UNIVERSIDAD DE SOTAVENTO A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

“PROTOCOLOS SET USO DE LAS TARJETAS DE CRÉDITO.”

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

ALEJANDRO REYES FERNÁNDEZ

ASESOR DE TESIS:
L.A. RAÚL DE JESÚS OCAMPO COLÍN

Coatzacoalcos, Veracruz **SEPTIEMBRE 2010.**

Dedicatoria

Mi tesis la dedico con todo mi amor y cariño. A ti DIOS que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento. Gracias por todo papa y mama por darme una carrera para mi futuro y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón el que estén conmigo a mi lado. Los quiero con todo mi corazón y esta tesis que me llevo tiempo hacer es para ustedes.

A mi hermana gracias por estar conmigo y apoyarme siempre, la quiero mucho. Y a mis abuelos por estar siempre conmigo y consentirme tanto, los amo.

Y a mis profesores por confiar en mí, por tenerme la paciencia necesaria, por apoyarme en momentos difíciles. Agradezco el haber tenido unos profesores tan buenas personas como lo son ustedes. Nunca los olvidare.

Y no me puedo ir sin antes decirles, que sin ustedes a mi lado no lo hubiera logrado, tantas desveladas sirvieron de algo y aquí está el futuro.
Les agradezco a todos ustedes con toda mi alma el haber llegado a mi vida y el compartir momentos agradables y momentos tristes, pero esos momentos son los que nos hacen crecer y valorar a las personas que nos rodean. Los quiero mucho y nunca los olvidare.

Índice

Índice de Tablas y Figuras

Capítulo I Protocolos SET

Capítulo II Uso de las Tarjetas de Crédito

Capítulo III Implementación de un Monedero Electrónico Seguro sobre el análisis del Protocolo SET

Problema

Desarrollar un monedero electrónico seguro haciendo uso de tecnología Java y smart card, sobre el análisis del protocolo SET, un entorno de computación portátil donde cada usuario cuenta con una tarjeta inteligente que puede manejar dinero electrónico para el pago de máquinas copiadoras e impresoras, autentificación, registro de cursos, etc.

Hipótesis

Evolución de la forma del uso del monedero electrónico seguro mediante la utilización de mecanismos de seguridad simples, pues asegura que la información es verificada/registrada por el servidor. Se da también la implementación para proteger la confidencialidad de los datos de las tarjetas de crédito que es muchas veces extraída y suministrando los recursos económicos, al igual que la utilización de la información, para el manejo inadecuado de las mismas.

Gracias a esta evolución del uso del monedero electrónico y permitiendo con ello la utilización e implementación del mismo, que se ha desarrollado, mediante el uso y utilidad.

Esperando que con ello se logre que los datos se mantengan íntegros, ya que al viajar encriptados y protegidos por una firma digital no pueden ser alterados en el camino. Mediante la autenticación del comerciante ante el comprador de que está autorizado para aceptar cobros con tarjetas de crédito. Y también la autenticación del cliente ante el comerciante como un legítimo titular de una tarjeta de crédito.

Protocolos SET Uso de las Tarjetas de Crédito

Objetivo General

- Desarrollar un monedero electrónico seguro haciendo uso de tecnología Java y smart card, sobre el análisis del protocolo SET un entorno de computación portátil donde cada usuario cuenta con una tarjeta inteligente que puede manejar dinero electrónico para el pago de máquinas copiadoras e impresoras, autentificación, registro de cursos, etc.

Objetivo Específico

- Establecer y Ayudar a cumplir las necesidades por la que se ha implementado este método.

- Dar a los usuarios las herramientas más prácticas, y con soluciones esperadas, para el manejo del monedero electrónico seguro haciendo uso de tecnología sobre el análisis del protocolo SET.

- Delimitar cuales son los beneficios que se lograran con el uso y el manejo del monedero electrónico seguro.

Justificación

El tema de Protocolos SET Uso de las Tarjetas de Crédito se basa más que nada en un sistema de comunicaciones que permite gestionar de una forma segura las transacciones comerciales en la Red. Y cuando decimos de una forma segura nos referimos a que aporta un mayor nivel de seguridad que su antecesor el SSL. Precisamente esa fue la razón que dio origen a su nacimiento.

El modelo de negocios ha evolucionado de su forma tradicional (cara a cara en una tienda) a las transacciones en línea por medio de unos cuantos clicks de ratón desde el hogar o la oficina Esta ola de crecimiento trae consigo nuevos retos derivados de los riesgos de seguridad que explotan vándalos cibernéticos y crackes.

Los Hackers son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección. Su motivación abarca desde el espionaje industrial hasta el mero desafío personal. Internet, con sus grandes facilidades de conectividad, permite a un usuario experto intente el acceso remoto a cualquier máquina conectada, de forma anónima.

Por los mismo es que se está implementando un Monedero Electrónico seguro con base a todo lo antes mencionado, se pretende que no cualquier persona tenga acceso a cierta información y este delimitado por medio de esta implementación, ya sea por medio de una tarjeta inteligente que solo permita el acceso a ciertas personas y no cualquiera tenga acceso a las mismas.

Introducción

El prototipo monedero electrónico seguro usa mecanismos de seguridad simples, pero asegura que la información es verificada/registrada por el servidor.

El comercio electrónico en Internet constituye una compleja operación en la que uno de los principales elementos es dar seguridad a vendedor y comprador de que la transacción comercial que están realizando se realiza sin intromisiones de ningún tipo y sin posibilidad de fraudes o engaños entre ninguna de ambas partes.

Durante los últimos 10 años han ido surgiendo un número considerable de tecnologías y sistemas de pago electrónico que ofrecen las garantías de seguridad e integridad necesarias para realizar estas transacciones de una forma fiable.

No obstante, este sigue siendo el mayor obstáculo (tanto técnico como psicológico) a vencer para que se produzca el definitivo despegue del comercio electrónico.

Mientras no exista confianza, mientras los usuarios teman al fraude, mientras se desconozcan los sistemas de pago empleados y su fiabilidad, es difícil que esta oportunidad de negocio prospere. SSL, Secure Sockets Layer, fue diseñado y propuesto por Netscape Communications Corporation en 1994 junto con su primera versión de Netscape Navigator.

Tras una accidentada historia inicial de revisiones alcanzó su madurez en 1995 con la versión 3.0, convirtiéndose hoy en día en la solución más extendida en los servidores que ofrecen servicios de comercio electrónico y dejando virtualmente en la cuneta a todos sus competidores a pesar de que no es ni el método más seguro ni el más idóneo para implantar este tipo de soluciones, puesto que fue diseñado como un protocolo seguro de propósito general.

En esta tesis nos centraremos en realizar un detallado análisis del, hasta ahora, ganador en esta carrera pero sin olvidar por completo los méritos de sus competidores.

La seguridad (o la aparente carencia de seguridad, según el lado desde el que miremos) es la barrera real y psicológica que es necesario franquear para el definitivo despegue del comercio electrónico. Los elementos que forman esta barrera son siete y van más allá de lo meramente físico (hardware) o lógico (protocolos, aplicaciones) e involucran factores tales como la legislación, la educación de los usuarios, etc.

Estos siete elementos son:

- ✓ Confidencialidad.
- ✓ Integridad.
- ✓ Disponibilidad.
- ✓ No Repudio.
- ✓ Verificación de la Identidad.
- ✓ Validez Legal.
- ✓ Confianza de los Usuarios

Capítulo I Protocolos SET

Capítulo I Protocolos SET

1.1. Que es el protocolo SET

El Protocolo SET (Secure Electronic Transaction o Transacción Electrónica Segura) es un sistema de comunicaciones que permite gestionar de una forma segura las transacciones comerciales en la Red. Y cuando decimos de una forma segura nos referimos a que aporta un mayor nivel de seguridad que su antecesor el SSL. Precisamente esa fue la razón que dio origen a su nacimiento.

El sistema SET fue desarrollado por Visa y MasterCard, con la colaboración de American Express, Microsoft, IBM, Netscape, VeriSign y otras empresas para dotar al comercio electrónico de mayores garantías de seguridad de las que tenía hasta entonces. Sin embargo, a pesar de sus evidentes ventajas, su utilización no se ha generalizado todavía.

Es un conjunto de especificaciones desarrolladas por VISA y MasterCard, con el apoyo y asistencia de GTE, IBM, Microsoft, Netscape, SAIC, Terisa y VeriSign, que da paso a una forma segura de realizar transacciones electrónicas.

Personas involucradas en las transacciones electrónicas:

- Usuario final,
- Comerciante,
- Entidades financieras,
- Administradoras de tarjetas y
- Propietarios de marcas de tarjetas.

SET constituye la respuesta a los muchos requerimientos de una estrategia de implantación del comercio electrónico en Internet, que satisface las necesidades de consumidores, comerciantes, instituciones financieras y administradoras de medios de pago.

Por lo tanto, SET dirige sus procesos a:

- Proporcionar la autentificación necesaria.
- Garantizar la confidencialidad de la información sensible.
- Preservar la integridad de la información.
- Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

SET utiliza para sus procesos de encriptación dos algoritmos:

De clave pública RSA (algoritmo simétrico): Diseñado por Rivest, Shamir y Adleman, cuyas iníciales componen su nombre.

De clave privada DES (Data Encryption Standard): De fortaleza contrastada y excelente rendimiento, conocido también como algoritmo asimétrico ya que emplea dos claves diferentes: una para encriptación y otra para desencriptación.

La base matemática sobre la cual trabajan los algoritmos, permite que, mientras un mensaje es encriptado con la clave pública, es necesaria la clave privada para su desencriptación.

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.

Para evitar que la clave pública de un usuario sea alterada o sustituida por otro no autorizado, se crea una entidad independiente llamada Autoridad Certificadora (Certifying Authority, CA), cuya labor consiste en garantizar y custodiar la autenticidad de la claves públicas de empresas y particulares, a través de la emisión de certificados electrónicos*.*

Vamos a analizar sus ventajas e inconvenientes, así como las razones que están dificultando su implantación.

1.2. Qué se precisa para utilizar el Protocolo SET

a) Que el comerciante disponga de un certificado digital emitido por una Autoridad de Certificación.
b) Que el comprador disponga de un certificado digital emitido por la entidad emisora de la tarjeta (por ejemplo, Visa), que incluye la firma digital de dicha institución y una fecha de expiración.

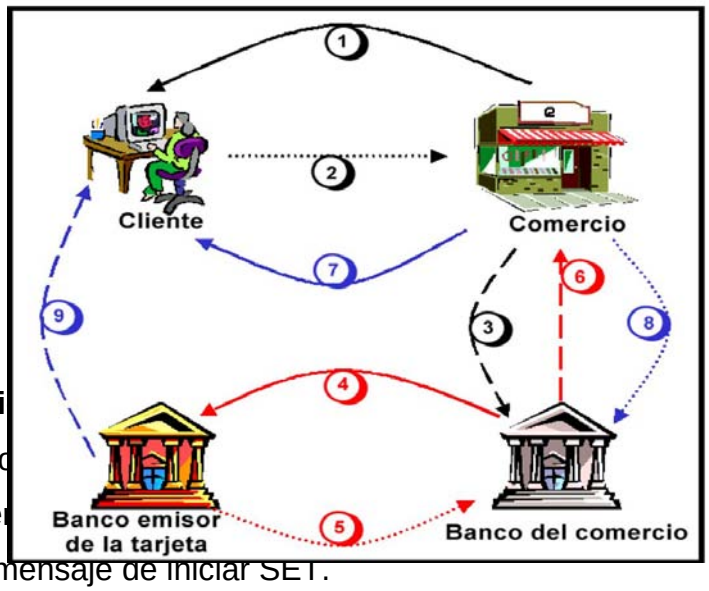
1.3. Cómo Funciona el Protocolo SET

Sin duda, el comercio electrónico demanda a gritos un mayor nivel de seguridad, y el SET se lo está ofreciendo. Tan sólo se precisa una mayor profesionalidad de los comerciantes y una maduración de los compradores para que confluyan en lo que hoy es el único sistema realmente seguro para realizar transacciones en la Red: el protocolo SET. De hecho, la gran mayoría de los negocios virtuales B2B ya lo están utilizando.

El proceso subyacente en una transacción SET típica funciona de forma muy parecida a una transacción convencional con tarjeta de crédito:

- Permite la identificación y autenticación de comerciante y cliente mediante certificados digitales.
- La transacción se cierra entre el comprador y el banco, por lo que el comerciante no ve ni puede conservar los datos de la tarjeta.
- Los datos viajan encriptados.

Ejemplo de Protocolo SET



1. **El cliente ini** el browser para selecci de orden correspondie n “pagar” y se envía un mensaje de iniciar SET.

2. **El cliente usando SET envía la orden y la información de pago al comerciante:** el software SET del cliente crea dos mensajes uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta.

   El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.
3. **El comerciante pasa la información de pago al banco:** el software SET del comerciante genera un requerimiento de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.

4. **El banco verifica la validez del requerimiento:** el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.

5. **El emisor de la tarjeta autoriza la transacción:** el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.

6. **El banco del comerciante autoriza la transacción:** una vez recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.

7. **El servidor del comerciante complementa la transacción:** el servidor del comerciante da a conocer que la transacción que la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.

8. **El comerciante captura la transacción:** en la fase final de SET el comerciante envía un mensaje de “captura” a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.

