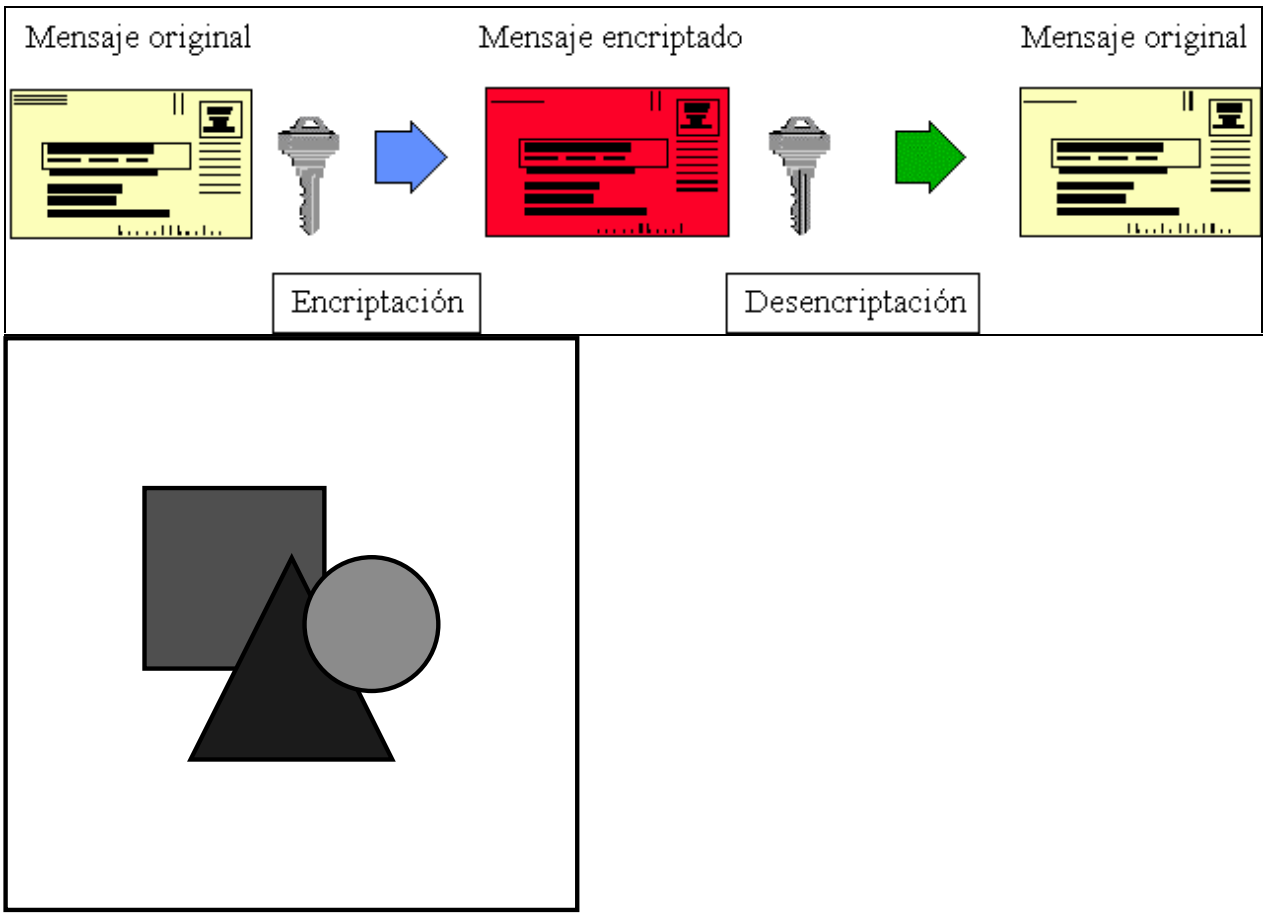
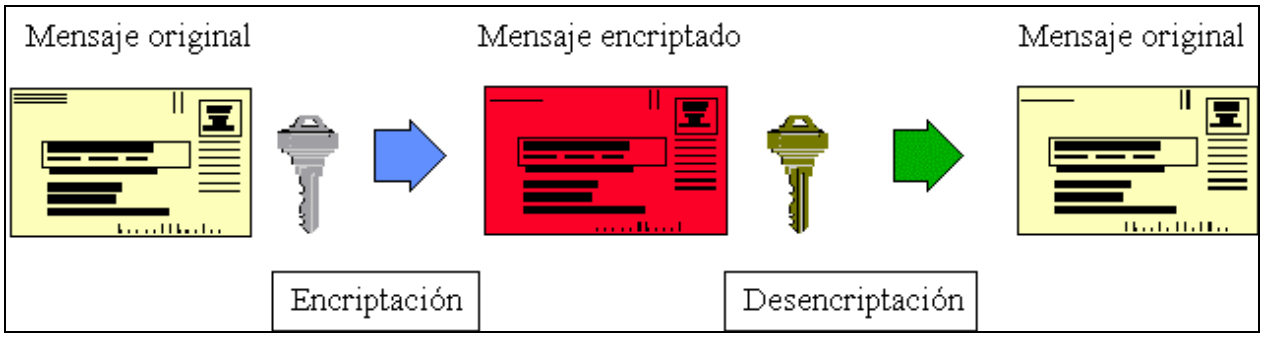



**Figura 7: Algoritmos de clave privada**

Los algoritmos de clave pública, como RSA, están sustentados en una base matemática tal que cada una de las partes intervinientes dispone de un par de claves: una se denomina **clave pública**, y está destinada a ser distribuida libremente. Es más, cuanto más ampliamente se haya distribuido esta clave, más garantías existen de que no es posible la "usurpación de personalidad". La otra clave, la **clave privada** será conocida solamente por su legítimo propietario, y debe ser custodiada con el mismo celo con que se haría para una clave DES. La base matemática aludida anteriormente hace que mientras que un mensaje puede ser encriptado con la clave pública, es necesaria la clave privada para su desencriptación.



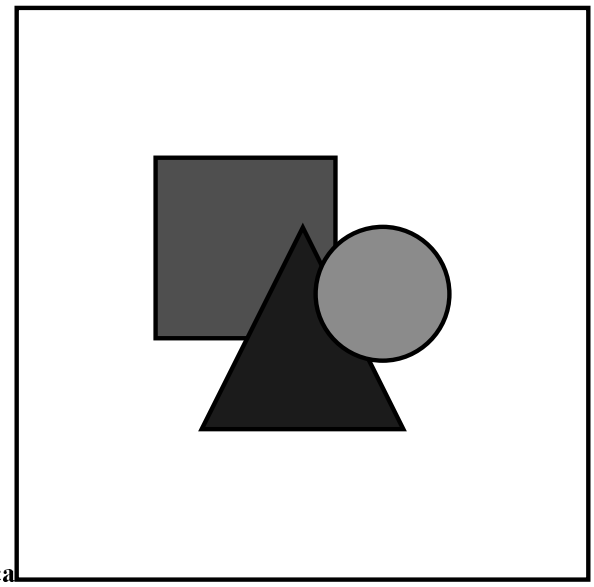


**Figura 8: Algoritmos de clave pública**

El mensaje original es encriptado con la clave pública del destinatario; este podrá obtener el mensaje original después de aplicar su clave privada al mensaje cifrado. Se resuelve así el problema de la distribución de claves sobre canales no seguros. Aparecen sin embargo nuevos problemas. Uno de ellos, es el relativo a la "usurpación de personalidad".

Veamos en que consiste. Juan y Elena son usuarios de un sistema de criptografía basado en RSA (por ejemplo, **PGP**). Juan obtiene la clave pública de Elena de una página Web generada por esta última. Sin embargo, astutamente, Carlos ha sustituido la clave pública original de Elena por la suya propia. Cuando Juan envía un mensaje a Elena, cifrado con su clave pública, en realidad está utilizando la de Carlos, que puede así intervenir estos mensajes. Para no levantar sospechas, Carlos reenvía el mensaje original a Elena, esta vez con la clave pública original de esta. Para resolver este problema potencial, en el contexto de los sistemas criptográficos de clave pública se ha diseñado la figura de la Autoridad Certificadora (*Certifying Authority*, CA).

**Confidencialidad de los mensajes: Sobres electrónicos.**

En SET, la confidencialidad de los mensajes está soportada primariamente por la utilización de claves simétricas para cifrar el contenido de los mismos. Estas claves, generadas de forma aleatoria, son cifradas a su vez con la clave pública del par de claves asimétricas del destinatario. La unión de la clave simétrica cifrada, junto con los datos del mensaje cifrados con esta, se conoce como **sobre electrónico** (*digital envelope*).

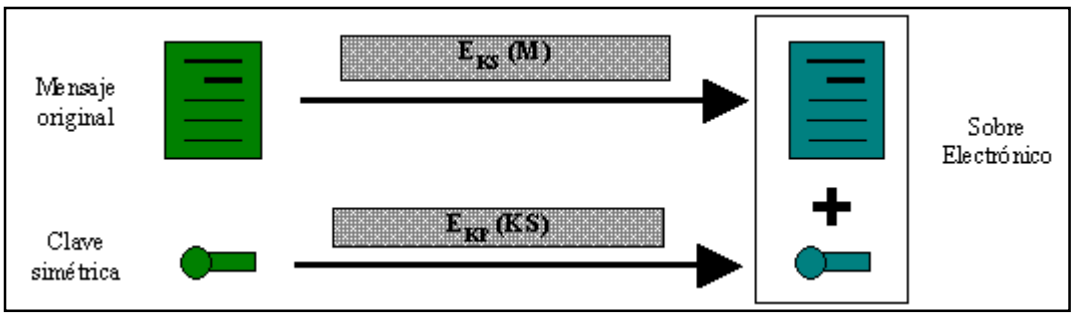



**Figura 9: Sobre Electrónico en SET**

A su recepción, el destinatario utiliza la clave privada de su par de claves asimétricas para descifrar la clave simétrica, que a su vez permitirá descifrar los datos del mensaje.

La generación de las claves simétricas aleatorias es un proceso de gran importancia. La programación y métodos empleados para ello deben garantizar que tales claves no serán inferidas del contenido del mensaje ni del entorno en el que se han producido.

**Integridad y autenticidad de los mensajes: Firmas electrónicas**

En SET la integridad, como garantía de que el contenido de los mensajes no ha sido alterado de forma fraudulenta, y la autenticidad, que garantiza que las partes intervinientes en el proceso lo hacen de forma legal y representan quien dicen ser, se basan en la generación de firmas electrónicas (*digital signatures*).

La firma electrónica se basa en las relaciones matemáticas entre las claves pública y privada del algoritmo asimétrico utilizado. Así, un mensaje cifrado con una de las claves solo puede ser descifrado con la otra. El remitente de un mensaje cifra su contenido con su propia clave privada; el destinatario puede descifrarlo con la correspondiente clave pública y determinar así la autenticidad del origen del mensaje.

Para garantizar la integridad del contenido del mensaje, y al mismo tiempo acelerar el tratamiento del mismo, se incorpora un proceso adicional consistente en generar un valor único y representativo de los datos. Este proceso, denominado literalmente como *digestión del mensaje* (*message digest*) consiste en hacer pasar los datos a través de una función irreversible (*one-way hash function*), como MD5, que produce un *destilado* del original que es único para un contenido dado. Es computacionalmente casi imposible producir el mismo destilado a partir de dos mensajes diferentes. El algoritmo empleado en SET produce un destilado de 160 bits y es tal que el cambio de un solo bit en el mensaje original produce, en promedio, el cambio de la mitad de los bits del producto.


**Figura 10: Firma Electrónica en SET**

El "destilado" del mensaje se cifra ahora con la clave privada del remitente, y el resultado se añade al mensaje original que se envía, constituyendo la firma electrónica del mismo.

El destinatario del mensaje descifra el "destilado" con la clave pública del remitente, aplica la misma función al mensaje original y compara ambos resultados. Si son iguales, la integridad y autenticidad del mensaje son correctas. Si el proceso de descifrado no es satisfactorio, el remitente no puede ser autenticado; si el "destilado" generado no es coincidente con el extraído de la firma electrónica, se ha producido una modificación en el contenido del mensaje.

SET emplea dos pares distintos de claves asimétricas: uno para las funciones de intercambio de las claves simétricas aleatorias y otro para las funciones de firma electrónica. Es importante recordar que las claves asimétricas operan en forma inversa en el intercambio de claves y en la firma electrónica.