9. **El generador de la tarjeta envía el aviso de crédito al cliente:** el cargo de SET aparece en estado de cuenta del cliente que se le envía mensualmente.

SET requiere un certificado digital en cada paso de autenticación y usa dos pares de claves, una para el cifrado del sobre digital y otra para la firma, (SSL solo usa un par de claves), actualmente SET usa la función hash SHA-1, DES y RSA de 1024 bits, estos parámetros fueron tomados para ser compatible con los certificados existentes, aunque el piloto de SET usó el sistema asimétrico de cifrado con curvas elípticas y se piensa que soporte también curvas elípticas en la próxima versión de SET.

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. Como los mensajes no necesitan transmitirse en tiempo presente, son posibles implantaciones de SET eficientes basadas en correo electrónico u otros sistemas asíncronos.

En su estado actual SET solamente soporta transacciones con tarjeta de crédito/débito, y no con tarjetas monedero. Se está trabajando en esta línea para extender el estándar de manera que acepte nuevas formas de pago. Al mismo tiempo se están desarrollando proyectos para incluir los certificados SET en las tarjetas inteligentes, de tal forma que el futuro cambio de tarjetas de crédito a tarjetas inteligentes pueda incorporar el estándar SET.

1.4. Puntos clave para una correcta función del Protocolo SET

Firmas Electrónicas

Las relaciones matemáticas entre la clave pública y la privada del algoritmo asimétrico utilizado para enviar un mensaje, se llama firma electrónica (digital signatures).

Quien envía un mensaje, cifra su contenido con su clave privada y quien lo recibe, lo descifra con su clave pública, determinando así la autenticidad del origen del mensaje y garantizando que el envío de la firma electrónica es de quien dice serlo.

Certificados de autenticidad

Como se ha visto la integridad de los datos y la autenticidad de quien envía los mensajes es garantizada por la firma electrónica, sin embargo existe la posibilidad de suplantar la identidad del emisor, alterando intencionalmente su clave pública.

Para evitarlo, las claves públicas deben ser intercambiadas mediante canales seguros, a través de los certificados de autenticidad, emitidos por las Autoridades Certificadoras.

Para el efecto SET utiliza dos grupos de claves asimétricas y 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.

Criptografía

Es la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos y cifras.

La palabra criptografía se limita a veces a la utilización de cifras, es decir, métodos de transponer las letras de mensajes (no cifrados) normales o métodos que implican la sustitución de otras letras o símbolos por las letras originales del mensaje, así como diferentes combinaciones de tales métodos, todos ellos conforme a sistemas predeterminados. Hay diferentes tipos de cifras, pero todos ellos pueden encuadrarse en una de las dos siguientes categorías: transposición y sustitución.
En las claves de transposición, el mensaje se escribe, sin separación entre palabras, en filas de letras dispuestas en forma de bloque rectangular.
Las letras se van transponiendo según un orden acordado de antemano, por ejemplo, por columnas verticales, diagonales o espirales, o mediante sistemas más complicados, como el salto del caballo, basado en el movimiento del caballo de ajedrez.

La disposición de las letras en el mensaje cifrado depende del tamaño del bloque utilizado y del camino seguido para inscribir y transponer la letras. Para aumentar la seguridad de la clave o cifra se puede utilizar una palabra o un número clave; por ejemplo, a la hora de transponer por columnas verticales, la palabra clave coma obligaría a tomar las columnas en el orden 2-4-3-1, que es el orden alfabético de las letras de la palabra clave, en lugar de la secuencia normal 1-2-3-4.

Las cifras de transposición se pueden reconocer por la frecuencia de las letras normales según el idioma utilizado. Estas cifras se pueden desentrañar sin la clave reordenando las letras de acuerdo con diferentes pautas geométricas, al tiempo que se van resolviendo anagramas de posibles palabras, hasta llegar a descubrir el método de cifrado.

Los Hackers

Son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección. Su motivación abarca desde el espionaje industrial hasta el mero desafío personal. Internet, con sus grandes facilidades de conectividad, permite a un usuario experto intentar el acceso remoto a cualquier máquina conectada, de forma anónima.

Las redes corporativas u ordenadores con datos confidenciales no suelen estar conectadas a Internet; en el caso de que sea imprescindible esta conexión, se utilizan los llamados cortafuegos, un ordenador situado entre las computadoras de una red corporativa e Internet. El cortafuego impide a los usuarios no autorizados acceder a los ordenadores de una red, y garantiza que la información recibida de una fuente externa no contenga virus.

1.5. Pasos para una transacción SET

- Cuando se va a cerrar el pedido, el cliente recibe la firma digital de la tienda y verifica su validez.
- El cliente envía al comerciante la siguiente información firmada digitalmente:
    - Los datos del pedido (básicamente: identificación del comerciante, importe y fecha)
    - La orden de pago, con una encriptación que sólo puede leer el banco.
    - La relación entre el pedido y la orden de pago, que los liga indisolublemente.
- El comercio recibe el pedido y verifica la validez de la firma digital.
- El comerciante pasa al banco la orden de pago (que él no ha podido leer) con su firma digital.
- El banco autoriza la transacción y devuelve dos confirmaciones, una para el comerciante y otra para el titular de la tarjeta.

1.6. Cómo SET protege sus transacciones

El protocolo SET ofrece una serie de servicios que convierten las transacciones a través de Internet en un proceso seguro y fiable para todas las partes implicadas:

Autenticación: Todas las partes involucradas en la transacción económica (el cliente, el comerciante y los bancos, emisor y adquiriente) pueden verificar mutuamente sus identidades mediante certificados digitales. De esta forma, el comerciante puede asegurarse de la identidad del titular de la tarjeta y el cliente, de la identidad del comerciante. Se evitan así fraudes debidos a usos ilícitos de tarjetas y a falsificaciones de comercios en Internet (web spoofing), que imitan grandes web comerciales. Por su parte, los bancos pueden asimismo comprobar la identidad del titular y del comerciante.

Confidencialidad: La información de pago se cifra para que no pueda ser espiada mientras viaja por las redes de comunicaciones. Solamente el número de tarjeta de crédito es cifrado por SET, de manera que ni siquiera el comerciante llegará a verlo, para prevenir fraudes. Si se quiere cifrar el resto de datos de la compra, como por ejemplo qué artículos se han comprado o a qué dirección deben enviarse, debe recurrirse a un protocolo de nivel inferior como SSL.

Integridad: Garantiza que la información intercambiada, como el número de tarjeta, no podrá ser alterada de manera accidental o maliciosa durante su transporte a través de redes telemáticas. Para lograrlo se utilizan algoritmos de firma digital, capaces de detectar el cambio de un solo bit.

Intimidad: El banco emisor de la tarjeta de crédito no puede acceder a la información sobre los pedidos del titular, por lo que queda incapacitado para elaborar perfiles de hábitos de compra de sus clientes.

Verificación inmediata: Proporciona al comerciante una verificación inmediata, antes de completarse la compra, de la disponibilidad de crédito y de la identidad del cliente. De esta forma, el comerciante puede cumplir con todos los pedidos sin riesgo de que posteriormente se invalide la transacción.

No repudio para resolución de disputas: La mayor ventaja de SET frente a otros sistemas seguros es la adición al estándar de certificados digitales (X.509v3), que asocian la identidad del titular y del comerciante con entidades financieras y los sistemas de pago de Visa, MasterCard, etc. Estos certificados previenen fraudes para los que otros sistemas no ofrecen protección, como el repudio de una transacción (negar que uno realizó tal transacción), proporcionando a los compradores y vendedores la misma confianza que las compras convencionales usando las actuales redes de autorización de créditos de las compañías de tarjetas de pago.

1.7. Quiénes Participan en SET

El pago mediante tarjeta es un proceso complejo en el cual se ven implicadas varias entidades:

El banco emisor

Emite la tarjeta del cliente, extiende su crédito y es responsable de la facturación, recolección y servicio al consumidor.

En el artículo 46 de la Ley de Comercio Minorista se establece que cuando el importe de una compra hubiese sido cargado utilizando el número de una tarjeta de crédito, sin que ésta hubiese sido presentada directamente o

identificada electrónicamente (por ejemplo por un hacker que robó el número en Internet), su titular podrá exigir la inmediata anulación del cargo.

El banco adquiriente

Forma relación con el comerciante, procesando las transacciones con tarjeta y las autorizaciones de pago.

El titular de la tarjeta

Posee la tarjeta emitida por el banco emisor y realiza y paga las compras.

El comerciante

Vende productos, servicios o información y acepta el pago electrónico. La parte débil en las transacciones electrónicas es el comerciante, a quien corresponde probar que su abono está justificado (a no ser que responda el banco o entidad financiera titular de la tarjeta, todo depende del contrato que tenga con el comerciante).

La pasarela de pagos

Mecanismo mediante el cual se autorizan y procesan las transacciones del comerciante (autorización, revocación, liquidación, etc.). La pasarela puede pertenecer a una entidad financiera (adquiriente) o a un operador de medios de pago. Conectan Internet con las redes privadas de autorización de pagos, largamente establecida y fiable.

El procesador (redes de medios de pago)

Proporciona servicios adicionales operando la infraestructura de telecomunicaciones sobre las que se realizan las transacciones.

Autoridad de certificación

Certifica las claves públicas del titular de la tarjeta, del comerciante y de los bancos. La Agencia de Certificación Española (ACE), formada por Telefónica, SERMEPA, CECA y Sistema 4B, viene ofreciendo el servicio de certificación SET desde finales de 1998 en España.

1.8. Elementos Primordiales para las Seguridad de SET

- Confidencialidad de los datos de la tarjeta de crédito, ya que al estar el comprador identificado ante la entidad financiera por un certificado digital emitido por ella misma, no es preciso que la información de la tarjeta de crédito viaje, con lo que nunca llega a manos del comerciante ni puede ser interceptada por nadie.
- Integridad de los datos, ya que al viajar encriptados y protegidos por una firma digital no pueden ser alterados en el camino.
- Autenticación del comerciante ante el comprador de que está autorizado para aceptar cobros con tarjetas de crédito.
- Autenticación del cliente ante el comerciante como un legítimo titular de una tarjeta de crédito.

1.9. Algunas de las Desventajas de la Utilización del SET

- Muchos ISP no están preparados para trabajar con protocolo SET.
- Aunque para el titular de la tarjeta es gratuito, la obtención del certificado digital puede tener un coste importante para el comerciante.

- La duración de la transacción es mayor que con SSL (suele estar entre 25 y 30 segundos).
- Supone una mayor complejidad para el comerciante, ya que trabajar con SET implica, hoy por hoy, trabajar simultáneamente con SSL, puesto que la mayoría de los clientes no tienen todavía certificado digital.

Sin duda, el comercio electrónico demanda a gritos un mayor nivel de seguridad, y el SET se lo está ofreciendo. Tan sólo se precisa una mayor profesionalidad de los comerciantes y una maduración de los compradores para que confluyan en lo que hoy es el único sistema realmente seguro para realizar transacciones en la Red: el protocolo SET.

1.10. Componentes de Software para Operar con SET

Existen cuatro componentes software distinto, necesario para completar el escenario de pago seguro mediante SET:

El Software de Cartera del Titular

Aplicación 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.

Para garantizar la seguridad de sus datos, el monedero los protege mediante una contraseña. Microsoft distribuye una aplicación monedero con su navegador Internet Explorer 4.0 ó superior (Herramientas, Opciones de Internet..., Contenidos, Pagos). SafeLayer comercializa en España una aplicación de cartera digital, poniendo a disposición del público una versión de demostración.

Para examinar un listado exhaustivo de monederos digitales actualmente disponibles, visite la matriz de compatibilidad de SETCo en. Si su banco emite certificados SET, distribuirá también software de monederos digitales.

El Software de punto de venta del Comerciante

Para que el sitio web del comerciante acepte pagos con SET necesitará instalar una aplicación de Terminal de Punto de Venta (POST) compatible con SET en su servidor, que acepte los pedidos y procese los pagos con el banco. Para obtener un listado de empresas que comercializan aplicaciones POST que hayan sido certificadas.

El Software del servidor de la pasarela de Pagos

Realiza el procesamiento automatizado de los pagos. La pasarela recibe peticiones de autorización/liquidación/reconciliación de pagos de los sistemas del comerciante (POST) en Internet y las encamina hacia los sistemas de pago propietarios (sistemas de autorización tradicionales).

El Software de la Autoridad de Certificación

Las entidades financieras que decidan soportar el estándar SET necesitarán este software para que sus respectivos clientes (titulares de tarjetas y comerciantes que aceptan pago con tarjeta) puedan participar en el juego. Permite registrar a los usuarios y emitir certificados digitales para ellos, que aseguren la confianza entre las partes.
Además, tanto los clientes como los comerciantes necesitan certificados para garantizar la identidad de los participantes.

1.11. El Papel de los Certificados en SET

SET proporciona los mecanismos necesarios para que tanto consumidores

como comerciantes se autentifiquen mutuamente antes de que la transacción tenga lugar. De esta manera se consigue replicar en el mundo digital la situación común en la que el cliente se encuentra físicamente delante del mostrador del vendedor a la hora de pagar la compra.

SET utiliza certificados digitales para realizar este proceso de autentificación. Estos certificados sirven como documentos de identidad digitales (algo así como un DNI virtual) que permiten verificar la identidad de una persona a través de una red de telecomunicaciones, de manera similar a como una firma en las tarjetas de crédito atestigua que el signatario es el legítimo titular.