Veamos a continuación un ejemplo de como se envían los mensajes encriptados entre dos usuarios, y como se usan los distintos tipos de claves:

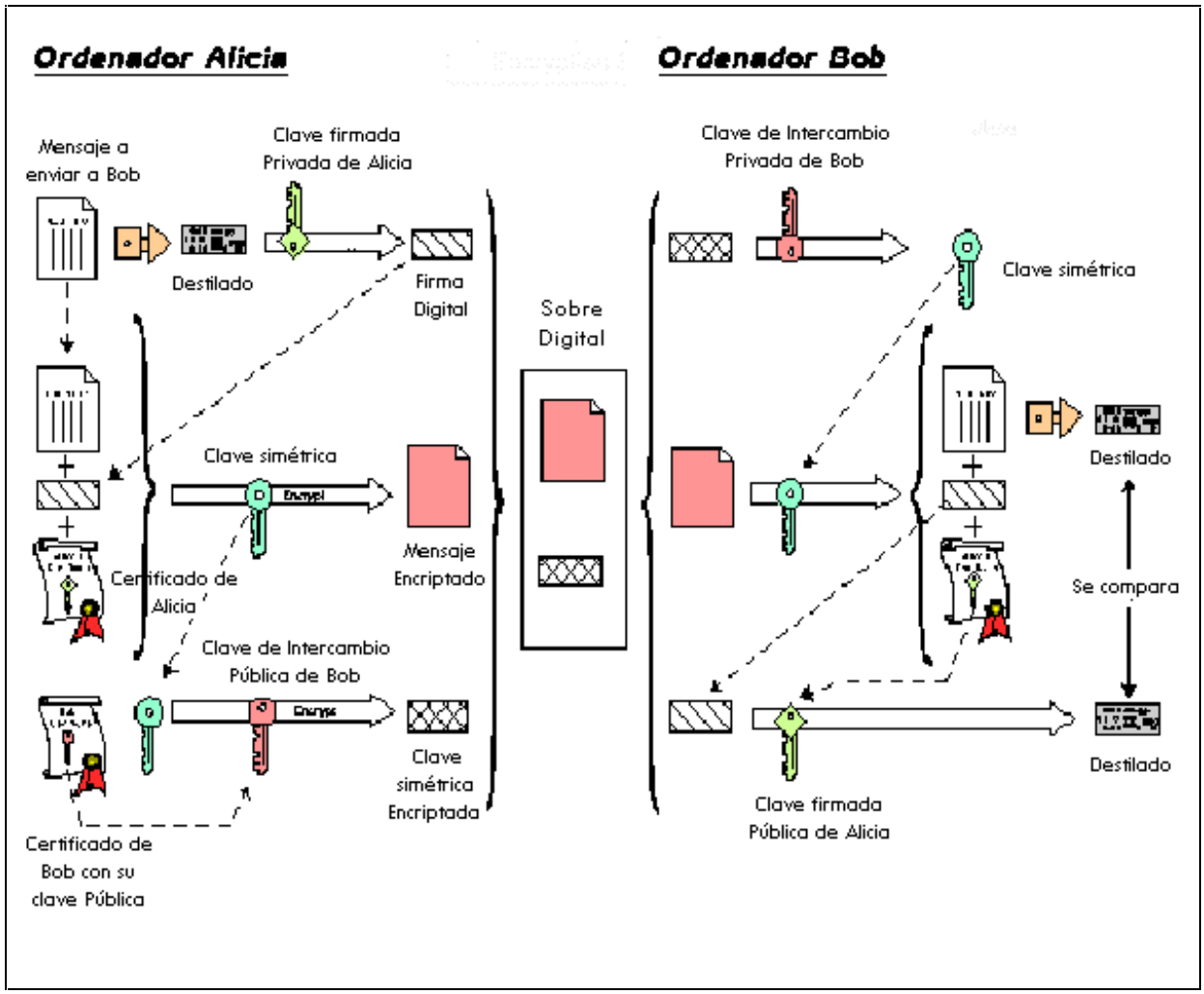



**Figura 11: Pasos que se realizan en la encriptación**

Este proceso descrito en el ejemplo de la figura anterior se repite constantemente en las transacciones bajo SET. Todos los envíos de información entre los distintos participantes se realizan de esta manera.

## Certificados de Autenticidad

SET es un protocolo que nace para su aplicación en redes abiertas y sobre canales no seguros. Por ello se tienen previstos desde el comienzo los procedimientos y procesos necesarios para garantizar la autenticidad y legitimidad de los usuarios que participen en un circuito de comercio electrónico.

La firma electrónica garantiza la autenticidad del remitente y la integridad de los datos contenidos en el mensaje. Sin embargo aún es posible que se haya producido una suplantación de la identidad del remitente, si su clave pública ha sido alterada de forma fraudulenta por una tercera persona. Una posible solución para el problema de la suplantación de identidad es el intercambio de claves públicas mediante canales seguros. Sin embargo esto no es viable en la mayoría de los casos y especialmente cuando los participantes no guardan una relación anterior, como en el comercio electrónico.

Una alternativa al intercambio seguro de claves es la utilización de **certificados de autenticidad** emitidos por entidades de confianza para todas las partes intervinientes. Tales entidades se denominan **Autoridades Certificadoras** (*Certificate Authorities, CA*). Un certificado de autenticidad contiene la clave pública de la persona o entidad para la que se emite, junto con infor-

mación propia, y todo ello firmado electrónicamente por la CA. Como la clave pública de la CA está ampliamente distribuida, no existe riesgo de suplantación de identidad.

Para cada uno de los agentes participantes en SET, se emite un certificado de autenticidad. En realidad, y dado que SET define la utilización de dos conjuntos de claves asimétricas, cada una de las partes dispone de dos certificados de autenticidad, uno para el intercambio de claves simétricas y otro para los procesos de firma electrónica.

La emisión y verificación de los certificados de autenticidad está sometida a una jerarquía de confianza, con una autoridad certificadora principal que emite certificados para los niveles inferiores.

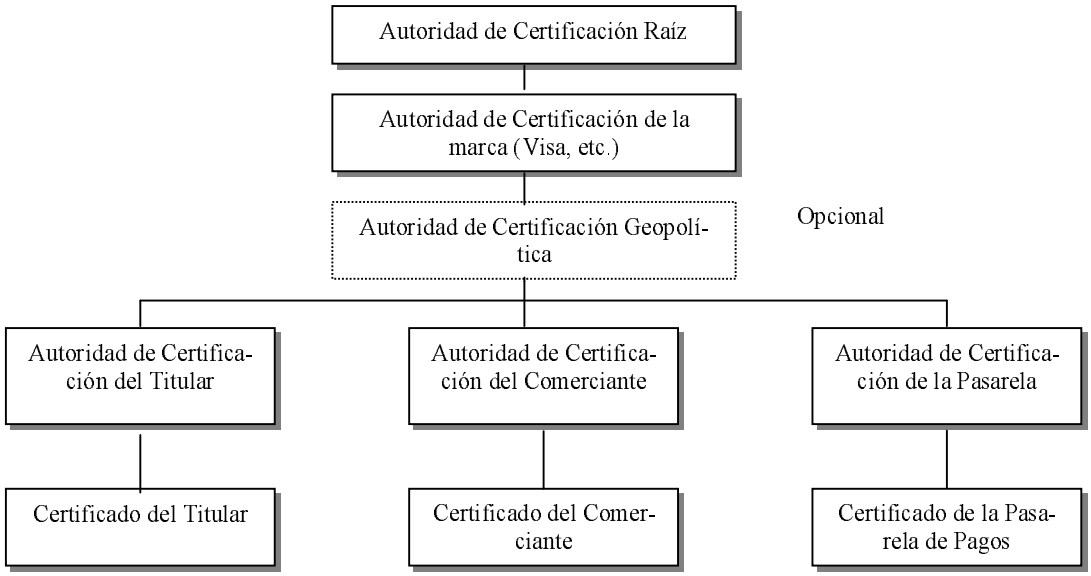



**Figura 12: Jerarquía de confianza**

El seguimiento de este árbol de confianza hacia arriba permite asegurar la autenticidad de un certificado, y por tanto de la clave certificada, para cada nivel dado. Cada certificado está enlazado a la firma del agente participante al que certifica.

La clave de la CA de primer nivel estará disponible para los fabricantes de software, en un certificado auto-firmado. Se han previsto los procesos necesarios para reemplazar la clave original, y para su verificación.

El **comprador** obtiene sus certificados de la entidad financiera que emite las tarjetas con las que opera para realizar las transacciones de comercio electrónico. Para todos los efectos, una vez que la entidad financiera ha identificado debidamente al comprador potencial, los certificados sustituyen, funcionalmente, a las tarjetas.

El **comerciante** obtiene sus certificados de la entidad financiera con la que firma contratos de adhesión para la aceptación de las diferentes tarjetas de crédito y débito emitidas por dicha entidad en nombre del propietario de la marca. Estos certificados sustituyen funcionalmente a las pegatinas que exhiben actualmente los escaparates de los comercios, y que permiten identificar la existencia de una relación comercial con una entidad financiera que les permitirá aceptar pagos con diferentes marcas y tipos de tarjetas. Evidentemente, un comerciante podrá disponer de más de un par de certificados, y tendrá tantos como marcas de tarjetas esté aceptando como medio de pago.

El **acquirer** (entidad financiera del comerciante) debe poseer certificados para poder operar como CA y emitir certificados para los comerciantes. El acquirer obtendrá sus certificados del propietario de la marca de tarjetas.

El **issuer** (entidad financiera del comprador) debe poseer certificados para poder operar como CA y emitir certificados para los compradores. El issuer obtendrá sus certificados del propietario de la marca de tarjetas.

### 4.4.- Fases que componen el comercio electrónico bajo SET

Una transacción SET típica funciona de forma muy parecida a una convencional con tarjeta de crédito y consta de:

1. *Decisión de compra*. El cliente está navegando por la web del comerciante y decide comprar un artículo. Rellenará algún formulario 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 pulsa el botón de Pagar.
2. *Arranque del monedero*. El servidor del comerciante envía una descripción del pedido que despierta a la aplicación monedero del cliente.
3. *El cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante*. La aplicación monedero 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 monedero del cliente genera una firma dual, que permite juntar 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 éstas, pero no al la información del pedido. Este mecanismo, reduce el riesgo de fraude, ya que ni el comerciante llega a conocer el número de tarjeta, ni el banco sabe los hábitos de compra del cliente.
4. *El comerciante envía la petición de pago a su banco*. 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 una 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. *El banco adquiriente valida al cliente y al comerciante y obtiene una autorización del emisor del cliente*. El 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.
6. *El emisor autoriza el pago*. 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. *El adquiriente envía al comerciante un testigo de transferencia de fondos*. En cuanto el banco del comerciante recibe una respuesta de autorización del emisor, genera y

firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, que se hace llegar al comerciante.

8. *Éste envía un recibo al monedero 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.
9. *Más adelante, el comerciante usa el 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. A su debido tiempo, el dinero se descuenta de la cuenta del cliente (cargo).

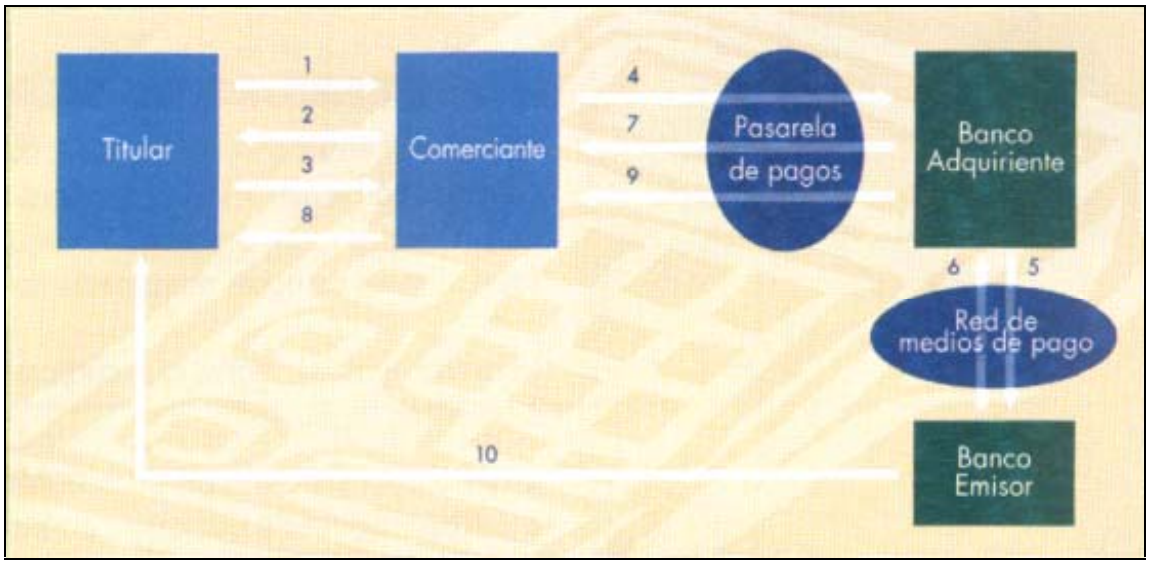



**Figura 13: Pasos del protocolo SET para pagar a través de Internet**

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. En su estado actual, SET solamente soporta transacciones con tarjeta de crédito/débito, y no con tarjetas monedero.

## 4.5.- Elementos necesarios para comprar con SET

Para realizar las compras por Internet pagando mediante el protocolo SET, es necesario hacerse antes con dos elementos:

1. *Un certificado digital SET*: funciona como un carnet digital que puede usar el comerciante para verificar la identidad del titular de la tarjeta a través de la Red. Los certificados SET son emitidos por la misma entidad financiera de la que recibió su tarjeta de crédito. Sirven para asegurarle al comerciante que usted es el legítimo titular de la tarjeta de crédito que va usarse en la compra. Si se desea utilizar más de una tarjeta de crédito, entonces se necesita un certificado digital distinto para cada una, pues es el propio banco o entidad financiera que proporciona la tarjeta de crédito la que emite el certificado.

2. *Un monedero digital (wallet)*: que permite a los compradores almacenar información acerca de sus datos personales para el envío de las mercancías compradas, así como información de pago, como número de tarjeta de crédito y banco emisor. Debe ser compatible con SET, ya que constituye el medio a través del cual se transmite la información de su certificado digital en los pagos por Internet.

## 4.6.- Elementos necesarios para vender con SET

Para poder vender por Internet bajo el control del protocolo SET es necesario:

1. *Un certificado digital* diferente para cada marca de tarjeta de crédito que desee aceptar. Estos certificados sirven un propósito similar al de los certificados de titular de tarjeta, ya que permiten autenticarse como un comerciante válido. Gracias a estos certificados el cliente goza de la misma seguridad que cuando paga con la tarjeta en su tienda física. Los certificados son emitidos por el mismo banco o entidad financiera con las que normalmente gestiona las ventas pagadas con tarjeta.
2. *Una aplicación terminal punto de venta* (POST) compatible con SET en el servidor.

Dado que SET sólo protege la información de pago de los clientes, no el resto de la información que se envía al servidor, es altamente recomendable ofrecer transacciones seguras a través de un canal cifrado con SSL. De esta manera el resto del proceso de compra (como que artículos compran, información demográfica, etc.) se mantiene a salvo de curiosos.

## 4.7.- Flujo de las transacciones en el proceso de pago

En este apartado se describe el flujo de las transacciones y como estas son procesadas por varios sistemas.

SET define una variedad de protocolos de transacción que usan los conceptos de criptografía vistos anteriormente para securizar el comercio electrónico. Este apartado describe las siguientes transacciones :

- Registro del comprador o titular de la tarjeta.
- Registro del comerciante.
- Solicitud de compra.
- Autorización del pago.
- Captura del pago (Cobro).

### 4.7.1.- Registro del comprador

La figura 22 proporciona un resumen a alto nivel del proceso de registro del comprador, mostrándolo en siete pasos fundamentales.

Nota: Nos referiremos al poseedor de una tarjeta de crédito como titular de la tarjeta o comprador. A la Autoridad Certificadora haremos referencia mediante “CA”.

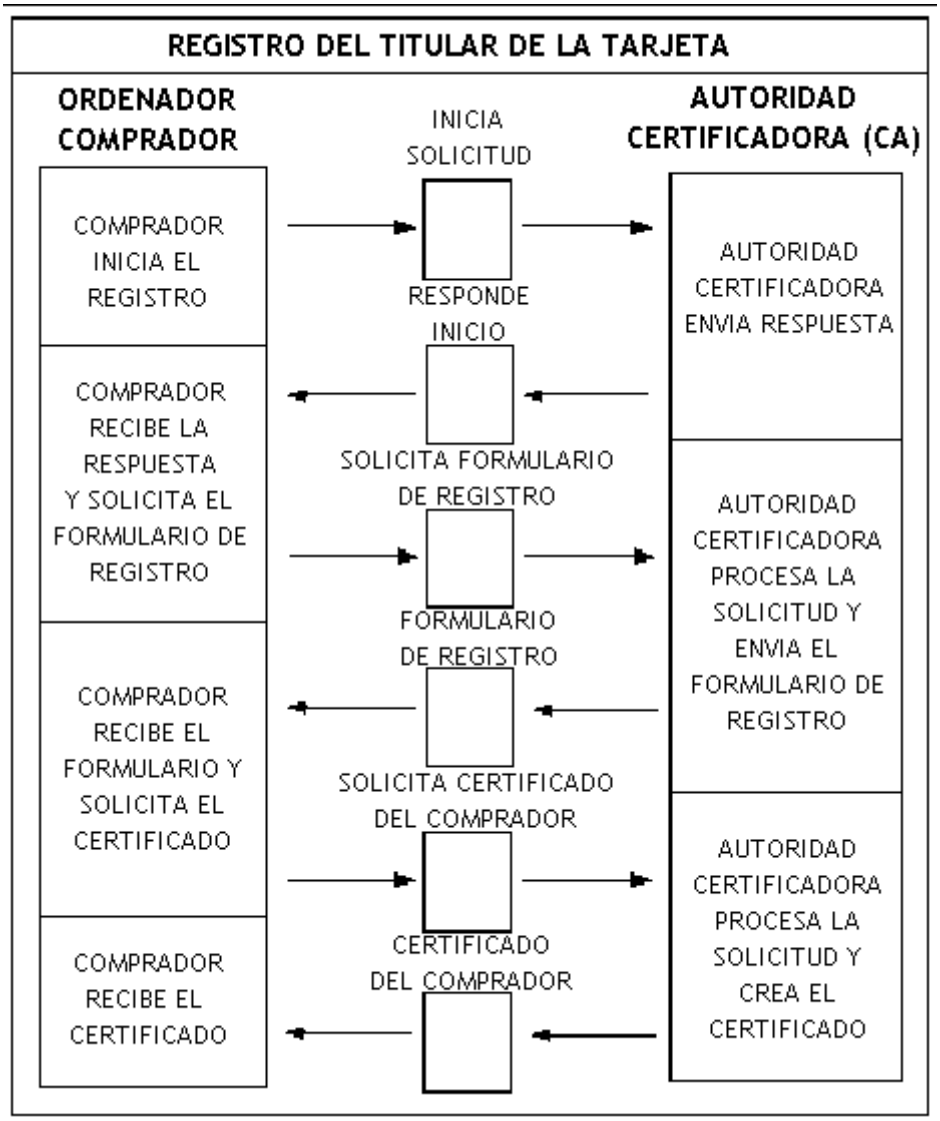



**Figura 14: Registro del comprador**

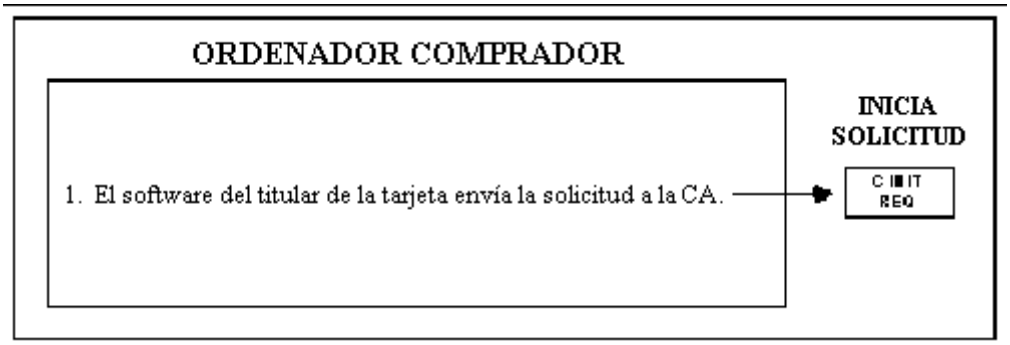
Veamos a continuación en más profundidad como se realiza estos 7 pasos:

**Paso 1: Comprador inicia el Registro.**

El titular de la tarjeta debe registrarse con una Autoridad Certificadora antes de poder enviar mensajes SET al comerciante. Para poder enviar mensajes a la CA, el titular debe tener una copia de clave de intercambio pública de la CA, que se obtiene del certificado de la CA.

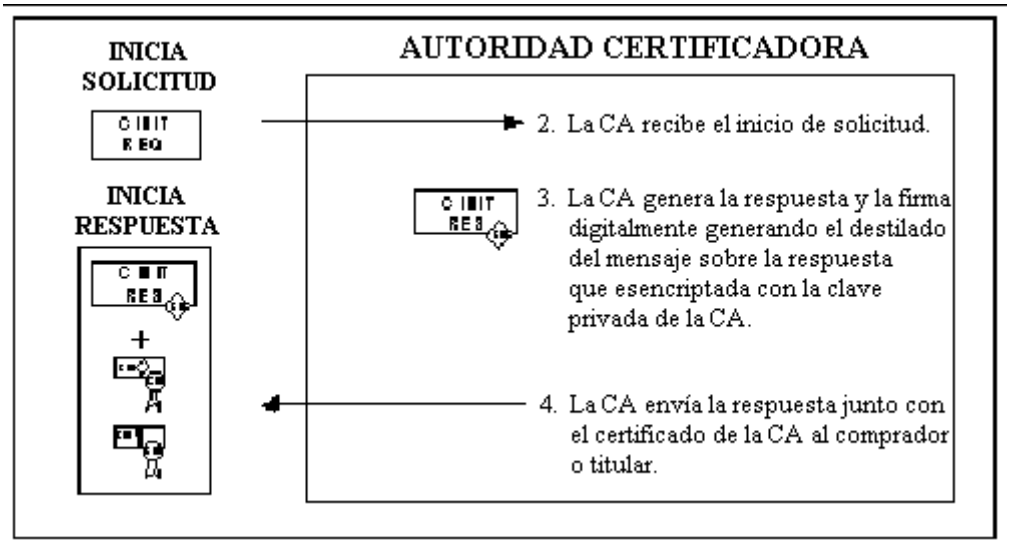
El titular también necesita una copia del formulario de registro de la institución financiera del titular. Para que la CA nos proporcione el formulario de registro, el software del titular debe identificar la entidad financiera emisora a la CA. Para obtener el formulario de registro se requiere dos intercambios entre el software del titular y la CA.

El proceso de registro comienza cuando el software del titular solicita una copia del certificado de la CA.



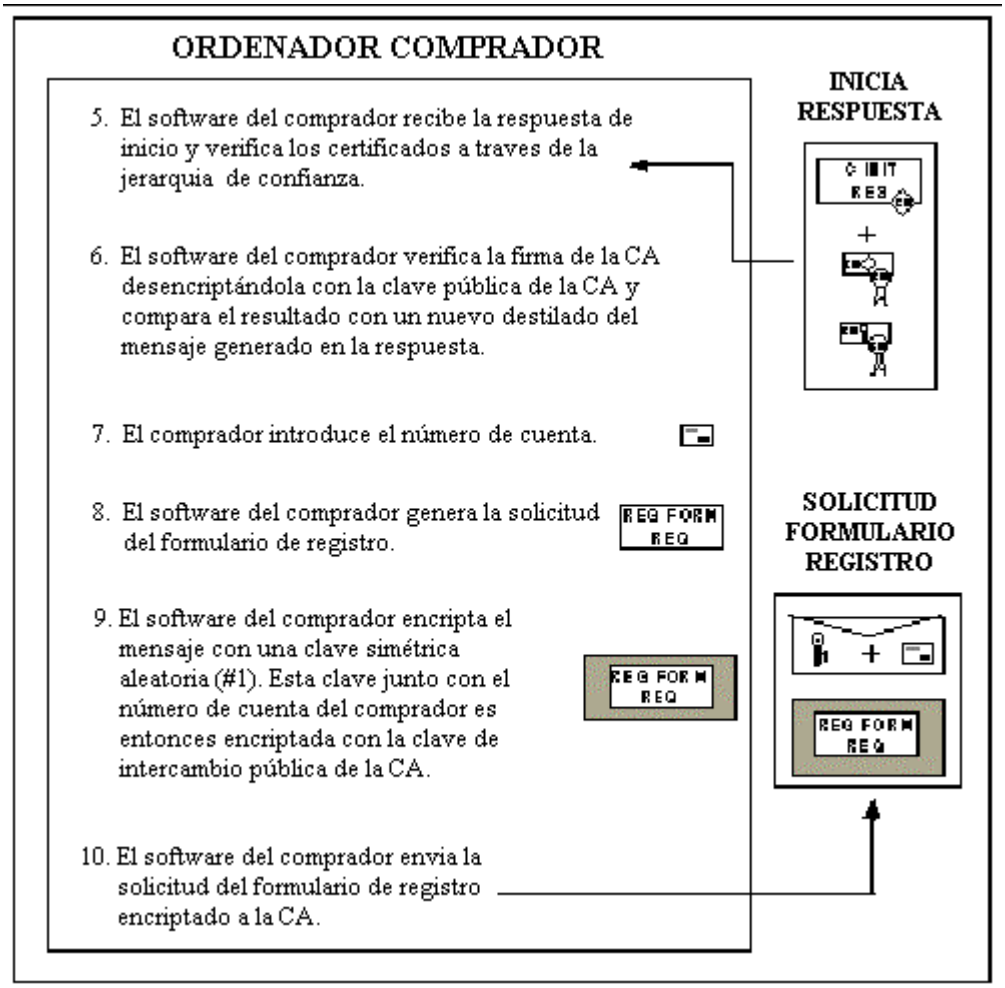

**Paso 2: Autoridad certificadora envía respuesta.**

Cuando la CA recibe la solicitud, esta envía el certificado al comprador. El certificado de la CA proporciona al software del titular todo los necesario para proteger el número de la tarjeta de crédito en la solicitud del formulario de registro.



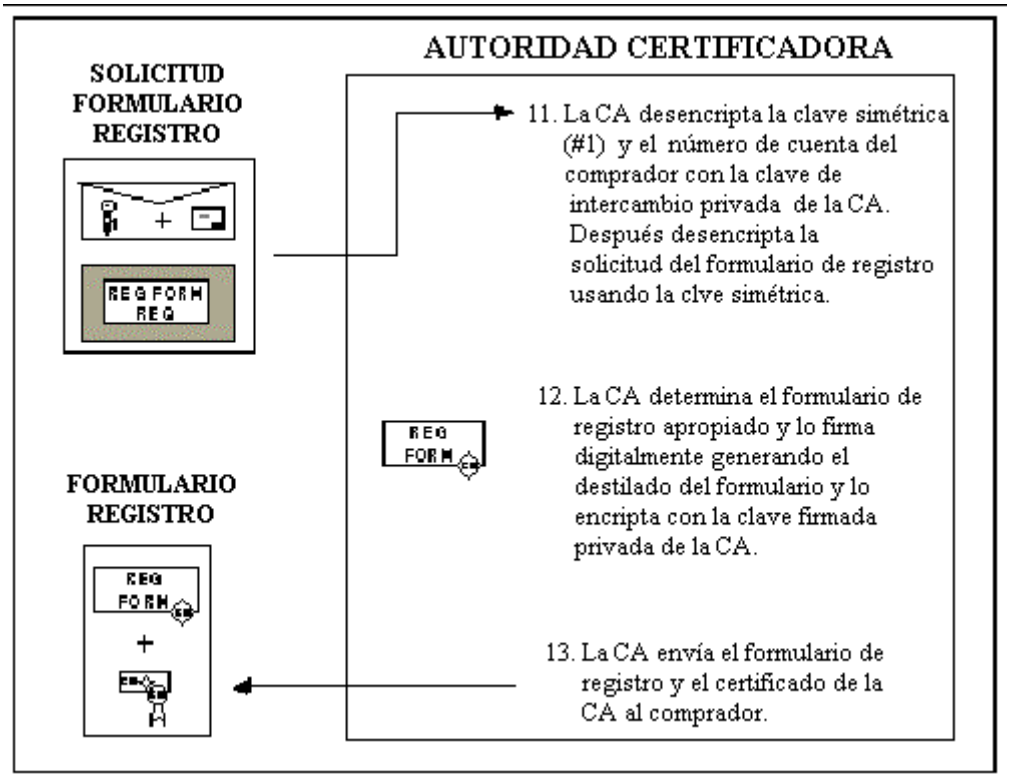

**Paso 3: Comprador recibe respuesta y solicita el formulario de registro.**

Una vez que el software del titular tiene el certificado de la CA, puede solicitar el formulario de registro.