Por su parte, los certificados emitidos a comerciantes equivalen a esas etiquetas mostradas en el escaparate en las que se informa de que aceptan pagos con tarjetas de esta o aquella casa, además de dar fe de su identidad. Los certificados son emitidos y gestionados por la misma entidad financiera o emisor de tarjetas de la que se recibió la tarjeta de pago.

Se necesita un certificado distinto para cada marca diferente de tarjeta de crédito con la que se efectúen las compras (caso del consumidor) o que sea aceptada en el comercio (caso del comerciante).

Los certificados SET son emitidos por autoridades de certificación (AC) dentro de la jerarquía de certificación SET. Esta jerarquía asegura la autenticación válida de los participantes. Garantiza además la seguridad de los datos intercambiados entre titulares, comerciantes, bancos y pasarelas de pagos. La autoridad raíz autentica y emite certificados a las casas de medios de pago, cada una de las cuales se establece a su vez como autoridad de certificación para su marca (Visa, MasterCard, American Express, etc.).

Cada marca de tarjetas de crédito establece su propia pasarela de pagos como una AC. La AC de la pasarela de pagos de cada marca emite certificados digitales para bancos adquirientes o procesadores de pago de terceras partes que actúan en representación de entidades adquirientes, de manera que estas entidades pueden aceptar transacciones por Internet y convertirlas a mensajes que las redes privadas de pago pueden entender para procesar el pago.

Las AC de marcas de tarjetas autentifican y emiten certificados a sus bancos y entidades de crédito miembros, a las que establecen como autoridades de certificación. Las entidades adquirientes se erigen en AC de comerciantes, mientras que las entidades emisoras lo hacen en AC de titulares.

Una vez erigida en AC de titular y/o comerciante, la entidad financiera puede autenticar y emitir certificados a sus clientes, sean estos particulares y/o comerciantes.

1.12. Obstáculos de SET

Entonces, si todo son alabanzas, ventajas y puntos fuertes, ¿por qué SET no termina de implantarse? En primer lugar, SET no resulta fácil de implantar, por lo que su despliegue está siendo muy lento.
SET exige software especial, tanto para el comprador (aplicación de cartera electrónica) como para el comerciante (aplicación POST o TPV), y los bancos (software de autoridad de certificación, pasarela de pagos, etc.). La creación y comercialización (o distribución gratuita, según el caso), de estos productos software se está desarrollando con lentitud, no existe suficiente información al respecto y en general la situación es cuando menos confusa.

En segundo lugar, aunque los productos anteriores cumplan con el estándar SET, esto no implica necesariamente que sean compatibles. Este es un problema que exige mayores esfuerzos de coordinación y más pruebas a

escala mundial para asegurar la interoperabilidad. Es difícil encontrar una aplicación cartera que pueda comprar con cualquier terminal POST, y viceversa (un TPV que acepte pagos de cualquier otra aplicación cartera).

Estas barreras constituyen un obstáculo importante que seguirán retrayendo el despliegue SET en tanto no se alcance la convergencia de aplicaciones.

SET puede llegar a originar un conflicto en muchos vendedores a la hora de integrar los productos SET con sus sistemas internos de entrada de órdenes. Como la información sobre el número de la tarjeta de pago del comprador está cifrada e inaccesible al vendedor, pueden surgir problemas con sistemas internos que precisan para su propia contabilidad el número de la tarjeta del cliente.

En tales casos, una posible solución sería que los propios comerciantes solicitaran los números de tarjeta de los compradores a las organizaciones de tarjetas de pago. Un inconveniente adicional de SET reside en su incapacidad para trabajar con pagos aplazados, modalidad muy extendida en países como España.

Sus puntos fuertes son también su talón de Aquiles: La autentificación de todas las partes exige rígidas jerarquías de certificación, ya que tanto clientes como comerciantes deben adquirir certificados distintos para cada tipo de tarjeta de crédito, trámites que resultan engorrosos, para la mayoría de los usuarios. Se añade el problema de la revocación de certificados, la portabilidad de los mismos cuando el usuario trabaja en distintas máquinas y las cadenas de certificación. En definitiva, SET descansa sobre una infraestructura de clave pública (PKI) que en la actualidad dista mucho de ser perfecta.

SET seguirá coexistiendo con SSL durante mucho tiempo, hasta que se

alcance una masa crítica de usuarios que propicien su utilización a gran escala, o caiga en el olvido superado por otra nueva iniciativa más ágil y mejor adaptada. Las opiniones de los analistas se encuentran divididas acerca de su futuro. En lo que todos coinciden es que aún le queda un largo camino por recorrer.

Capítulo II Uso de las Tarjetas de Crédito

2.1. Definición de Tarjeta de Crédito

Análisis de todos los usos de las tarjetas de crédito. Hay algunos conocidos (Medio de pago, financiación), pero otros que desconocemos y de los que hay sacar partido. (Puntos, cash back, financiación gratuita).
Un **pequeño crédito** del cual se hace uso, por medio de la emisión de una tarjeta de plástico personalizada que dispone de una **banda magnética** y un **número de relieve**.

Hay muchas ventajas de las tarjetas de crédito, pero la más importante es la flexibilidad en el pago de los saldos gastados. Puedes pagar al final de mes, a plazos, o un saldo mínimo.
El funcionamiento de las tarjetas de crédito, es sencillo, puedes gastar hasta el límite concedido. El crédito se repone automáticamente una vez hayas pagado las deudas de tarjetas pendientes.

2.2. Principales Ventajas de las Tarjetas de Crédito

- ✓ **Garantizan tus derechos de consumidor:** Las mercancías compradas con las tarjetas de crédito pueden devolverse o cambiarse de una forma más rápida que si se hubiesen pagado en efectivo.
- ✓ **Medio de Pago:** Te permite comprar sin efectivo. **Es más fácil comprar.** No tienes que llenar la billetera de efectivo. **Eliminas los riesgos de robo del efectivo**.

Figura 2.2. Principales Ventajas de las Tarjetas de Crédito

- ✓ **Pagos en internet:** A pesar de todas las incertidumbres que generan, utilizar tarjetas crédito internet en un sitio de confianza, **es quizás más seguro que pagar en un mostrador**. Internet además te abre un abanico de posibilidad muchos más amplios que las tiendas de tu ciudad.

Para pagar por internet, hay bancos que ofrece **tarjetas virtuales** con un saldo limitado. Son como tarjetas prepago pero no hay tarjeta física.

Las ventajas de las tarjetas de crédito. Te ofrecen mayor garantía en tus compras, te permiten obtener un crédito gratuito, pagar por internet, atender gastos inesperados.

2.3. Principales Usos de las Tarjetas de Crédito

Tanto para las personas que ya cuentan con una tarjeta de crédito, pero que no han sabido manejarla con mesura, como para aquellas que aún no la tienen pero están interesadas.

Según el uso que se vaya hacer, las tarjetas de crédito **sirven para lo siguiente:**

- ✓ Como medio de pago
- ✓ Para realizar compras y aplazar los pagos durante los varios meses. Obtener crédito
- ✓ Para cancelar otras deudas.
- ✓ La forma inteligente de utilizar las tarjetas de crédito.

2.4. Beneficios Asociados a la Tarjeta de Crédito

Seguros de compra: Muchas tarjetas tienen un seguro asociado que te garantizan contra el robo del producto. Cuando contratas un vuelo o un viaje con la tarjeta, puedes beneficiarte de un seguro de viaje.

Puntos de Tarjetas: Hay **tarjetas de puntos** con los que acumulas puntos canjeables por otros artículos (billetes de avión, gasolina etc.) Hay otras que te devuelven un % del dinero gastado.

Financiación: Recibes un préstamo gratis por la duración del periodo de gracia, normalmente unos 20 a 25 días. No obstante hay que tener claro cómo eliminar las **deudas con tarjetas de crédito.**

Algunas tarjetas te permiten hacer transferencia de dinero desde la tarjeta con una **comisión de traspaso** 0%, Es una forma de obtener un dinero líquido sin intereses.

2.5. Control de las Finanzas dentro de la Tarjetas de Crédito

Es más fácil llevar un control del gasto mensual. Mirando los extractos puedes llevar una contabilidad más precisa de tus cuentas. Con el efectivo no podrías hacer esto.

Para aquellos con dificultades para ajustarse a un presupuesto, existen las tarjetas prepagos, en donde tú mismo limitas el saldo que puedes gastar.

Principales problemas con tarjetas de crédito. Aprenda a utilizar las tarjetas de créditos.
Desventajas de las tarjetas de crédito: Interés compuesto, pagos mínimos, excesivo gasto, demasiadas tarjetas.

2.6. Puntos a considerar para un Buen Manejo de su Tarjeta de Crédito

1.- Recuerde que una tarjeta de crédito es dinero, que al fin y al cabo es prestado por el banco y que tendrá que pagar junto con comisiones e intereses, por lo tanto gaste solamente lo que puede pagar.

2.- Controle los gastos con la tarjeta de crédito y no olvide guardar todos los comprobantes de lo que haya comprado, estos le servirán para compararlos con su estado de cuenta; de esta forma también podrá detectar a tiempo, en caso de que el banco le haga cargos incorrectos.

3.- Programe los pagos de su tarjeta de crédito junto con sus otros gastos mensuales como la renta, la luz, el agua, teléfono, colegiaturas; así podrá cumplir a tiempo con estos pagos sin que le cobren recargos.

4.- Es mucho mejor si hace los pagos de la tarjeta de crédito antes de la fecha límite, así el cálculo de los intereses que le cobrará el banco serán sobre un monto menor y evitará que le cobren intereses moratorios. Haga lo mismo para sus otros pagos.

5.- Si va a realizar pagos con cheque y de otros bancos, tenga cuidado de que sea con la anticipación necesaria, tome en cuenta que el banco tarda 72 horas después en darle el trámite de recepción a este documento.

6.- Si es posible y para disminuir su deuda de la tarjeta de crédito, pagué por lo menos el doble del pago mínimo requerido.

7.- Utilice la tarjeta a partir del día siguiente de la fecha de corte y durante los siguientes primeros días del periodo, ya que será mayor el período de tiempo entre la compra y la fecha de pago. 8.- Si está en la posibilidad, liquide el importe total de las compras efectuadas durante el período, así no pagará intereses (si no se ha excedido en sus gastos, le será más fácil).

9.- Al programar sus pagos de la tarjeta, también tome en cuenta que eventualmente le cobrarán además comisiones por anualidad de titular y adicional, así podrá pagar lo requerido, sin tener que tomar de algún dinero ya programado para otras cuestiones.

10.- Revise en su estado de cuenta, que el saldo inicial concuerde con el estado de cuenta anterior; compare este saldo con sus comprobantes o bauchers. También revise en caso de que los haya, la procedencia de los cargos extras por cuota anual, reposiciones, tarjetas adicionales, etc.

11.- Recuerde que en caso de que quiera hacer una reclamación al banco, tiene 45 días naturales contados a partir de la fecha de corte de su tarjeta de crédito. Así también recuerde que es necesario que conserve todos los documentos y comprobantes referentes al manejo de su tarjeta, ya que son estos los que presentará al momento de hacer su inconformidad.

12.- Es importante revisar que en el estado de cuenta aparezcan todos los pagos que se hicieron en el periodo anterior.

13.- Analice si realmente necesita los servicios adicionales que ofrece el banco a través de su tarjeta como: asistencia médica, vial y segura de accidentes en viajes; porque esto puede aumentar el cargo mínimo a pagar, si no los necesita puede cancelar estos servicios por escrito y evitar esos cargos.

14.- No utilice tantas tarjetas de crédito, ya que puede perder el control de lo que se gasta con ellas, además de que pagará más por comisiones.

Es mejor si sólo controla una, así podrá llevar un nivel adecuado de consumo. Compare y analice si puede juntar sus deudas en una sola tarjeta de crédito.

Platique con el banco que le ofrezca mejores condiciones.

15.- No descuide la fecha de vigencia de su tarjeta, así evitará que se la rechacen en algún establecimiento y hasta en un momento inesperado o que realmente necesita usarla.

Figura 2.6. Puntos a considerar para un Buen Manejo de su Tarjeta de Crédito

2.7. Las Tarjeta como medio de Pago

La tarjeta sustituye a dinero efectivo. Las compras realizadas durante el periodo se acumulan en un saldo mensual que se cargan en la cuenta del titular de la tarjeta.

Las tarjetas para obtener crédito: Las tarjetas de crédito se utilizan para obtener créditos de pequeñas cantidades, hasta el límite de la tarjeta, sin necesidad de aprobación previa. El dinero aplazado incurre en unos intereses de tarjetas.

Las tarjetas de crédito para cancelar deudas: Uso de las tarjetas de crédito muy extendido, pero completamente equivocado. Hay mejores soluciones para cancelar otras deudas. Siempre, hable con su banco, primero.

2.8. La forma inteligente de utilizar la Tarjeta de Crédito

Las dos formas más aconsejables de utilizar las tarjetas son las siguientes:

- **Como medio de pago**: Una de las ventajas de las tarjetas de crédito es su seguridad como medio de pago. Es un **medio seguro y accesible de realizar compras no solamente en persona sino también en internet**. Si se utiliza con cuidado, la tarjeta te da la posibilidad de comprar cualquier en cualquier lugar del mundo.
- Se puede utilizar también para **obtener pequeñas cantidades de crédito**, pero siempre hay que mirar con cuidado las comisiones de las tarjetas de crédito y los intereses de tarjeta. El titular de la tarjeta siempre puede anticipar el pago de o bien pagar una cantidad mínima. Mensual.
- **Obtener financiación gratuita**, durante el periodo de gracia. Si pagas el total y no sobre pasas el límite puedes obtener una financiación a 30 días sin coste alguno

2.9. Cómo Funcionan las Tarjetas de Crédito

Cómo funcionan las tarjetas de crédito: periodo de liquidación, sistema de pago, estado de cuentas, pago mínimo.

2.10. La 10 Principales Claves de Tarjetas de Crédito

A continuación le enumeramos las siguientes claves para sacar el mejor partido a su tarjeta de crédito.

10. Disponga al menos de una tarjeta de crédito para emergencia. Independientemente que le guste utilizar las tarjetas de crédito, siempre es aconsejable tener al menos una tarjeta de crédito de **bajo interés.**

9. Tenga cuidado con las tarjetas de puntos–Las tarjetas de puntos pueden ser beneficiosas pero sólo si se utilizan correctamente. Estas tarjetas suelen tener **intereses más altos de lo normal**, justificados en base a la oferta de un sistema de puntos y beneficios. **Los puntos pueden no ser tan interesantes como parece**.

Para canjear los puntos tiene un tiempo limitado. **Solo interesa, en el caso**

de que pagues todo el saldo al final de mes y utilices a menudo la tarjeta. Si la utilizas poco, y aplazas los pagos, nuca es interesante tener una tarjeta de puntos.

8. Si decides tener una tarjeta de puntos, **disponga siempre de dos tarjetas**. La tarjeta de puntos para realizar todos los pagos diarios, cuyo saldo lo pagaras al final de mes. Una segunda tarjeta, con un interés lo más bajo posible para cubrir gastos extraordinarios para los que necesita un aplazamiento.

7. Investiga antes de solicitar tarjetas de crédito. No contrates la primera tarjeta que te oferten por correo. Investiga antes.

6. Lee la letra pequeña En la letra pequeña **se incluyen todas las condiciones de cómo funcionan las tarjetas de crédito.** Qué pasa si no efectúas un pago a tiempo, que tipo de interés se aplica, responsabilidad en caso de robo etc. El texto de las condiciones no suele ser muy largo, por lo que no es difícil léeselo.

5. Pague el saldo pendiente al final de mes La mayoría de las tarjetas suelen tener unos interese muy altos en comparación a otros préstamos. **Si necesita hacer una compra de importe elevado, pida un préstamo, no utilice la tarjeta**.

4. Solicita siempre mejores condiciones. Pasado unos meses y suponiendo que has sido un buen pagador, pide siempre una mejora de tus condiciones. La competencia entre las entidades emisoras es grande y siempre es difícil conseguir buenos clientes.

3. Trate con el departamento de cancelaciones. Cuando pienses que no le

están tratando bien o que no le ofrecen las mejores condiciones, amenace con irse. Le traspasarán con un departamento específico en donde intentarán convencerle de que se quede. Siempre es más fácil obtener cosas de este departamento que de otros.

2. No disponga de efectivo con su tarjeta de crédito Aparte de dejar de pagar la tarjeta, esta es la segunda cosa peor que usted puede hacer al utilizar la tarjeta. Los anticipos de efectivos en los cajeros tienes un interés altísimo.

1. Nunca deje de pagar la tarjeta. Esto es lo peor que puede hacer. No pagar suponen mayores interese y comisiones extras, además de imposición de seguros de pagos

Figura 2.10. La 10 Principales Claves de Tarjetas de Crédito

Consejos prácticos para hacer el mejor uso de las tarjetas de crédito. Descripción de los principales errores que nos encontramos al utilizar las tarjetas de crédito.

2.11. Como se usan las tarjetas de crédito: No cometa errores

Conozca sus límite de endeudamiento

El dinero gastado en una tarjeta es un préstamo que tiene ser devuelto más tarde o más temprano. Al principio, evite en los límites altos. Ajústese al límite mensual. Con las tarjeta es fácil que la deuda se acumule especialmente si el interés el alto.

Evite los Pagos mínimos

Todas las tarjetas tienen la posibilidad de pagar un **mínimo mensual**. Sin embargo evite esta posibilidad en todo lo posible, ya que es muy difícil rebajar el total endeudado, y lo intereses siempre se calculan sobre el total no devuelto. Es un círculo vicioso.

Además si no hace un pago un mes, se te puede cancelar la tarjeta y esto puede afectar a tu capacidad de crédito futura.

No pagar tarde

Pagar fuera de plazo es un camino hacia el desastre. Las comisiones de tarjetas por descubiertos en tarjetas de crédito son muy grandes. Más información sobre las comisiones de las tarjetas.

Guardar los recibos.

Es siempre importante **guardar todos los recibos y documentos de las transacciones realizadas con la tarjeta de crédito**. Más sobre cómo utilizar correctamente las tarjetas de créditos.

Procure no dejar los extractos en la bolsa de sus compras. Un ladrón que robase su compra tendría la información de su tarjeta.

2.11.1. Comprobar el resumen de gastos mensual

Compruebe que los gastos del resumen mensual coincidan con sus recibos de compra. Compruebe el concepto y la cantidad. Más sobre el manejo de las tarjetas de crédito.

Informe inmediatamente a la entidad emisora sobre cualquier tipo de incidencia. Cuando compruebe que el pago se ha realizado en su cuenta bancaria, tire tanto los recibos como el resumen.

Compare antes de comprar los productos asociados a la tarjeta de crédito.

Las entidades suelen ofrecen otros productos junto con la tarjeta. Seguros, etc. Generalmente son más caros que la media del mercado, por eso aconsejamos comparar todas las ofertas del mercado. Mas sobre las claves de las tarjetas de crédito

2.12.. Tarjetas de Crédito Caducadas

Cuando le llegue una nueva tarjeta, asegúrese de **eliminar la antigua**. Simplemente córtela por la mitad. Tire los restos de la tarjeta por separado. Más medidas de seguridad tarjetas crédito

2.13. Cuidado con los Duplicados de las tarjetas

A pesar de lo tentador que pueda ser dar duplicado de tu tarjeta a un hijo tuyo o un amigo o empleado, evítelo. La responsabilidad de pagar la deuda será siempre del titular de la tarjeta, no del usuario. Mas la seguridad de las tarjetas de crédito. Recuerde también que la responsabilidad de la protección de la información de la tarjeta (números PIN), y el uso general de la misma es del titular de la tarjeta, no de la entidad emisora.

2.14. Solicitar Tarjetas de Crédito

Factores a considerar al solicitar tarjetas de crédito

- **Comprueba tu historial crediticio**.
  Hay varias agencias donde puedes solicitar tu informe sobre incidencias crediticias. Puedes solicitarlo también a tu banco.
- **Averigua el interés real de la tarjeta de crédito,** TAE
  No hay que dejarse engañar por las ofertas publicitarias. Muchas veces el interés publicado es un interés de lanzamiento y con una duración limitada. Mira siempre el TAE, nunca el interés nominal. Asegura te de que el tipo de interés **es anual no mensual**.
- **Elija tarjetas que le reporten algún beneficio**.
  Busca siempre tarjetas de puntos, o tarjetas con descuentos
- **Mantenga una "Relación entre Deudas e Ingresos" baja**.
- Empieza siempre con un **límite de crédito bajo** y súbelo a medida que te acostumbres al uso de las tarjetas de crédito.
- Al rellenar las solicitudes **diga siempre la verdad**. Si se descubre alguna incoherencia puede suponer la denegación de la tarjeta.
- **No solicites muchas tarjetas al mismo tiempo**.

2.15. Evaluación de la Solicitud Tarjetas Crédito.

Criterios:

- **Valoración de solvencia crediticia:** Es un reflejo de tu seriedad en el pago de tus créditos. Esta valoración se realiza en base a los datos aportados en tu solicitud y sobre todo base a tu **historial crediticio**. Si nunca has dejado de pagar unos préstamos y por lo tanto no tienes

anotación en ningún registro, es muy probable de que consigas una tarjeta con facilidad.

- **Valoración de tu Capacidad crediticia:** Para ello debes considerar **el ratio deudas/ingreso**. El ratio lo obtienes dividendo el total de la deuda mensual por el ingreso neto mensual

  Para calcular este ratio por un parte debes incluir todos tus **pagos mensuales por deudas** (Hipotecas, coches, pagos mínimos de tarjetas, etc.). Y por otra todas tus ingresos líquidos mensuales.
  Guía orientativa de cual sería tu situación en función de este ratio.

  • **30% o menos** es un porcentaje excelente.
  • **20% - 36%** es un buen porcentaje.
  • **36% - 40%** te pone en el límite de la aceptabilidad. Podrían pedirte garantías adicionales.
  • **40% o más** es un porcentaje muy alto que te pondrá las cosas difíciles para solicitar u préstamo o una tarjeta.

- Manejo de tarjetas de crédito. Consejos Prácticos. Seguros asociados a las tarjetas crédito.
  Recomendaciones practicas para hacer el mejor manejo de tarjetas de crédito.

2.16. Como hacer el mejor manejo de Tarjetas de Crédito

A continuación le ofrecemos algunas claves para hacer un buen manejo de tarjetas de crédito

Manejo de Tarjeta de crédito Truco 1: Pague todo el saldo pendiente al final de mes. Cancele su saldo por completo todos los meses.

Si puede permíteselo, cancele su **deuda de la** tarjeta mes a mes. Se ahorrará importantes **comisiones** y dispondrá de crédito gastos extraordinarios.

Figura 2.16. Como hacer el mejor manejo de Tarjetas de Crédito

Manejo de Tarjeta de crédito Truco 2: Pague más que el mínimo

Si no puede pagar el saldo completo, intente pagar todo lo posible. Siempre más que el mínimo. Pagando el mínimo, nunca conseguirá disminuir la duda e incurrirá en unos **intereses** importantes.

Manejo de Tarjeta de crédito Truco 3: Pague puntualmente.

Pagar puntualmente siempre beneficia. Te ahorras importantes gastos en **comisiones de tarjetas de crédito** y te ayuda a tener un buen historial crediticio y buena reputación con el banco.

Manejo de Tarjeta de crédito Truco 4: Nunca omita un pago.

Es lo peor que puedes hacer. Nunca lo haga, le perjudicara no solo por las **comisiones** que le aplicaran, sino en sus **informes de crédito.**

Manejo de Tarjeta de crédito Truco 5: Verifique su estado de cuentas mensual

Asegúrese de que su **estado de cuentas** refleje lo que usted compró. Si aparece algo que no le suene familiar, llame a su compañía de tarjeta de crédito de inmediato.

Manejo de Tarjeta de crédito Truco 6: Compare para obtener las mejores

condiciones en una tarjeta de crédito

Si usted es de las personas que utilizan la tarjeta para como medio de financiación, intente obtener una tarjeta de crédito con una **tasa de interés** baja. Intente conseguir una tarjeta sin cuota anual, o una **tarjeta de puntos** (con reembolso de dinero en efectivo o descuentos en las tiendas).

Mantenga una "Relación entre Deudas e Ingresos" baja.

Asegúrese de contraer deudas que usted sabe podrá cancelar. Si su nivel de deuda llega muy alto, podría afectar su calificación crediticia. Otras **causas de la deuda de las tarjetas de crédito.**

No solicite demasiadas tarjetas de crédito a la vez.

Su situación de riesgo se registra en los distintos informes bancarios, Muchas tarjetas podrían inducir a pesar que usted está pasando por dificultades financieras.

2.17. Principales Problemas con Tarjetas de Crédito

Las tarjetas incitan al gasto.

Uno de los principales problemas con tarjetas de crédito es que se pierde el límite de los gastos, ya que gastar resulta demasiado fácil. El gasto incontrolable puede llevar a acumular deudas impagables. El dinero dispuesto no es un dinero del que se posee sino que es una deuda. Es muy fácil sobrepasarse en el límite de tu disponibilidad sobre todo cuando la tarjeta dispone de un límite my alto

2.18. Efecto Exponencial de los Intereses

Otros de los problemas con tarjetas de crédito es el efecto exponencial de los intereses. El efecto de no pagar el saldo total al final de mes tiene **un efecto espiral sobre los intereses aplicados**. Si un mes no pagas el saldo pendiente, se te aplicara los intereses. El siguiente mes si tampoco pagas el saldo, los intereses se te aplicaran sobre el saldo pendiente más los intereses acumulados, creando un efecto espiral en la deuda.

Con cualquier repago que usted haga, la entidad bancaria liquidará aquellos saldos que les reportan menos tasas de interés, mantenido siempre las mayores.

Figura 2.18. Efecto Exponencial de los Intereses

2.18.1.Pagos Mínimos

Las emisoras de las tarjetas permiten hacer **pagos mínimos. (2,5% de la deuda pendiente).** Sepa que con este sistema nunca conseguirá rebajar la deuda. Con el efecto espiral de los intereses, la rebaja en el principal se compensa con el aumento del interés, quedando el resultado final igual.
Dejar de pagar el pago mínimo también tiene un efecto muy negativo para su

historial de crédito. Más consejos sobre el manejo de las tarjetas de crédito.
A los bancos les interesa este sistema ya que es una forma muy efectiva de cobrar altos intereses.