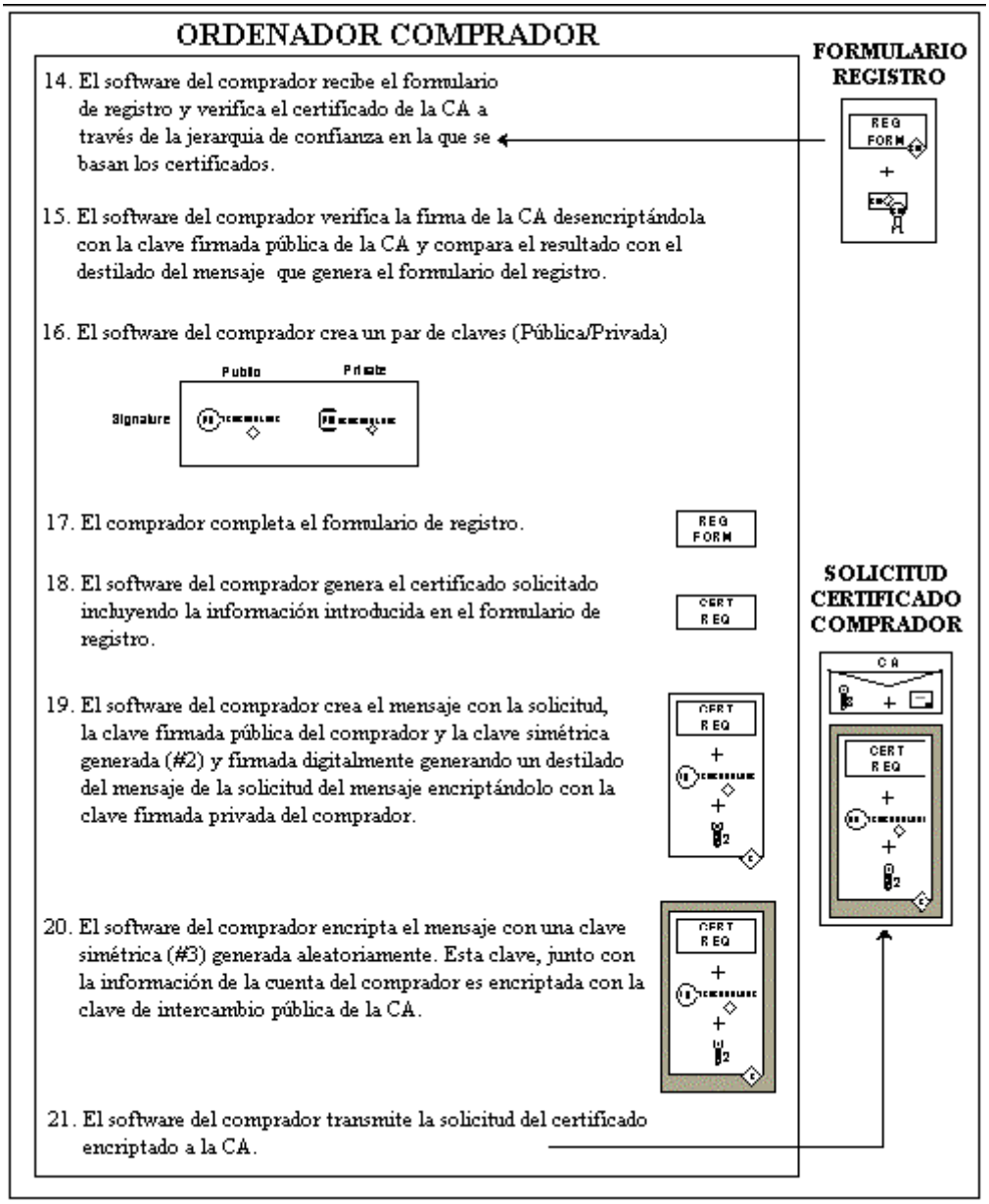

**Paso 4: CA procesa solicitud y envía el formulario de registro**

La CA identifica a la institución financiera del comprador (usando los primeros 6 a 11 dígitos del número de cuenta) y selecciona el formulario de registro apropiado. En algunos casos, la propia institución financiera del titular puede operar como la Autoridad Certificadora.



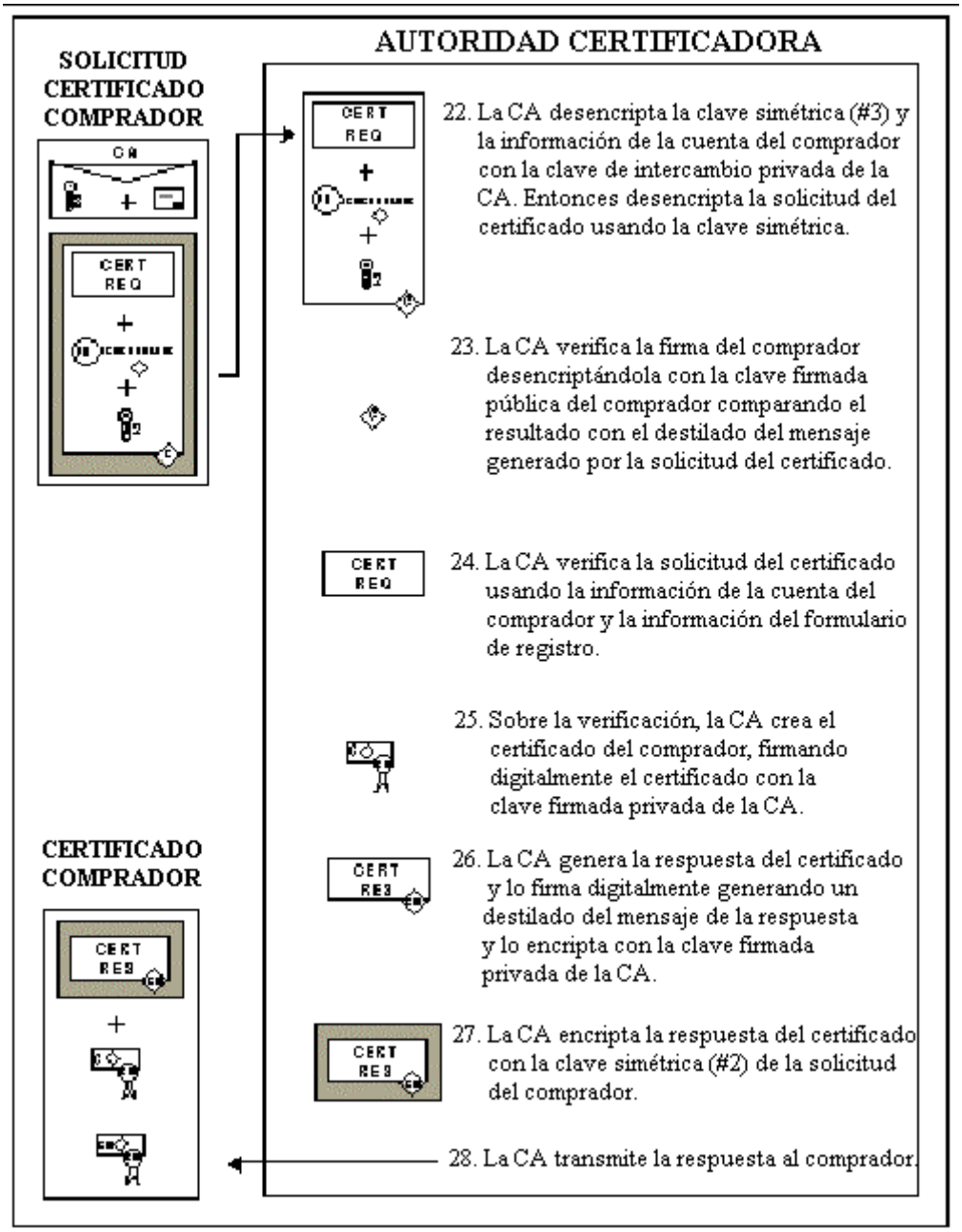

**Paso 5: Comprador recibe el formulario de registro y solicita el certificado**

Para registrar el número de cuenta, el titular rellena un formulario de registro que devolverá a la CA con información como el nombre del titular, fecha de expiración de la tarjeta e información adicional sobre la institución financiera del titular necesaria para juzgar e identificar el certificado solicitado como titular válido.



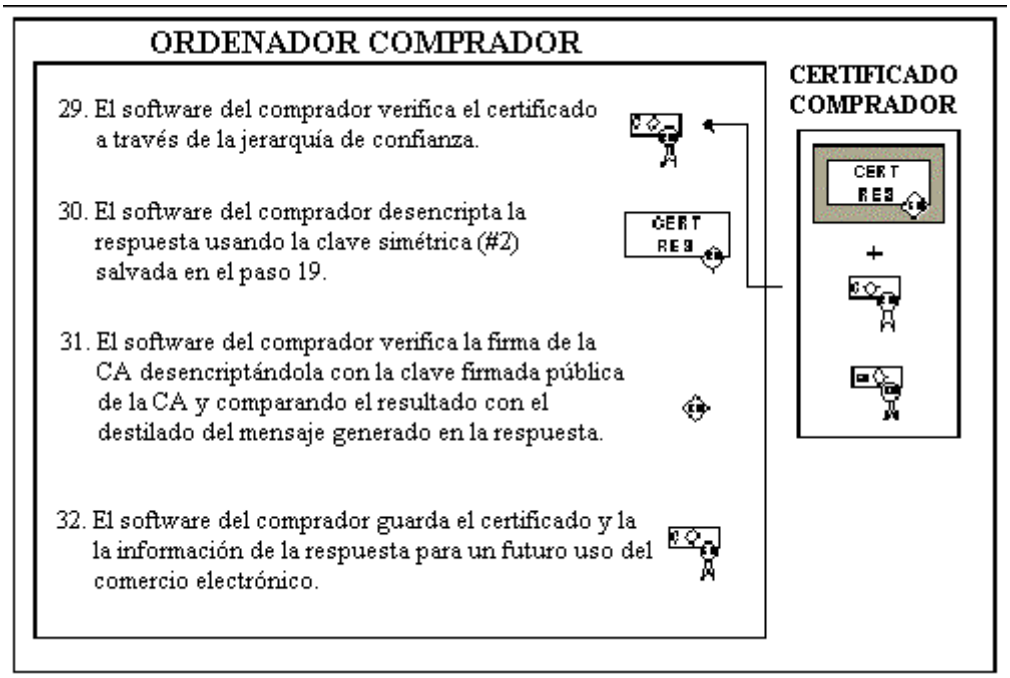

**Paso 6: CA procesa la solicitud y crea el certificado**

Para emitir el certificado, la información de la solicitud de registro debe ser verificada. Primero, la CA genera un número aleatorio que es combinado con el número aleatorio creado por el software del titular y que como resultado da un valor secreto. Este valor secreto es usado para proteger la información del número de cuenta en el certificado del titular. El número de cuenta, la fecha de caducidad y el valor secreto son codificados usando un algoritmo de resumen. El resultado de este algoritmo es guardado en el certificado del titular. El número de cuenta, la fecha de caducidad o el valor secreto no se puede obtener mirando el certificado. A continuación, la CA crea el certificado del titular. El periodo de validez de este certificado será determinado por la política de la CA; aunque normalmente se corresponde con la fecha de caducidad de la tarjeta de crédito, aunque puede expirar antes.




**Paso 7: Comprador recibe el certificado**

El titular recibe el certificado y el software del comprador lo almacena para usarlas en futuras transacciones electrónicas.




### 4.7.2.- Registro del comerciante

La figura 23 proporciona un resumen a alto nivel del proceso de registro del comerciante, mostrándolo en cinco pasos fundamentales.

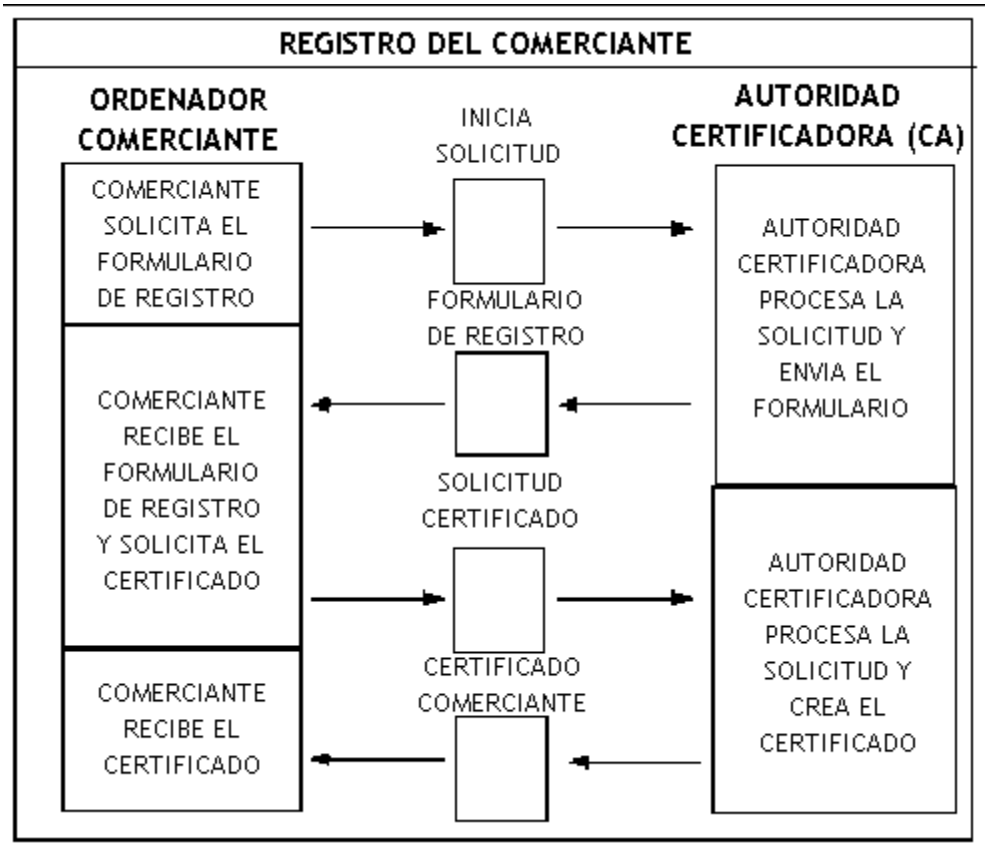
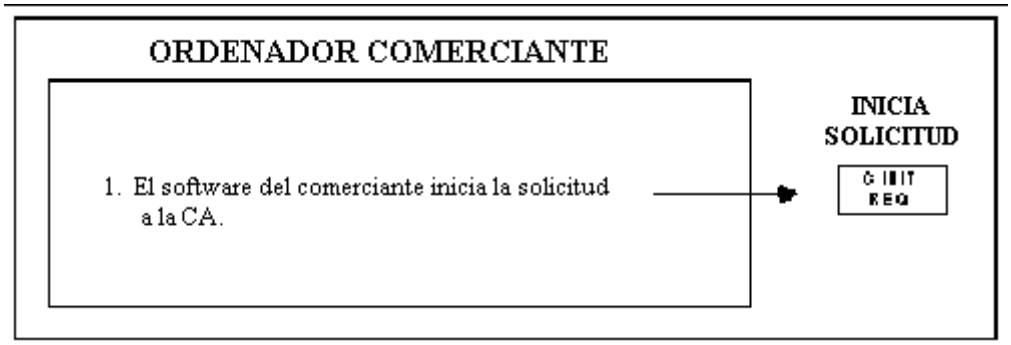



**Figura 15: Registro del comerciante**

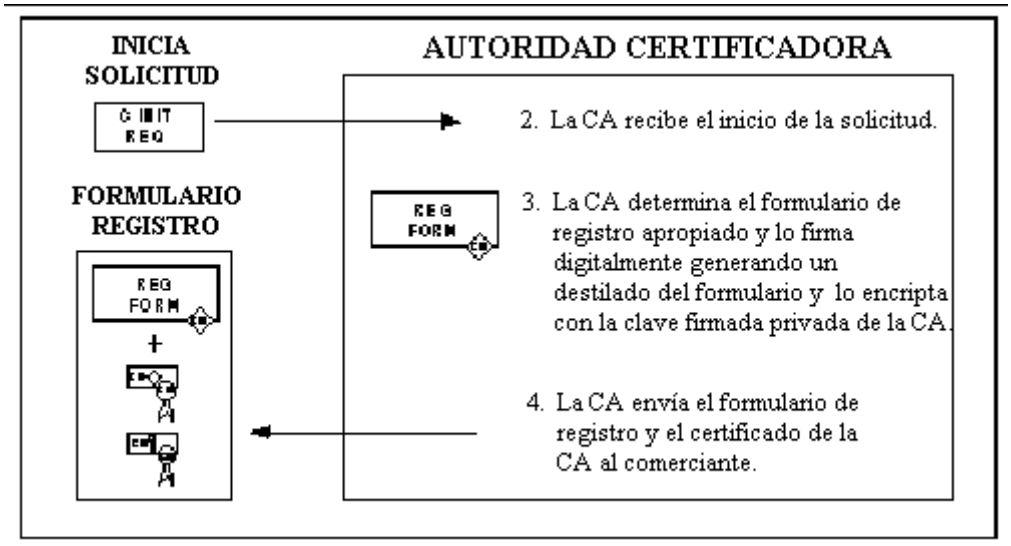
**Paso 1: Comerciante solicita el formulario de registro**

El comerciante debe registrarse en una CA antes de poder recibir instrucciones de pago de un titular o procesar transacciones SET a través de una pasarela de pagos. El comerciante también necesitará una copia del formulario de registro de la entidad financiera del comerciante. El software del comerciante debe identificar la entidad financiera a la CA.




**Paso 2: CA procesa la solicitud y envía el formulario de registro**

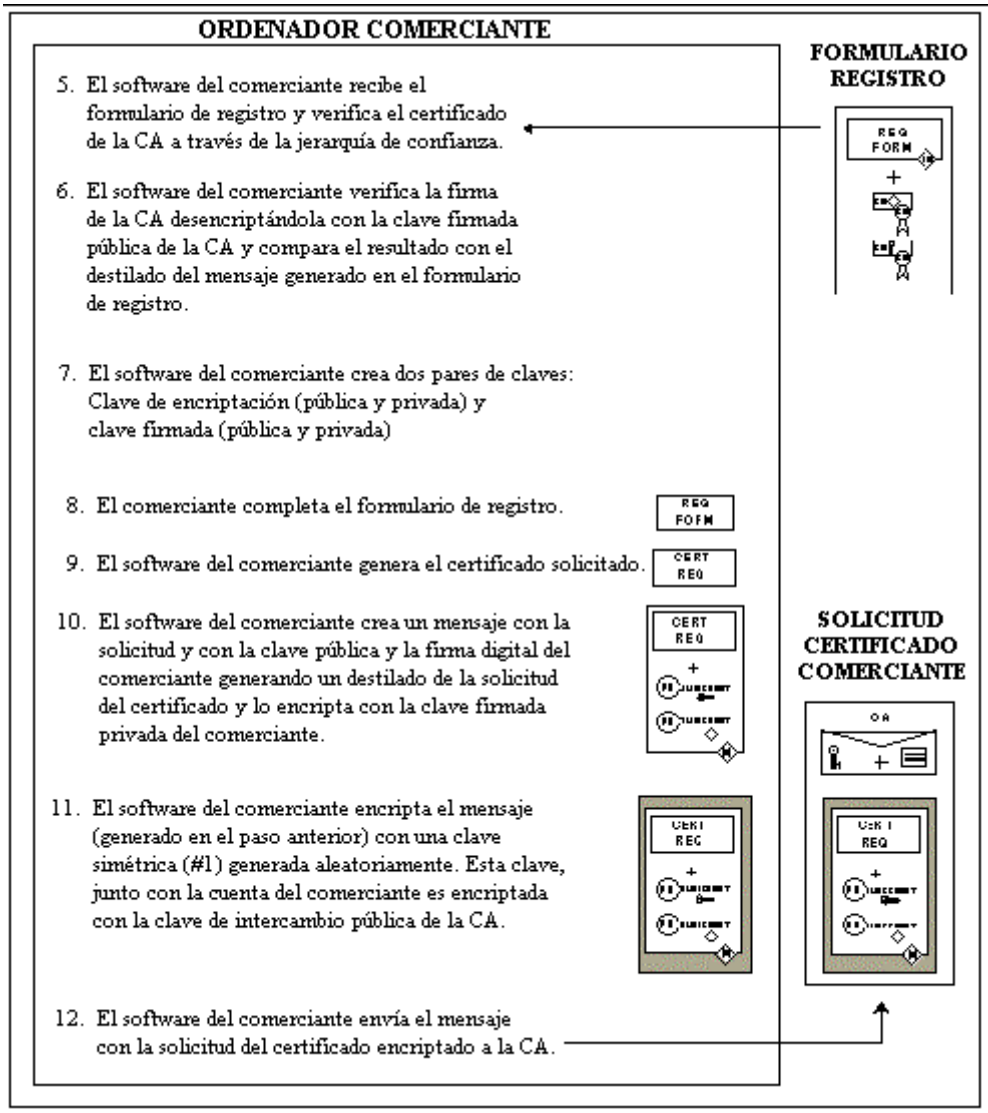
La CA procesa la solicitud y envía el formulario de registro.




**Paso 3: Comerciante recibe el formulario de registro y solicita el certificado**

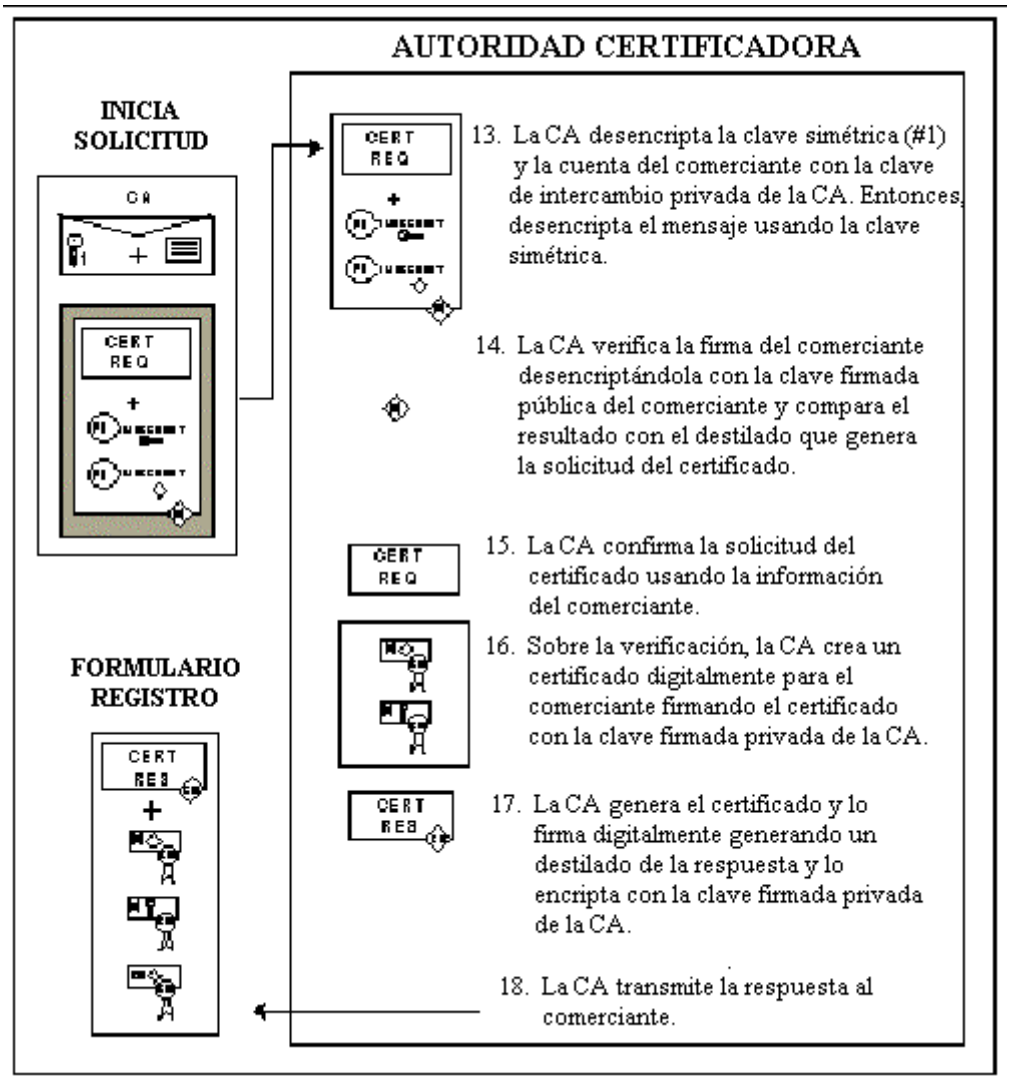
El comerciante debe tener un relación con una entidad financiera que procese las transacciones SET antes de que una solicitud de un certificado pueda ser procesado. El comerciante necesita dos pares de claves pública/privada para usar con SET: clave de intercambio y clave firmada. El software del comerciante genera estos pares de claves si no existen todavía.

Para registrarse, el comerciante debe rellenar un formulario de registro con información como el nombre del comerciante, dirección, e identificación del comerciante.



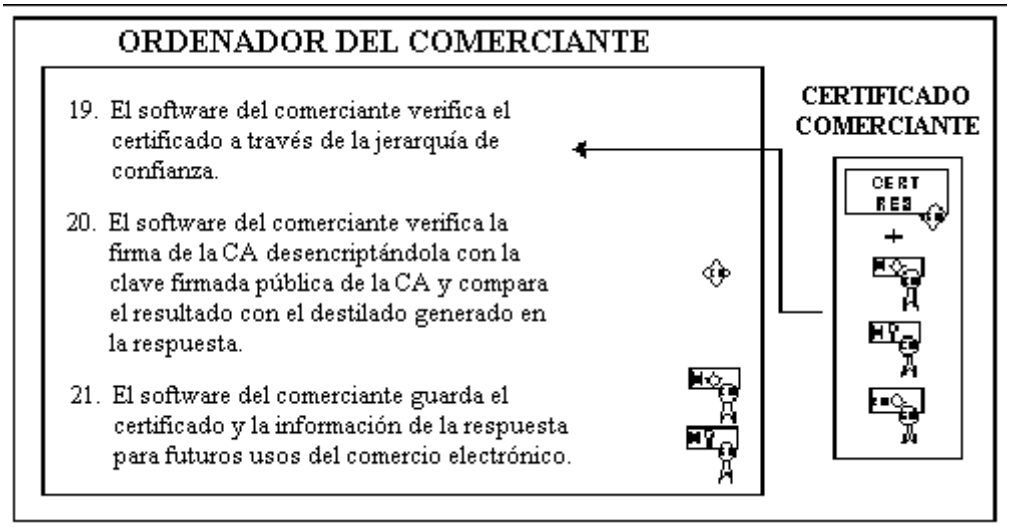

**Paso 4: Autoridad Certificadora procesa la solicitud y crea el certificado**

Cuando la información de registro es verificada, la CA crea el certificado del comerciante. El periodo de validez del certificado lo determina la CA. Normalmente se corresponde con la fecha de expiración del contrato entre el comerciante y la entidad financiera, pero puede expirar antes.




**Paso 5: Comerciante recibe certificados**

El certificado es guardado en el ordenador del comerciante para futuras transacciones.



### 4.7.3.- Solicitud de compra

La figura siguiente muestra los pasos que se siguen en una parte del pedido de la compra que el comprador pide.