2.19. Muchas Tarjetas

Es una tentación pensar que cuanto más tarjetas mejor, ya que se tiene un abanico mayor de posibilidades de compra. Hay muchos problemas con esto:

- Más tentaciones para comprar.
- **Más riesgo de fraude en la tarjeta de crédito**
- **Historial Crediticio:** Solicitar muchas tarjetas de crédito al mismo tiempo puede tener una incidencia negativo en tu historial, y puede perjudicarle en el momento de solicitar un préstamo de verdadera necesidad.
- **Puntos:** Los puntos y otros beneficios puede inducirnos a pensar que estamos ganando algo. Sin embargo, estos beneficios se compensan claramente con los intereses de la deuda.

2.20. Riesgos en Uso de las Tarjetas de Créditos

Un día cenando pagas la cuenta con tarjetas de créditos, le das la tarjeta al camarero, quien procesa la operación y después te la devuelve.

Posibilidad de fraude con tarjeta de créditos: el camarero hace una copia de todos los datos de tu tarjeta (número de tarjeta, vencimiento, código de control).
Los utiliza posteriormente para hacer pagos por internet o teléfono.
Otro fraude. Recibes una carta anunciando que has

ganado un viaje gratis y que tienes que hacerte socio de un club de viaje para obtener el viaje. Das los datos de tu tarjeta.

Otros caso. Un ladrón encuentra recibos de tus tarjetas en los basureros cercanos a los cajeros y con esa información puede llegar a realizar comprar.

2.21. Medidas de Seguridad con la Tarjetas de Créditos

Si ha dejado una propina en la mesa tache el espacio en el recibo de la tarjeta destinado a este concepto, incluso ponga mano “propina dejada en la mesa”.

Cuando reciba una nueva tarjeta, no olvide nunca firmar el reverse en el momento de la recepción.

Para llevar las tarjetas de un sitio a otro, utiliza una **cartera distinta para el dinero efectivo y otra para las tarjetas.**

Guarda todos los recibos y justificantes de los pagos y extracciones de efectivos de las tarjetas. Compruébelos con el resumen mensual y después tírelos troceándolos. Más sobre el funcionamiento de tarjetas de créditos.

Si cambias de dirección, notifica inmediatamente tu nueva dirección y asegúrate que las cartas que todavía se reciben en tu

antigua dirección se recojan por alguien de confianza

.

➔ **Nunca escribas el número de tarjeta o el pin en un papel y lo guardes en la cartera.** Cuando pagues en establecimientos públicos con tarjeta de crédito, tache todos los espacios encima de la firma en donde se puedan incluir a mano otras cantidades. **Observa siempre al camarero en todas las transacciones que realice.**

Cuando compres en línea, asegúrate que la web donde compres es segura. La web debería tener un certificado SLL y mostrarlo en la web, ➔ o al menos disponer de un domino que empiece con "https", Más consejos sobre crédito por internet.

Si tienes que dar tu número de tarjeta por teléfono, asegúrate que la compañía a quien das la información es de fiar. Más formas de evitar la ➔ clonación de tarjetas de crédito.

Nunca se te olvide abrir los resúmenes mensuales, incluso si piensas que no has hecho ninguna compra. A veces podrían aparecer compras que no has hecho y debes reclamarlas. Más sobre el ➔ manejo de las tarjetas de crédito

Si observas alguna compra que no identifiques totalmente, debes llamar primero a la empresa o tienda en donde supuestamente hayas hecho esa compra para comprobar la veracidad de dicha compra. Mas sobre ➔ robos de tarjetas de crédito

Si no consigues el nombre de la tienda, o esté totalmente seguro de que no has hecho ninguna compra en este establecimiento, llamar al banco ➔ y denunciar el caso.

Figura 2.21.Medidas de Seguridad con las Tarjetas de Créditos

Capítulo III Implementación de un Monedero Electrónico Seguro sobre el análisis del Protocolo SET

Capítulo III Implementación de un Monedero Electrónico Seguro sobre el análisis del Protocolo SET

3.1. Secure Electronic Transactions

Secure Electronic Transactions es un conjunto de especificaciones desarrolladas por VISA y MasterCard, con el apoyo y asistencia de GTE, IBM, Microsoft, Netscape, SAIC, Terisa y Verisign, que da paso a una forma segura de realizar transacciones electrónicas, en las que están involucrados:

usuario final, comerciante, entidades financieras, administradoras de tarjetas y propietarios de marcas de tarjetas.

SET constituye la respuesta a los muchos requerimientos de una estrategia de implantación del comercio electrónico en Internet, que satisface las necesidades de consumidores, comerciantes, instituciones financieras y administradoras de medios de pago.

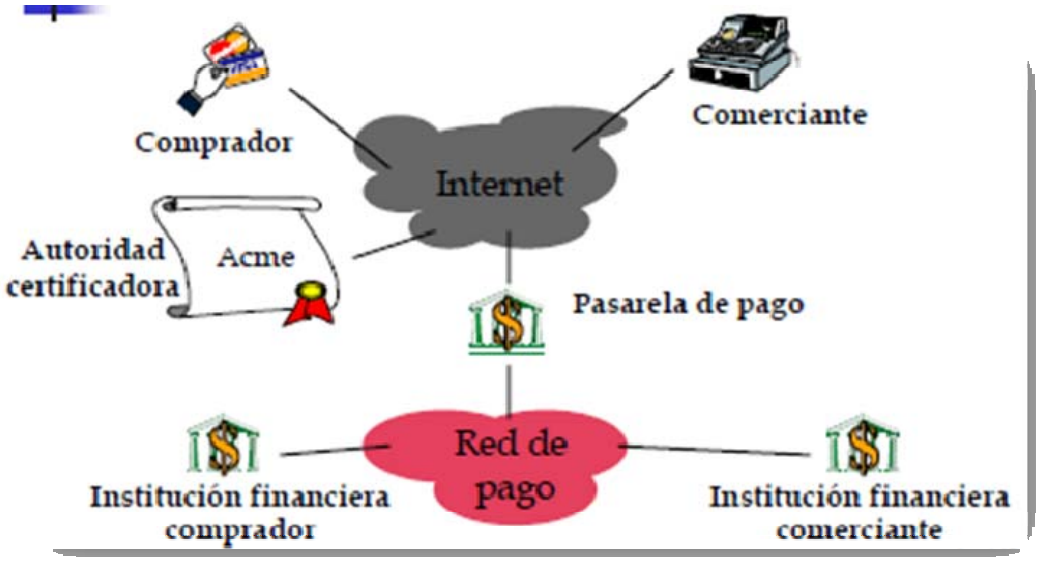


Figura 3.1. Secure Electronic Transactions

3.2. Procesos de los Protocolos SET

- Proporcionar la autentificación necesaria.
- Garantizar la confidencialidad de la información sensible.
- Preservar la integridad de la información.
- Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

Figura 3.2. Procesos de los Protocolos SET

SET utiliza para sus procesos de encriptación dos algoritmos:

- De clave pública RSA (algoritmo simétrico), diseñado por Rivest, Shamir y Adleman, cuyas iníciales componen su nombre.

- De clave privada DES (Data Encryption Standard), de fortaleza contrastada y excelente rendimiento, conocido también como algoritmo asimétrico ya que emplea dos claves diferentes: una para encriptación y otra para desencriptación.

La base matemática sobre la cual trabajan los algoritmos, permite que, mientras un mensaje es encriptado con la clave pública, es necesaria la clave privada para su desencriptación.

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.
Para evitar que la clave pública de un usuario sea alterada o sustituida por otro no autorizado, se crea una entidad independiente llamada Autoridad Certificadora (Certifying Authority, CA), cuya labor consiste en garantizar y custodiar la autenticidad de la claves públicas de empresas y particulares, a través de la emisión de certificados electrónicos*.*

3.3. Seguridad

Qué seguridad proporciona el SET:

- Confidencialidad de los datos de la tarjeta de crédito, ya que al estar el comprador identificado ante la entidad financiera por un certificado digital emitido por ella misma, no es preciso que la información de la tarjeta de crédito viaje, con lo que nunca llega a manos del comerciante ni puede ser interceptada por nadie.
- Integridad de los datos, ya que al viajar encriptados y protegidos por una firma digital no pueden ser alterados en el camino.
- Autenticación del comerciante ante el comprador de que está autorizado para aceptar cobros con tarjetas de crédito.
- Autenticación del cliente ante el comerciante como un legítimo titular de una tarjeta de crédito.

3.4. Implementación de un Monedero Electrónico Seguro sobre el Análisis del Protocolo SET

SET hace seguras las transacciones en línea mediante el uso de certificados digitales.
Con SET se puede verificar que tanto clientes como vendedores están autorizados para realizar o aceptar un pago electrónico.

Desarrollado por Visa y MasterCard.

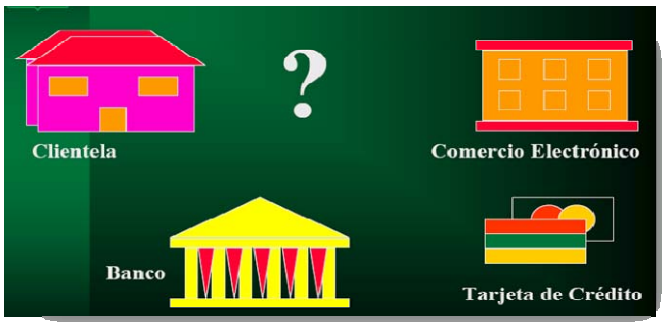
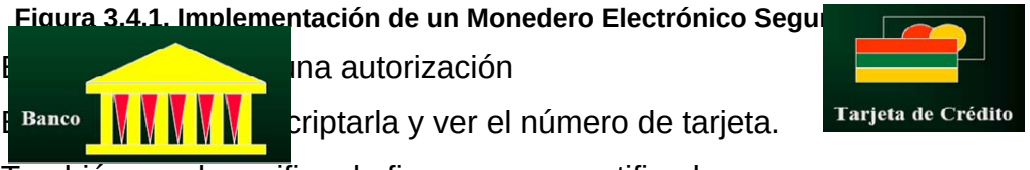


Figura 3.4. Implementación de un Monedero Electrónico Seguro del Protocolo SET

El cliente envía el pedido y una autorización con firma encriptado.
Proveedor no puede tener acceso al número de tarjeta, ya que se encuentra encriptado.

Figura 3.4.1. Implementación de un Monedero Electrónico Segu SET



na autorización
criptarla y ver el número de tarjeta.
También puede verificar la firma con un certificado.

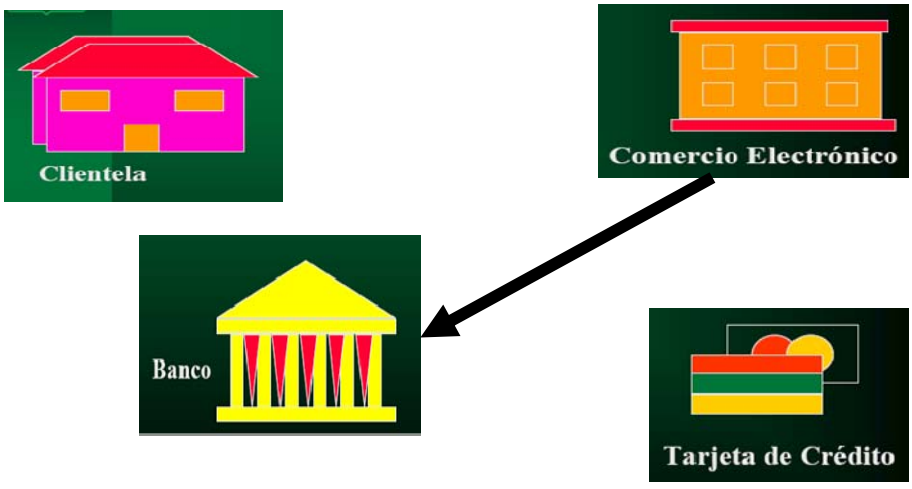


Figura 3.4.2. Implementación de un Monedero Electrónico Seguro del Protocolo SET

El Banco verifica con la compañía emisora de tarjetas para ver si es válida.

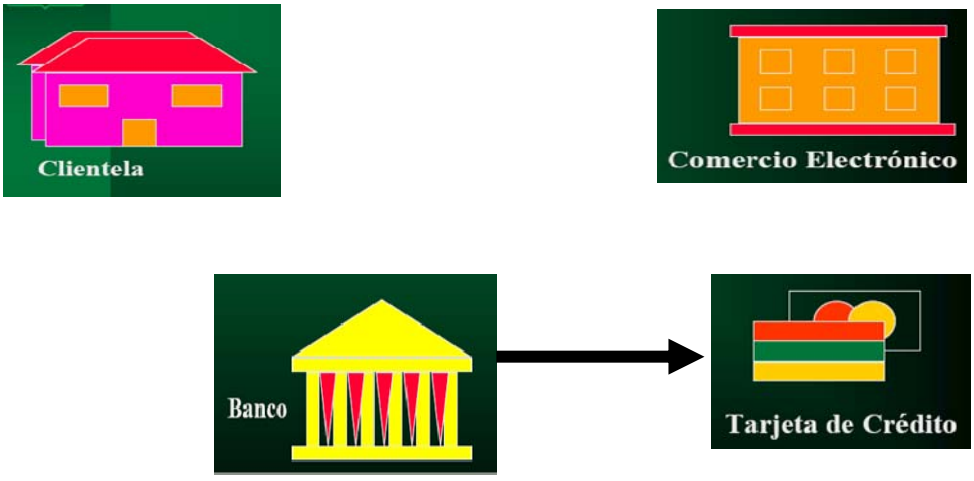


Figura 3.4.3. Implementación de un Monedero Electrónico Seguro del Protocolo SET

La compañía emisora autoriza y firma la transacción.