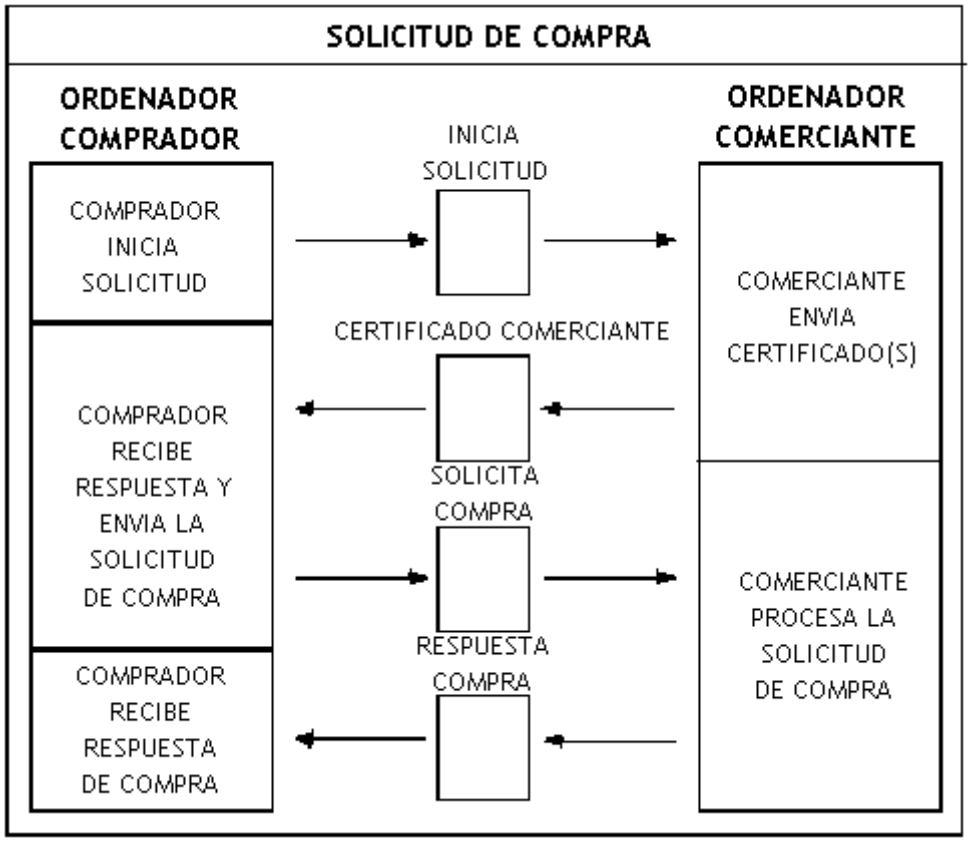
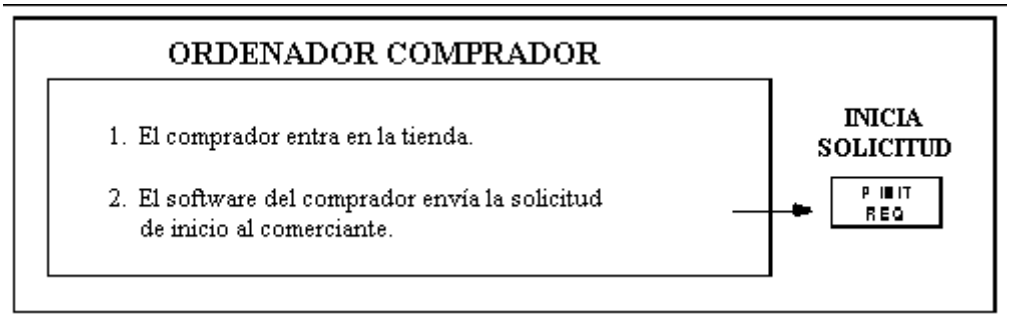



**Figura 16: Solicitud de compra**

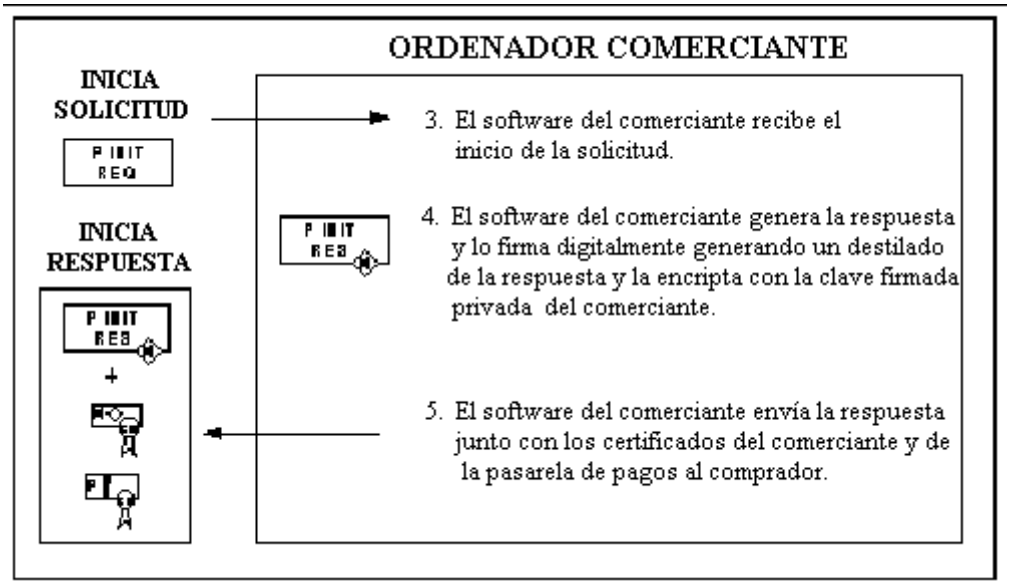
**Paso 1: Comprador inicia solicitud**

El protocolo SET es invocado después de que el titular ha completado la selección y el pedido de la compra.




**Paso 2: Comerciante envía certificados**

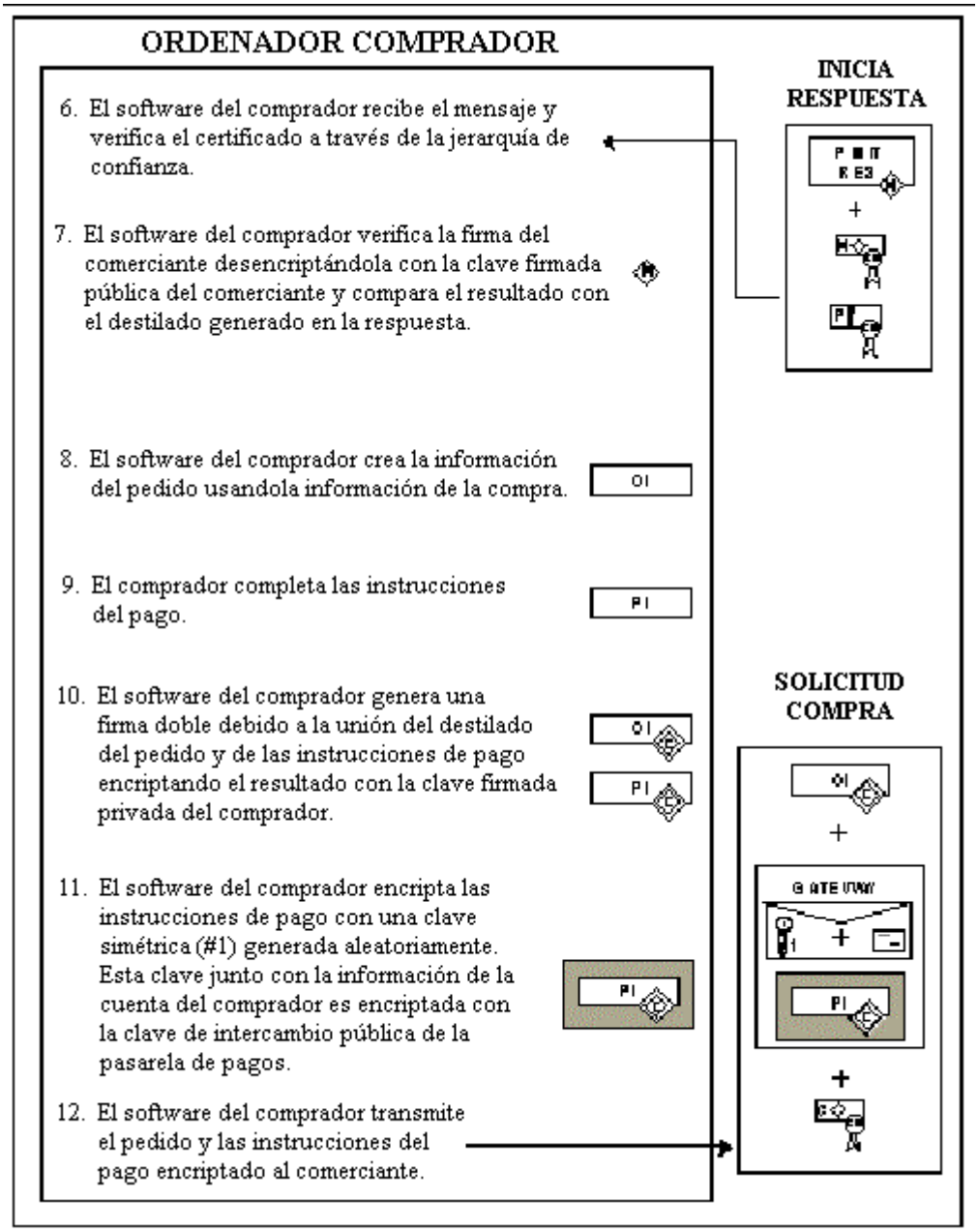
Cuando el comerciante recibe la solicitud, asigna un identificador único a la transacción del mensaje. Entonces, envía los certificados del comerciante y de la Pasarela junto con el identificador de la transacción al comprador.




**Paso 3: Comprador recibe respuesta y envía solicitud de compra**

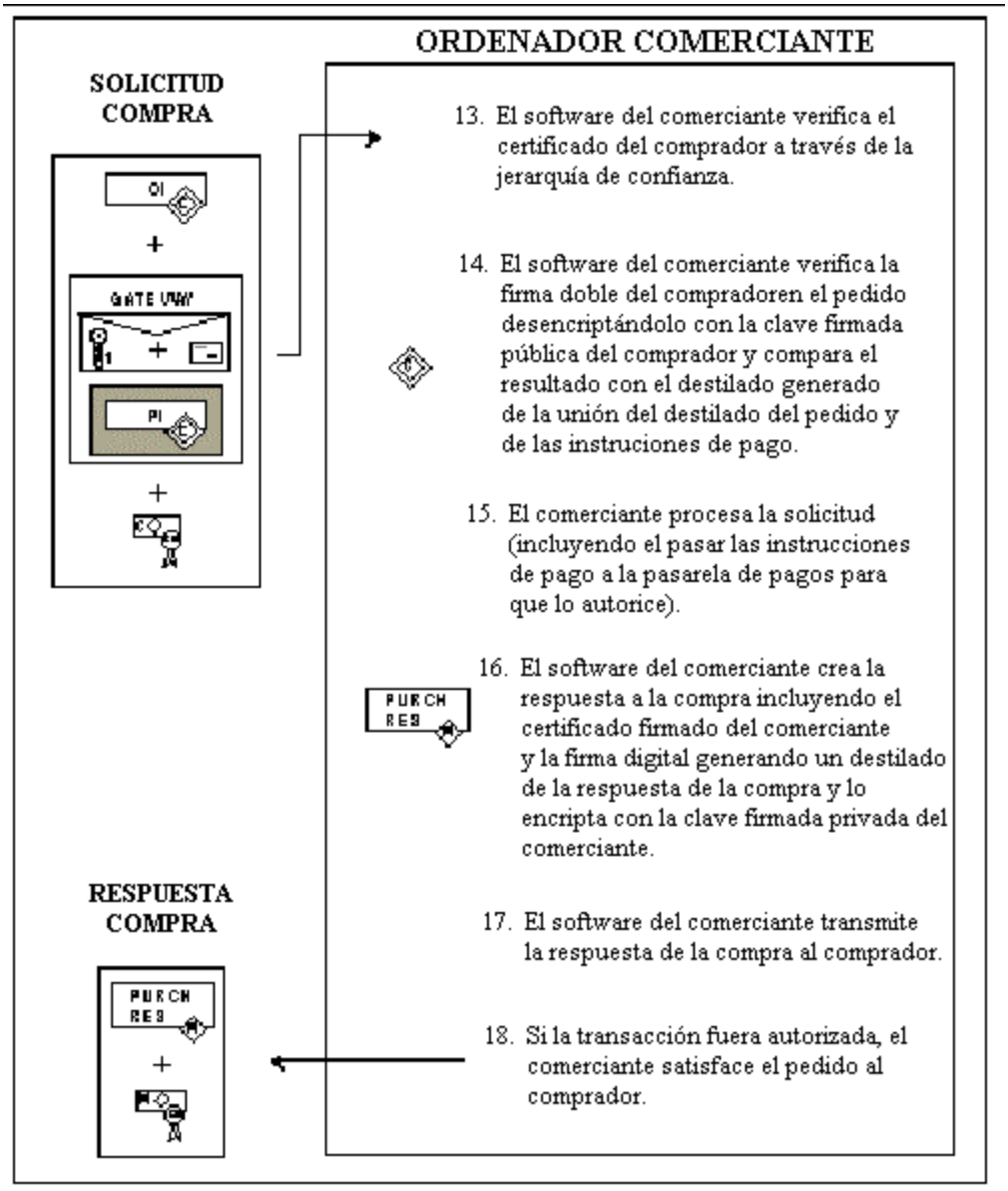
El software del titular crea la información del pedido (OI) y las instrucciones del pago (PI). El software reconoce el identificador asignado a la transacción por el comerciante en la información del pedido y en las instrucciones de pago; este identificador será usado por la Pasarela de Pagos para unirla a las información del pedido y a las instrucciones de pago cuando el comerciante solicite la autorización.

Nota: La información del pedido no contiene datos del pedido como las mercancías (los artículos y las cantidades) o los términos del pedido (como el número de plazos en pagar). Esta información es intercambiada entre el comprador y el software del comerciante durante la fase de compra antes del primer mensaje SET.




**Paso 4: Comerciante procesa la solicitud de compra**

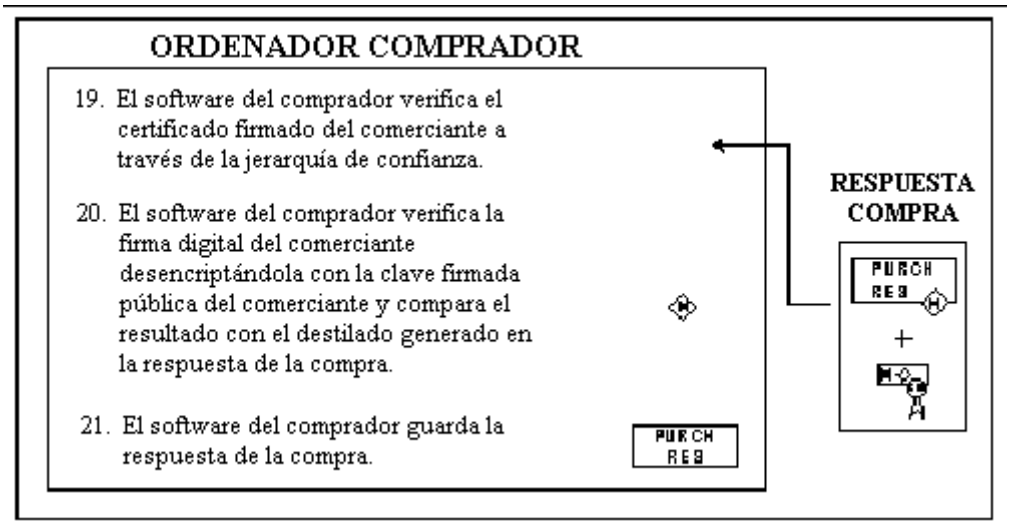
Si la respuesta de la autorización indica que la transacción fue aprobada, el comerciante enviará la mercancía al comprador.




**Paso 5: Comprador recibe la respuesta de la compra**

Finalmente, el software del comprador realiza algunas acciones basadas en el contenido del mensaje de respuesta, como mostrar un mensaje al titular o actualizar una base de datos con el estado del pedido.

El comprador puede determinar el estado del pedido (como si ha sido autorizado o pendiente de pago) enviando un mensaje preguntando por el mismo.




### 4.7.4.- Autorización del pago

La figura siguiente muestra los pasos que se siguen en el proceso de autorización del pago al comerciante.

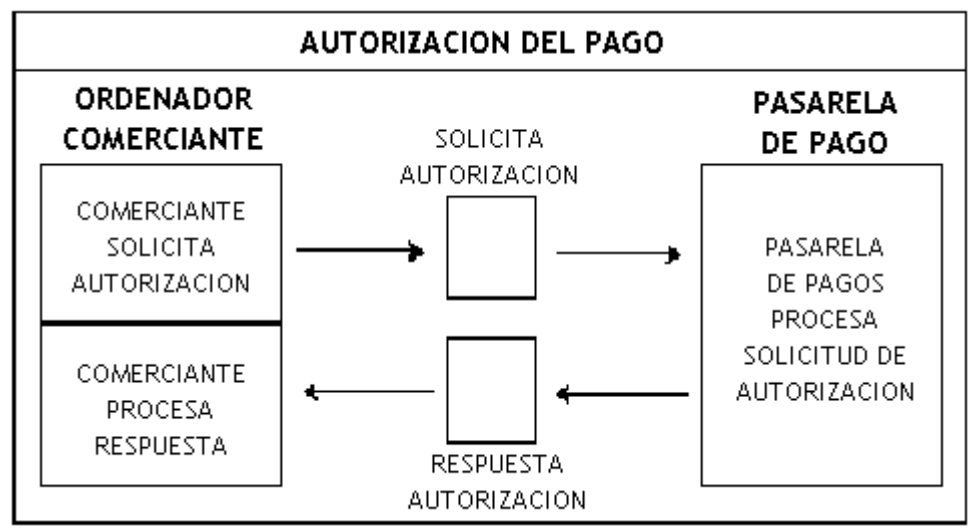
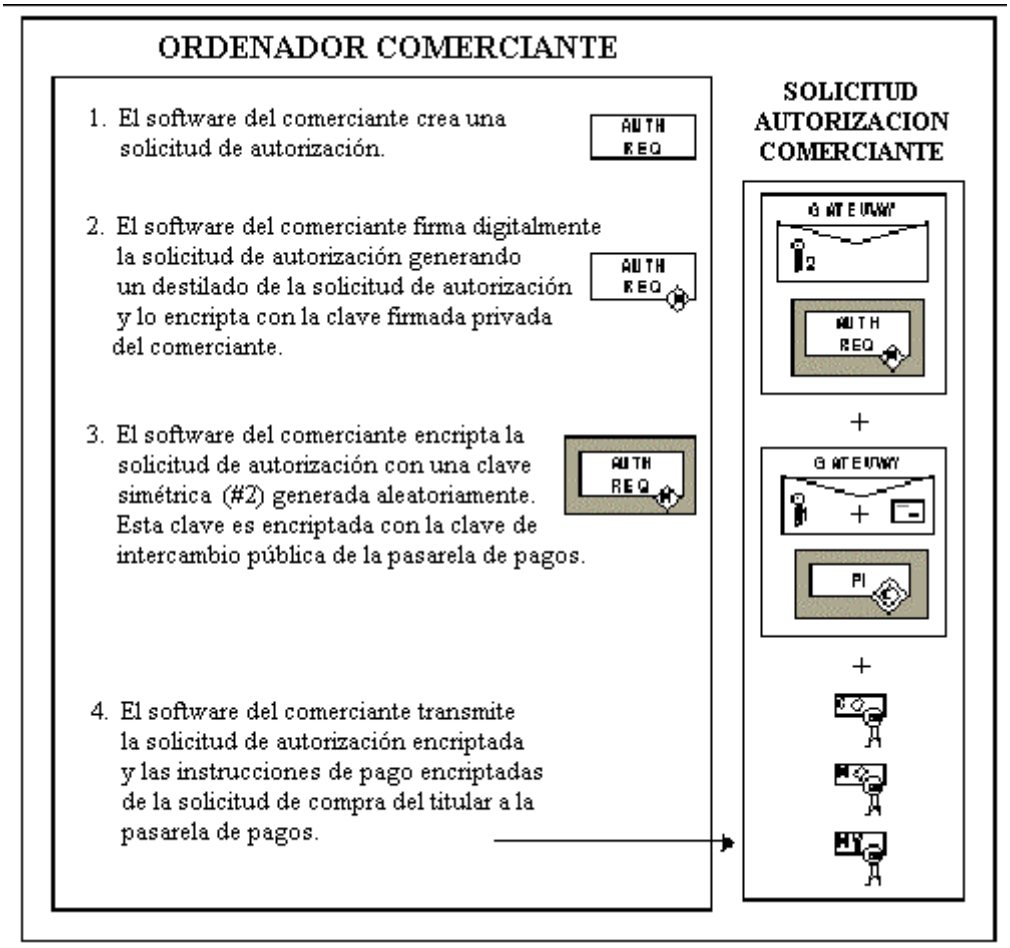



**Figura 17: Autorización del pago**

**Paso 1: Comerciante solicita autorización**

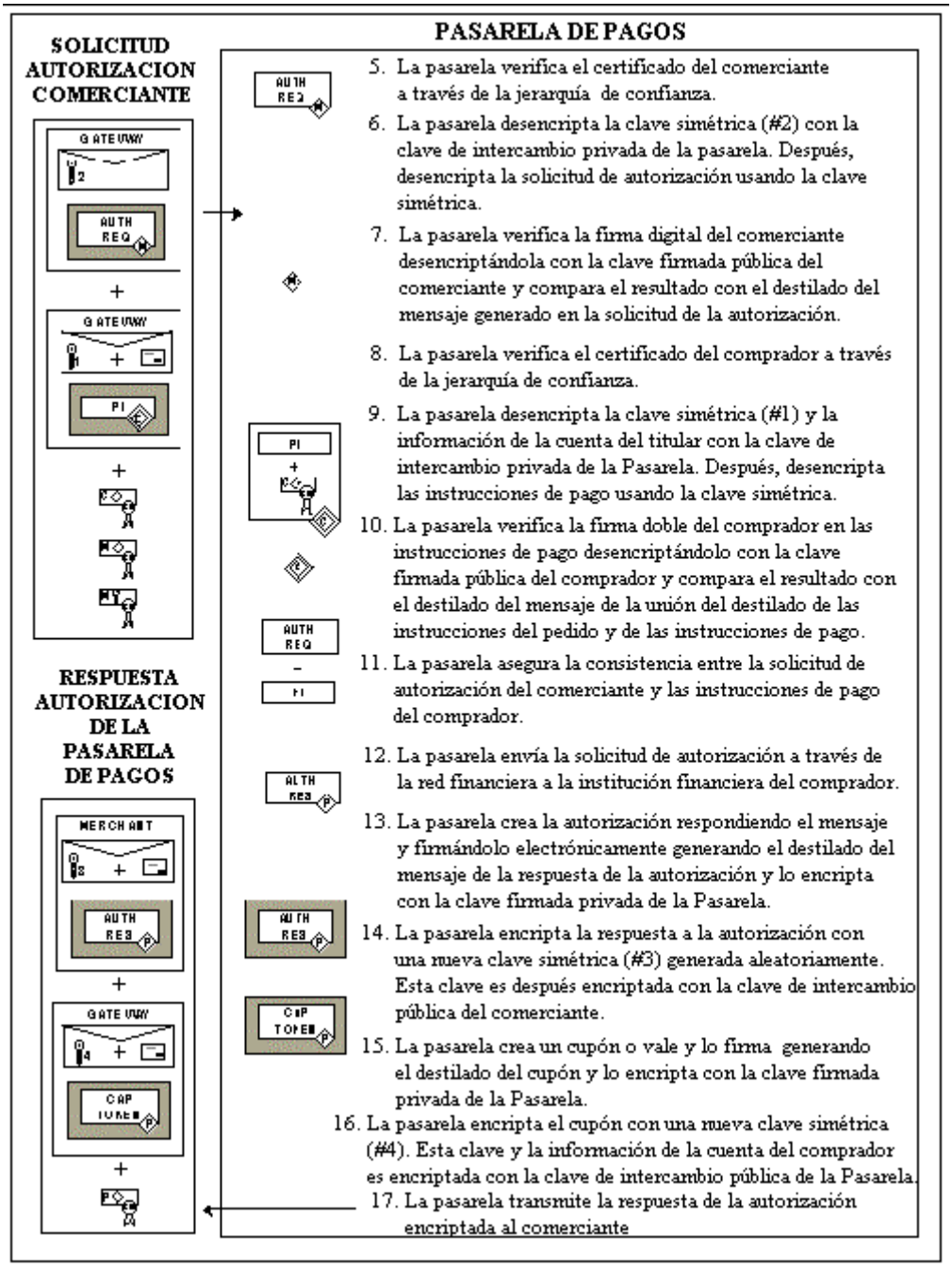
Durante el proceso del pedido de un comprador, el comerciante autorizará la transacción. El software del comerciante solicita la autorización, que incluye la cantidad a ser autorizada, el identificador de la transacción de la información del pedido, y otras informaciones acerca de la misma.




**Paso 2: Pasarela de Pagos procesa la solicitud de autorización**

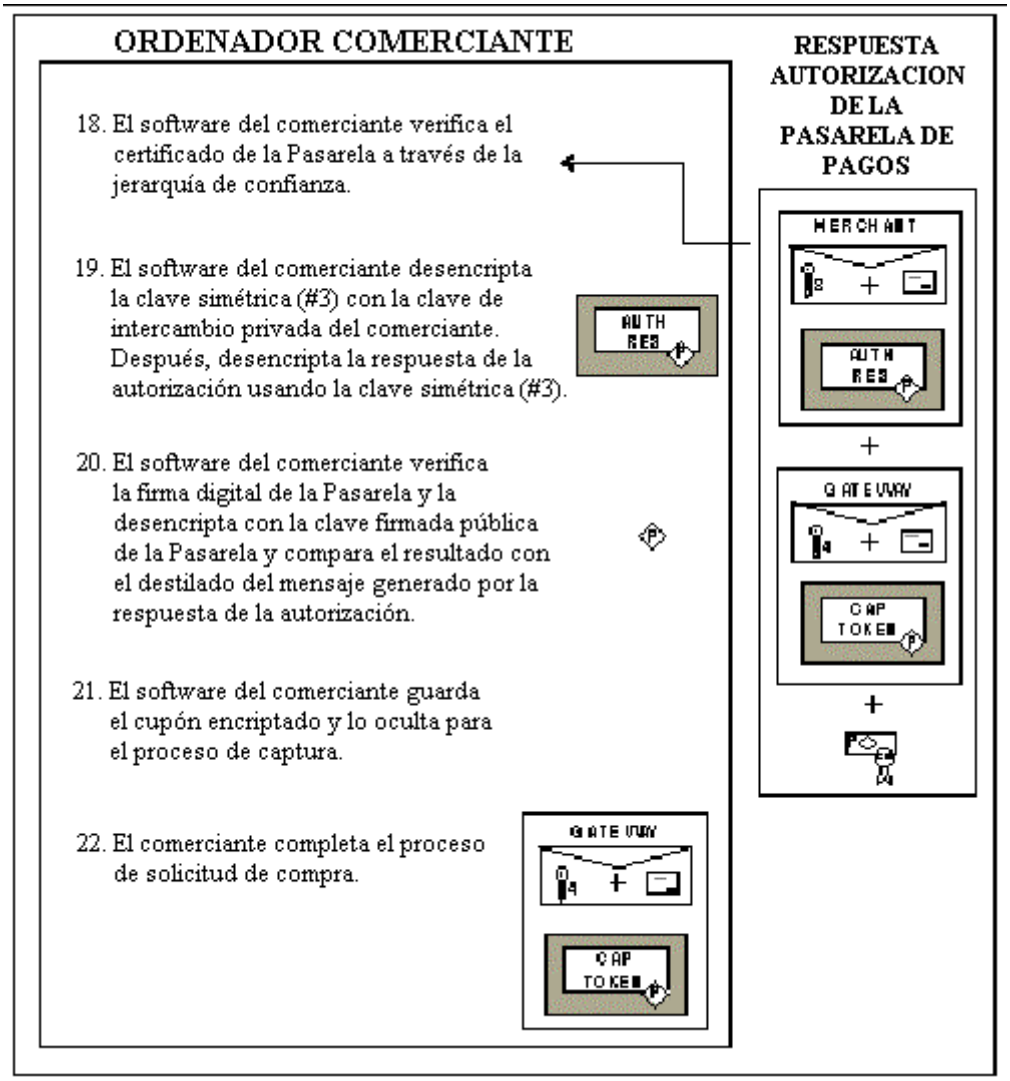
Cuando la Pasarela de Pagos recibe la solicitud de autorización, verifica que el certificado no haya caducado y la firma del mismo.