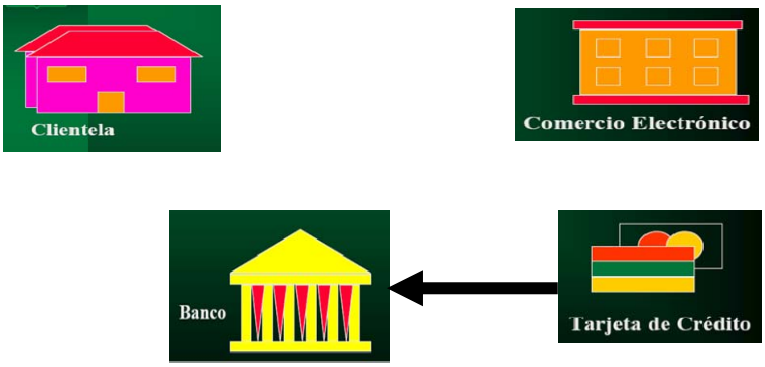


Figura 3.4.4. Implementación de un Monedero Electrónico Seguro del Protocolo SET

El Banco autoriza al proveedor y firma la transacción.

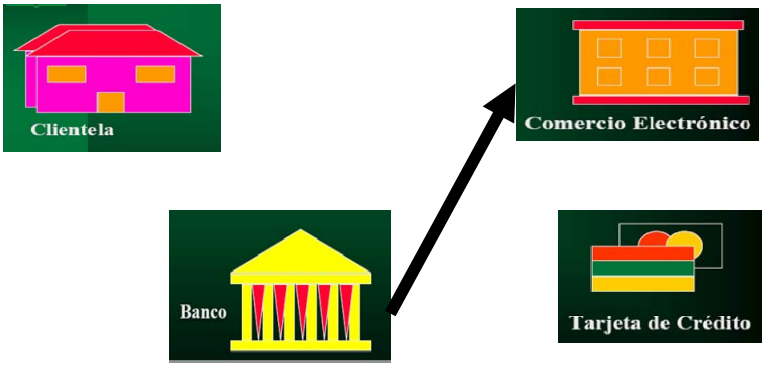


Figura 3.4.5. Implementación de un Monedero Electrónico Seguro del Protocolo SET

El Cliente obtiene lo pedido y un recibo (baucher).

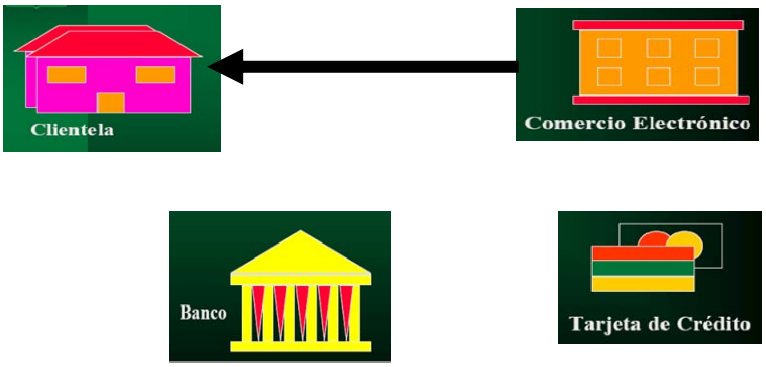


Figura 3.4.6. Implementación de un Monedero Electrónico Seguro del Protocolo SET

El Proveedor solicita “capturar” la transacción y obtener su dinero.

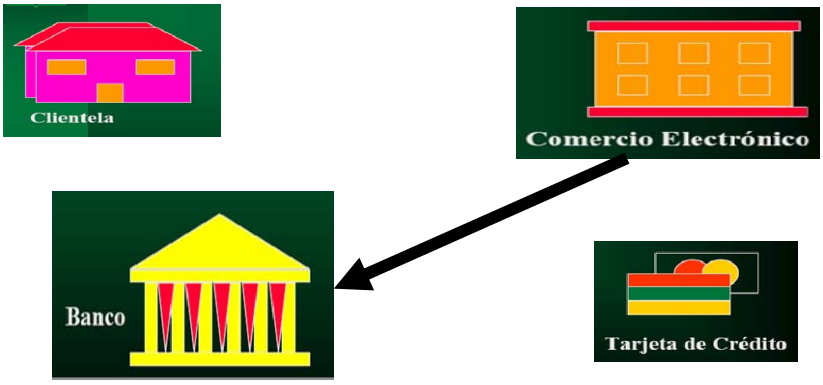


Figura 3.4.7. Implementación de un Monedero Electrónico Seguro del Protocolo SET

El Proveedor obtiene su pago de acuerdo con el contrato.

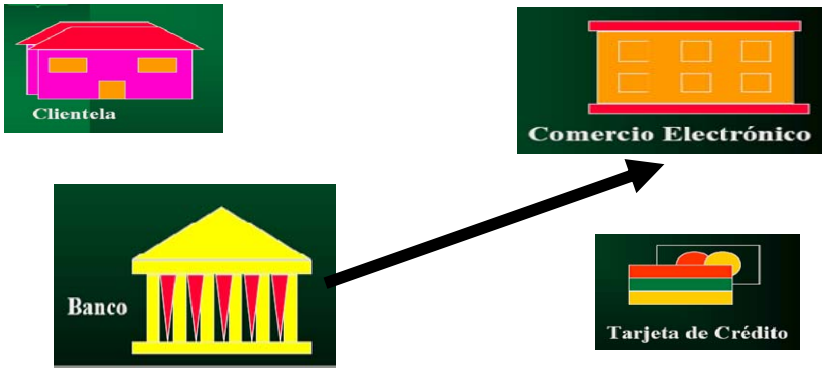


Figura 3.4.8. Implementación de un Monedero Electrónico Seguro del Protocolo SET

El Cliente obtiene el cargo mensual en su tarjeta por parte de la compañía emisora.

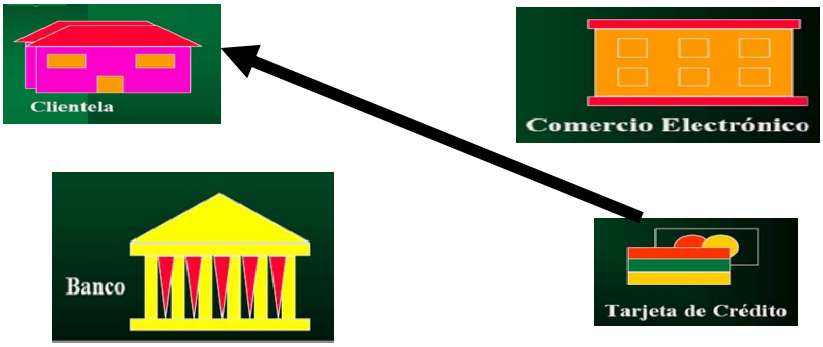


Figura 3.4.9. Implementación de un Monedero Electrónico Seguro del Protocolo SET

3.5. Servicios

Privacidad e integridad de los datos del usuario mediante tarjetas con procesador

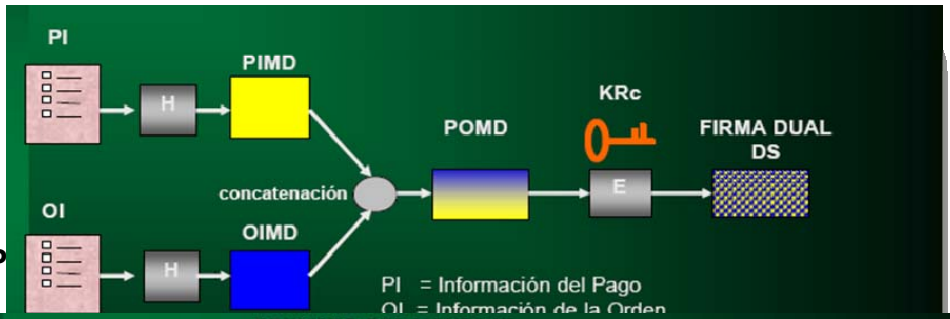
Comunicación segura sobre los canales que conectan a todos los participantes.

Garantía de seguridad 3TP mediante certificados digitales.

Privacidad e integridad de los datos del usuario mediante tarjetas con procesador.

3.6. Firma Dual

3.7. P



3.8.

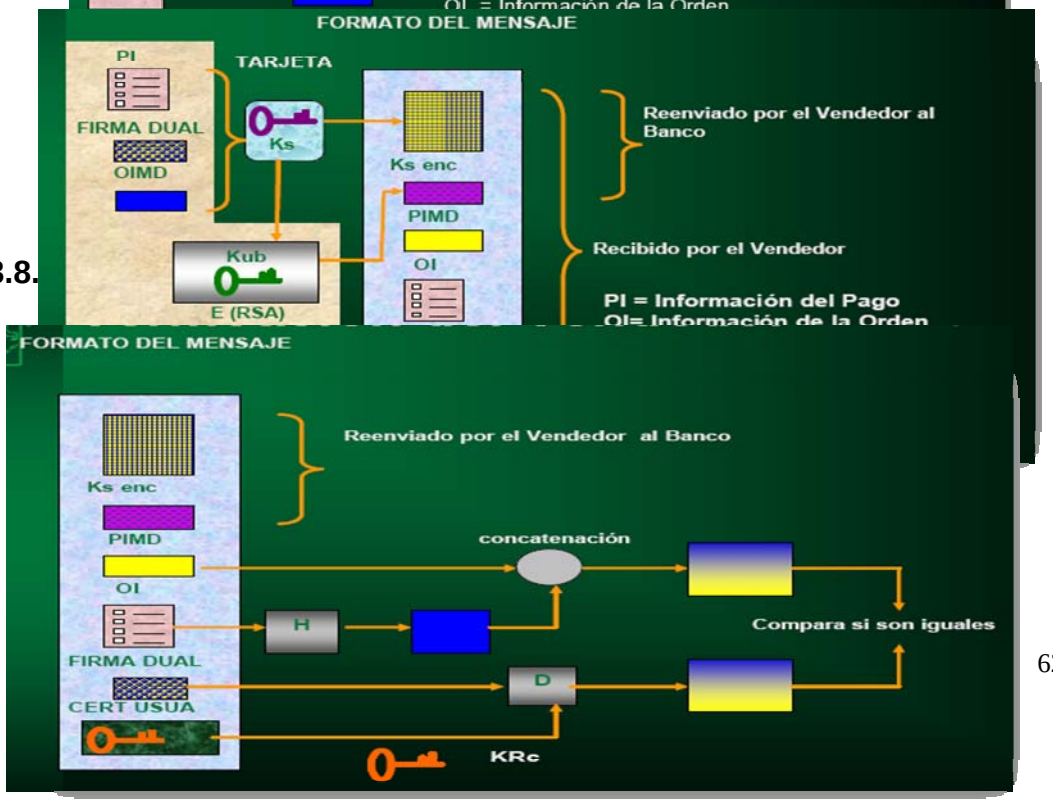


Figura 3.8. Verificación del Vendedor

3.9. SET con Smart Card

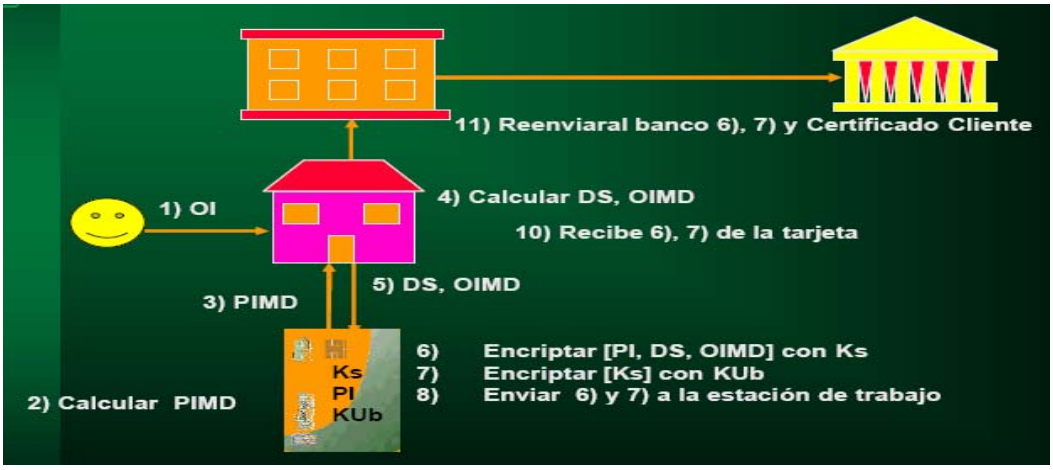


Figura 3.9. SET con Smart Card

3.10. Monedero Electrónico Seguro

CARDLET: Aplicación java que al ser ejecutada habilita las transacciones en el monedero. Dentro de ésta aplicación se guarda lo siguiente:

IDCARD: Identificador único de la tarjeta.
MATRICULA: Matrícula del alumno titular de la smart card.
BALANCE: Corresponde al dinero contenido en la smart card y disponible para su uso
PIN: Numero de Identificación Personal asignado por el titular
kCard y kServ: Llaves de criptográficas del cliente y servidor respectivamente.