Entonces, la Pasarela de Pago envía una solicitud de autorización a la entidad financiera del comprador mediante un sistema de pago.




**Paso 3: Comerciante procesa la respuesta**

El software del comerciante guarda la respuesta de la autorización y el vale de compra para ser usado cuando el cobro sea solicitado. El comerciante entonces acaba procesando el pedido del comprador enviando la mercancía o realizando los servicios indicados en el pedido.




### 4.7.5.- Captura del pago

La figura siguiente muestra los pasos que se siguen en el proceso del cobro por parte del comerciante.

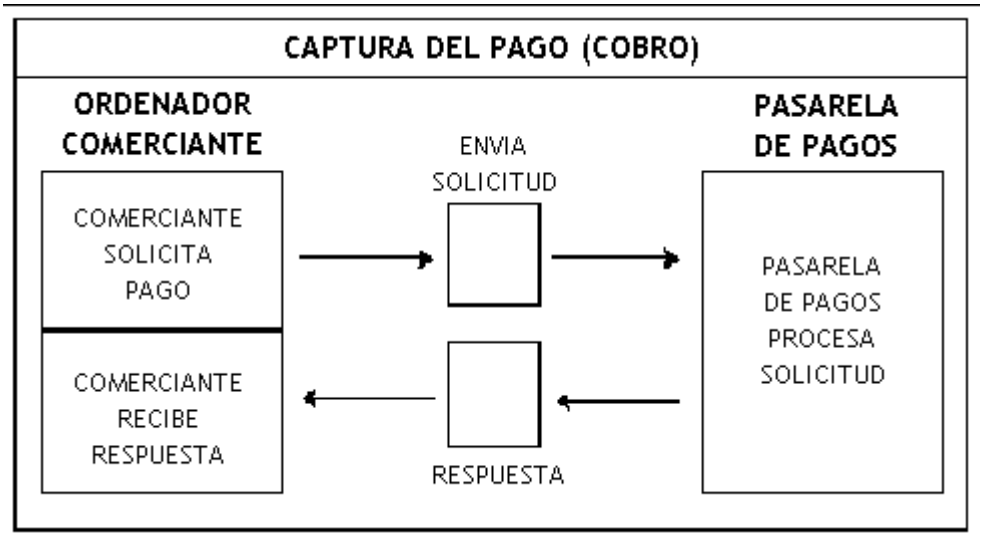
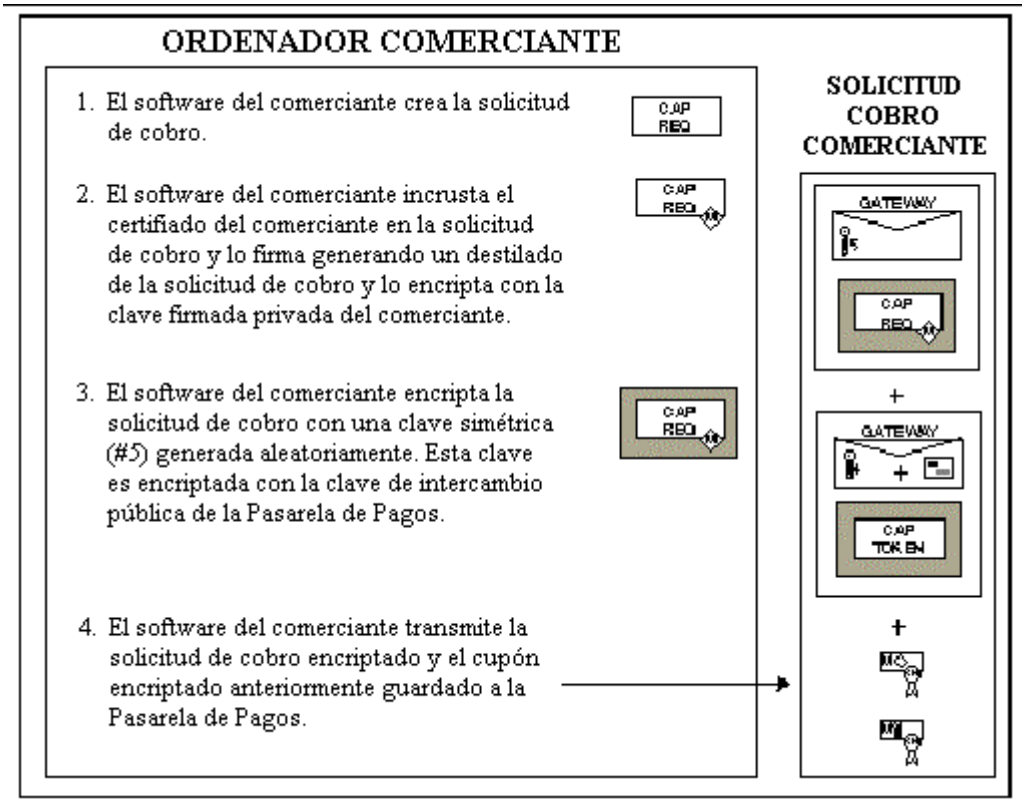



**Figura 18: Captura del pago**

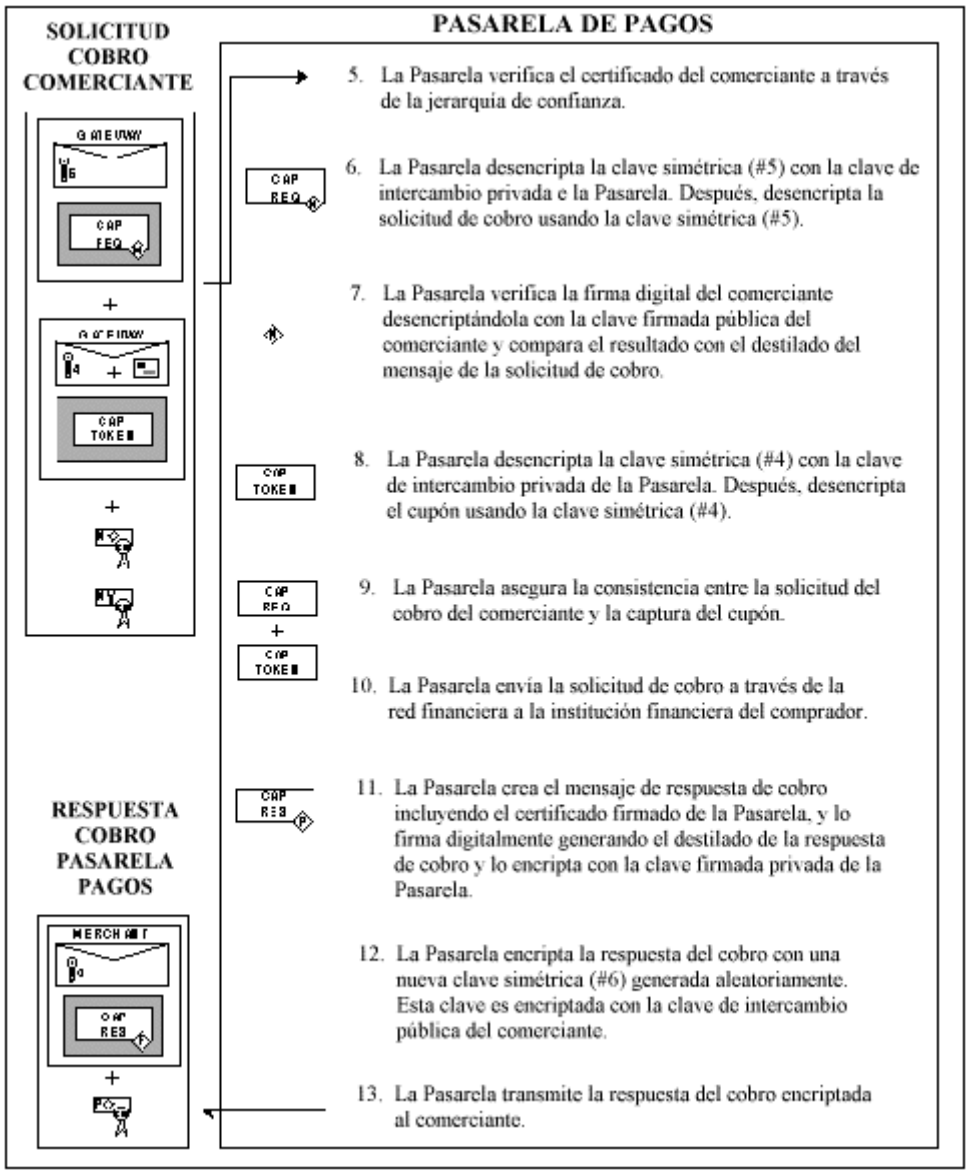
**Paso 1: Comerciante solicita el cobro**

Después de completar el proceso del pedido del comprador, el comerciante solicitara el pago. Suele pasar un tiempo entre el mensaje de solicitud de autorización y el mensaje de solicitud de pago.



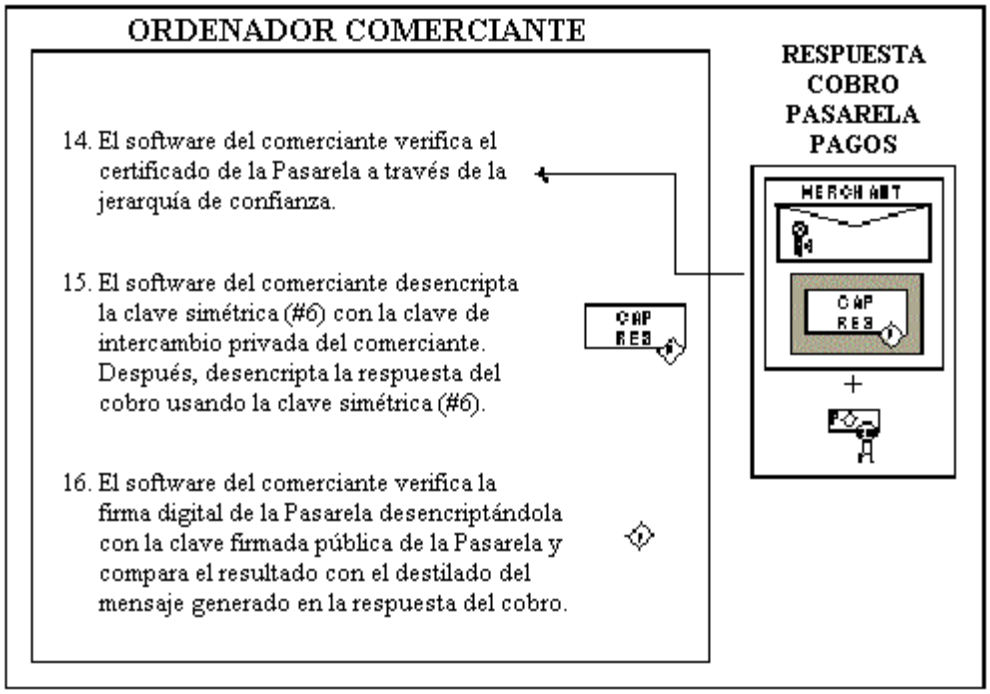

**Paso 2: Pasarela de Pagos procesa la solicitud**

La Pasarela de Pagos usa la información de la solicitud de cobro y del vale de compra para enviar la solicitud a la entidad financiera del comprador por vía del sistema de pago de la tarjeta de crédito.




**Paso 3: Comerciante recibe respuesta**

El software del comerciante guarda la respuesta para poder recibir el cobro por parte de la entidad financiera.


ORDENADOR COMERCIANTE
RESPUESTA COBRO PASARELA PAGOS
14. El software del comerciante verifica el certificado de la Pasarela a través de la jerarquía de confianza.
15. El software del comerciante desencripta la clave simétrica (#6) con la clave de intercambio privada del comerciante. Después, desencripta la respuesta del cobro usando la clave simétrica (#6).
16. El software del comerciante verifica la firma digital de la Pasarela desencriptándola con la clave firmada pública de la Pasarela y compara el resultado con el destilado del mensaje generado en la respuesta del cobro.
MERCHANT

## 5.- Bibliografía


- www.Setco.org:
  - SET's Specification Book: The business description.
  - SET's Specification Book: Programmer's guide.
- www.visa.com: New Technologies.
- www.mastercard.com
- www.kriptopolis.com

- www.kriptonomicon.com:
  - Los secretos del comercio electrónico.
  - Falsas expectativas del comercio electrónico.
  - El lado oscuro de SET.
  - Luces y sombras en la compra por Internet.
  - Seguridad en el comercio electrónico. ¿SSL o SET?

- Criptografía y Seguridad en Computadores. Manuel José Lucena López. Dpto. de Informática Escuela Politécnica Superior de Jaen. Segunda Edición, 1999.