Además lo complementan un protocolo de comunicación y 2 aplicaciones para ser ejecutadas en PCs

3.11. Monedero Electrónico Seguro: Protocolo Implementado

1. Para realizar un pago el cliente entrega la tarjeta al comerciante.
2. El comerciante inserta tarjeta en el lector y activa la opción monedero en el Host.
3. El Host solicita al Servidor verifique si la tarjeta es válida.
4. El Servidor verifica y envía aprobación de tarjeta al Host.
5. Host recibe aprobación de tarjeta y requiere PIN del titular.
6. Se ingresa PIN y es enviado a la tarjeta para su aprobación.
7. La tarjeta envía al Host la aceptación del PIN.
8. Host habilita la interfaz para operaciones en el monedero electrónico seguro.
9. En Host se proporciona el monto junto con la transacción a realizar y se envía a la tarjeta
10. La tarjeta recibe y procesa transacción
11. La tarjeta devuelve un paquete al Host para enviarse al Servidor
12. Host recibe el paquete y lo envía al Servidor
13. Servidor registra transacción
14. Comerciante cierra en Host la conexión a la tarjeta
15. El comerciante retira tarjeta del lector y la entrega al Cliente
16. El Cliente recibe su tarjeta

Se activa el monedero en Smart Card se pide el *identificador* para ser Verificado por el Servidor.

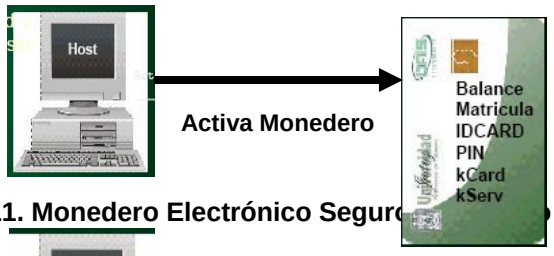
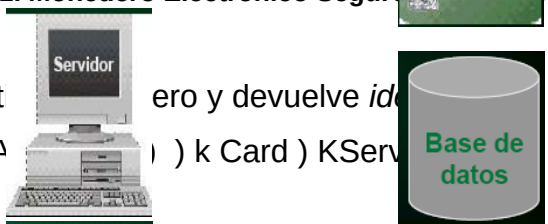


Figura 3.11. Monedero Electrónico Seguro: Protocolo Implementado



La smart card act ero y devuelve *id* al Host.
(Matricula, (IDCA) k Card) KServ

Figura 3.11.1. Monedero Electrónico Segu o Implementado

Host envía el *ider* es recibido por el para su Verificación.

Figura 3.11.2. Monedero Electrónico Seguro: Protocolo Implementado

El Servidor descifra con *kServ* y consulta en base de datos para obtener *kCard*.

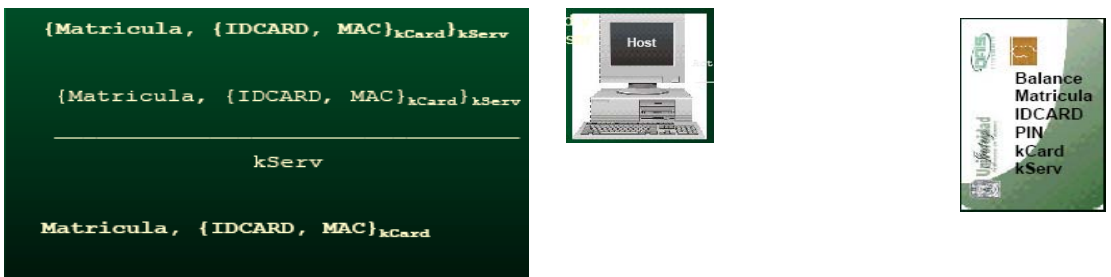
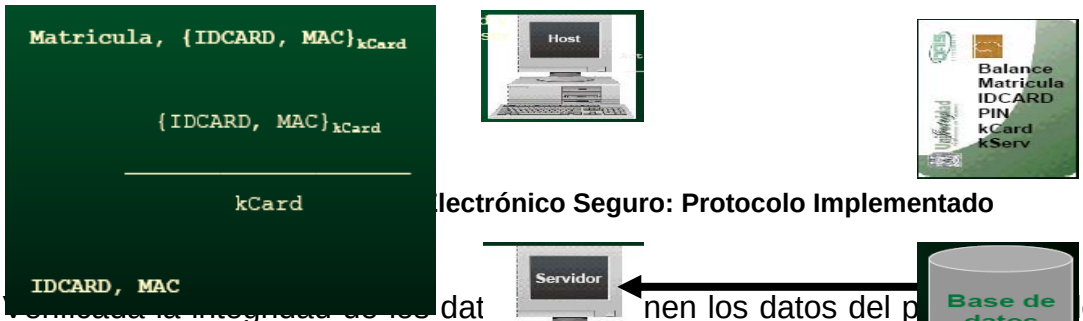


Figura 3.11.3. Monedero Electrónico Seguro: Protocolo Implementado

Se obtiene *kCard* y se descifra, segundo se verifica la integridad de los datos del *identificador*.



lectrónico Seguro: Protocolo Implementado

dat nen los datos del p e la smart card.

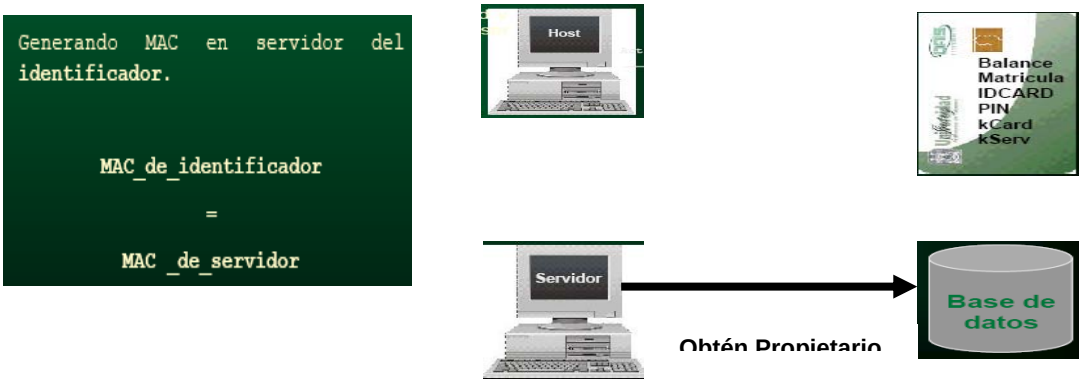


Figura 3.11.5. Monedero Electrónico Seguro: Protocolo Implementado

Se obtienen, preparan y envían los datos del propietario al Host para permitir transacciones en el monedero.

El paquete formado es el siguiente:
{Datos_ propietario}

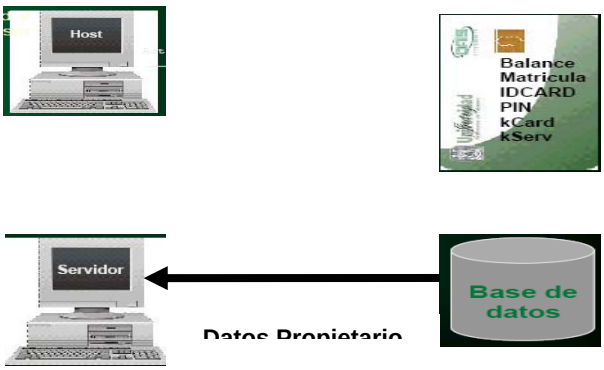


Figura 3.11.6. Monedero Electrónico Seguro: Protocolo Implementado

Se envía el paquete al Host y este lo recibe

Figura 3.11.7. Monedero Electrónico Seguro: Protocolo Implementado

Se muestra los datos del propietario y se requiere ingrese PIN.

Figura 3.11.8. Monedero Electrónico Seguro: Protocolo Implementado

El Cliente ingresa el PIN y se envía a la smart card para su validación.

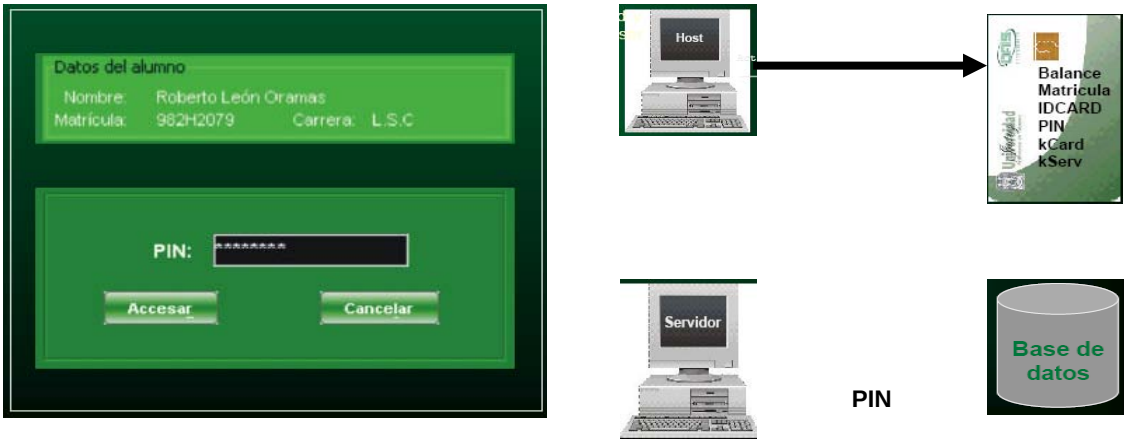


Figura 3.11.9. Monedero Electrónico Seguro: Protocolo Implementado

El PIN es aceptado y se muestra interfaz para transacciones junto con el Balance actual en la smart card.

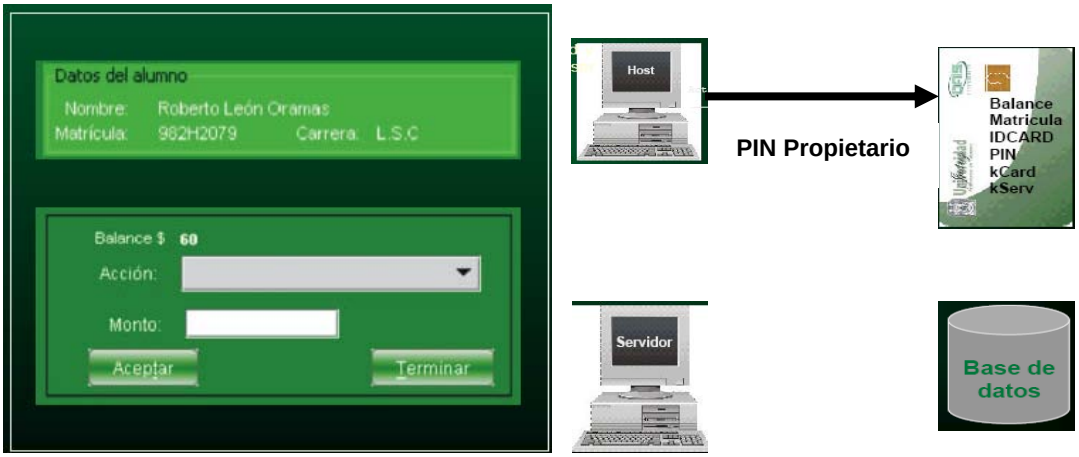


Figura 3.11.10. Monedero Electrónico Seguro: Protocolo Implementado

Selecciona la transacción (incremento o decremento de saldo) a realizar y proporcionando el monto; se envía a la smart card para ser procesado.

{Transacción, Monto}

Figura 3.11.11. Monedero Electrónico Seguro: Protocolo Implementado

La smart card recibe petición de transacción junto con el monto a procesar.

{ Transacción, Monto }

Se realiza el incremento o decremento del Balance.

Incremento:

Balance = Balance + Monto

Decremento:

Balance = Balance – Monto

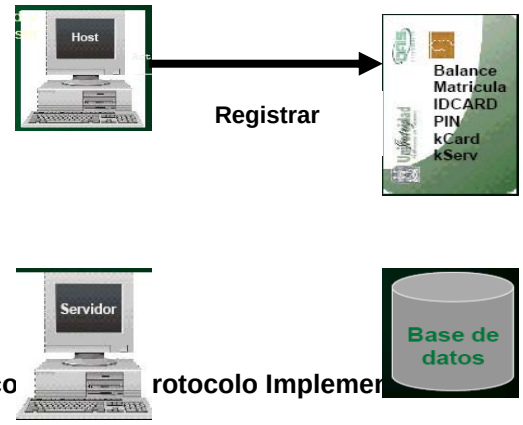
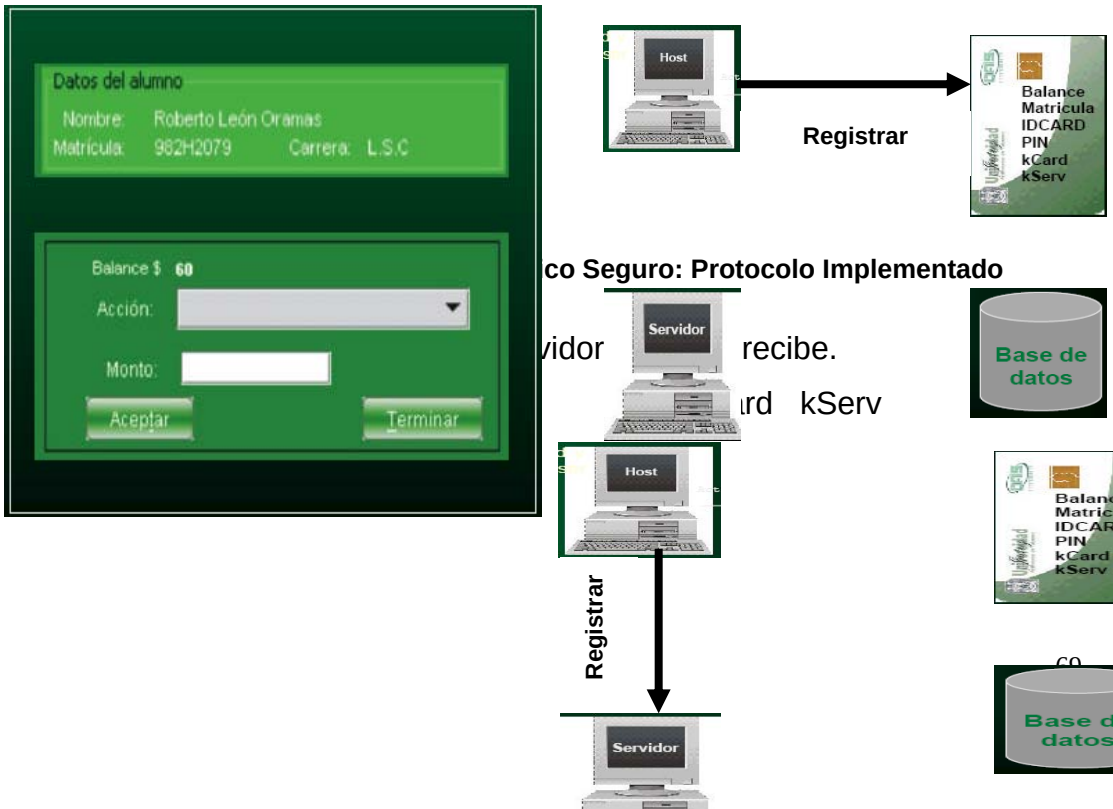


Figura 3.11.12. Monedero Electrónico rotocolo Implemen

Concluido la transacción en la smart card, esta devuelve el paquete *registrar* al Host para ser enviado al Servidor y se actualiza el balance en la interfaz.

{Matricula, {Acción, Monto, MAC} kCard kServ



co Seguro: Protocolo Implementado

vidor recibe.

rd kServ

Figura 3.11.14. Monedero Electrónico Seguro: Protocolo Implementado

Servidor descifra con kServ y consulta en base de datos para obtener kCard.

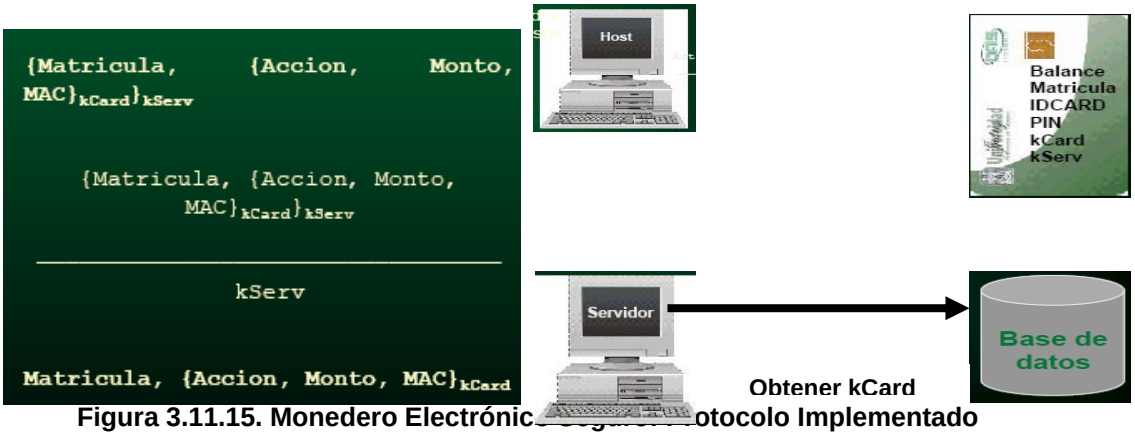


Figura 3.11.15. Monedero Electrónico Seguro: Protocolo Implementado

Se obtiene kCard y se descifra, seguido se verifica la integridad de los datos de *registrar*

Figura 3.11.16. Monedero Electrónico Seguro: Protocolo Implementado

Verificada la integridad de los datos el Servidor registra la transacción.

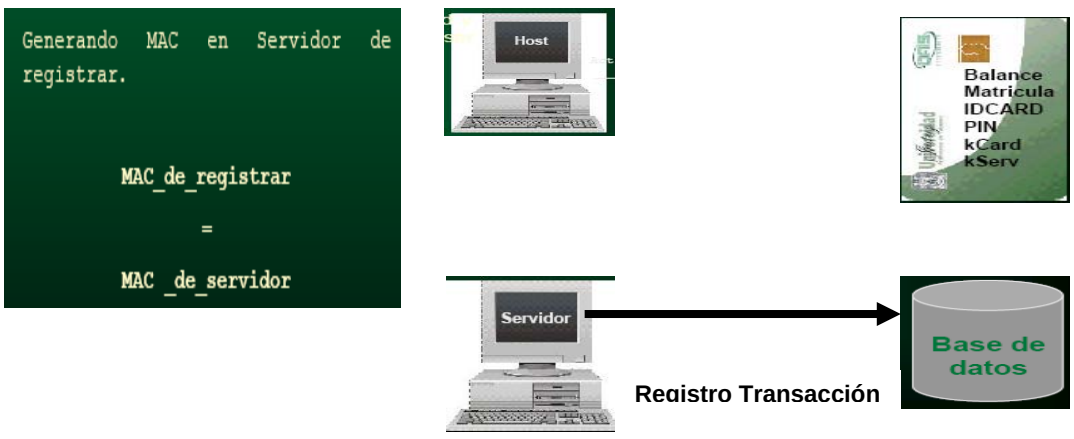


Figura 3.11.17. Monedero Electrónico Seguro: Protocolo Implementado

Así se procede para cada transacción, cada operación debe ser enviada a la smart card, esta debe devolver *proceso terminado*, el dato obtenido en respuesta es enviado al Servidor para su respectivo tratamiento.

Figura 3.11.18. Monedero Electrónico Seguro: Protocolo Implementado

Una vez concluida las operaciones se indica a la aplicación el desactivar y liberar la smart card.

Figura 3.11.19. Monedero Electrónico Seguro: Protocolo Implementado

3.12. Aplicación Cliente: Host *Equipo*

El equipo para punto de venta tiene las siguientes características.

- Computadora con plataforma Linux Red Hat 7.3.

- Java 1.2.
- JBuilder 9.0 versión Personal (incluye el java 1.4.0).
- PCSC.
- JPCSC (Librería para java).
- Lector de smart card instalado, registrado y configurado.
- Tarjeta de Red.

3.12.1. Aplicación Cliente: Host *Función*

Las funciones que realiza la aplicación cliente son las siguientes:

- Habilitar/deshabilitar la conexión a la smart card
- Enviar orden de ejecutar/detener monedero en smart card
- Verificar con el servidor que la smart card sea válida
- Envió de transacciones a la smart card
- Enlace entre el Servidor y la smart card para registro de transacciones.

Ésta aplicación no realiza operaciones de cifrado ó descifrado de datos.

3.14. Smart Card: *Características*

Las smart cards usadas tienen las siguientes características:

- Aplicación Monedero listo para su ejecución
- Microprocesador de 8 bits.
- Memoria EEPROM.
- Soporte java (Java Card)

Capacidades de cifrado/descifrado de datos.

3.15. Smart card: Monedero Electrónico *Función*

Las funciones que realiza el monedero electrónico son las siguientes:

- Recibir del Host la petición de operación (PIN ó transacción)

- Validación de operación requerida
- Notificar al Host la respuesta a su petición
- Datos del titular de la smart card
- Llave propia (aleatoria) y del servidor
- Validación de incremento/decremento de Balance
- Cifrado/generar MAC para los datos a enviarse al exterior.

3.16. Aplicación Servidor: Servidor *Equipo*

El equipo servidor tiene las siguientes características:

- Computadora con plataforma Windows
- JBuilder versión 9.0 Personal (incluye el java 1.4.0)
- Administrador de Base de Datos MySQL.(Appserv 1.4.0)
- Base de Datos SmartCard (MySQL)
- MySQL-Front (utilidad)
- Tarjeta de Red
- Librería
- bcprov-jdk14-121.jar para verificación de
- MAC

3.16.1. Aplicación Servidor: Servidor *Función*

Las funciones que realiza el servidor son las siguientes:

- Descifrado y verificación de integridad de datos
- Enviar aprobación ó rechazo de smart card al Host
- Registrar en la Base de Datos las transacciones.

La función primordial del servidor es descifrar lo cifrado en la smart card comprobando la compatibilidad entre java y la smart card en el mecanismo criptográfico empleado.

3.17. Resultados

Pruebas de Cifrado DES-ECB: Compatibilidad de la criptografía Java y la smart card Cryptoflex.

Se implementó DES como mecanismos criptográfico para proteger la información que viaja al Servidor desde la smart card.

Integridad MAC: Se hace uso de MAC para asegurar que se registra la transacción sin haber sido modificada accidental o intencionalmente

3.18. Trabajo Futuros

Implementar criptografía RSA en la smart card u otros algoritmos como ECC.
Fortalecer el prototipo para soportar la carga de una Red, lo que permitirá implantar el monedero electrónico seguro de manera gradual en las divisiones de la UJAT.
Reforzar la validación del tarjetahabiente haciendo uso de dispositivos biométricos.
Desarrollo de aplicaciones para Windows haciendo uso del monedero electrónico.

Hacer que la tarjeta procese todas las operaciones criptográficas:

- ✓ Huellas,
- ✓ Firma dual y
- ✓ Ks con la llave pública del Banco,
- ✓ Por medio de tarjetas más poderosas

Conclusión

El tema de Protocolos SET Uso de las Tarjetas de Crédito se basa más que nada en un sistema de comunicaciones que permite gestionar de una forma segura las transacciones comerciales en la Red.

Y cuando decimos de una forma segura nos referimos a que aporta un mayor nivel de seguridad que su antecesor el SSL. Precisamente esa fue la razón que dio origen a su nacimiento.

La encriptación es un método excelente ya que nos permite proteger los equipos que se encuentran en red.

Pero lo malo es que existen usuarios que son expertos en infiltrarse en los sistemas más inaccesibles, por eso todos están en peligro, aunque sean muy expertos en ocultar, de sufrir una infiltración que peligre a su sistema con sufrir alguna alteración o daño. Esto lo hace posible la criptología que permite descifrar los códigos y contraseñas, aunque este método es muy difícil de usar.

Parece excelente que exista la encriptación en internet ya que podemos hacer cualquier tipo de trámite que nos da la posibilidad de comprar o vender muy cómodamente, por ello existen tarjetas con números o códigos que nos permiten comprar un bien por internet, además existen las claves que se les dan a usuarios determinados que tengan alguna relación con la empresa o entidad que se las da, que permite trabajar, conseguir entretención, comprar, vender, etc. Es un mercado electrónico que cada vez crece más y que cada vez se usa más por parte de las empresas ya que es el futuro del mercado.

Creo que el Comercio Electrónico es muy similar al común y corriente que conozco, pero tiene la ventaja de que es más rápido y no hay que pasearse por varios lugares para encontrar lo que uno está buscando.
Por lo visto es seguro ya que se requiere descifrar la clave del cliente y la del servidor para poder extraer la información personal de las personas envueltas en la venta del producto.

El método de encriptación parece ser muy eficiente ya que es bastante difícil desencriptar un mensaje oculto y sobre todo si los involucrados se preocupan de la confidencialidad de los datos personales, ya sea cambiando seguidamente las claves o cambiando el lugar donde se guardan éstas.

Los avances tecnológicos permiten reforzar la seguridad de la información mediante dispositivos externos que no dependen del poder de cómputo del equipo Host.

Conclusión

El tema de Protocolos SET Uso de las Tarjetas de Crédito se basa más que nada en un sistema de comunicaciones que permite gestionar de una forma segura las transacciones comerciales en la Red.

Y cuando decimos de una forma segura nos referimos a que aporta un mayor nivel de seguridad que su antecesor el SSL. Precisamente esa fue la razón que dio origen a su nacimiento.

La encriptación es un método excelente ya que nos permite proteger los equipos que se encuentran en red.

Pero lo malo es que existen usuarios que son expertos en infiltrarse en los sistemas más inaccesibles, por eso todos están en peligro, aunque sean muy expertos en ocultar, de sufrir una infiltración que peligre a su sistema con sufrir alguna alteración o daño. Esto lo hace posible la criptología que permite descifrar los códigos y contraseñas, aunque este método es muy difícil de usar.

Parece excelente que exista la encriptación en internet ya que podemos hacer cualquier tipo de trámite que nos da la posibilidad de comprar o vender muy cómodamente, por ello existen tarjetas con números o códigos que nos permiten comprar un bien por internet, además existen las claves que se les dan a usuarios determinados que tengan alguna relación con la empresa o entidad que se las da, que permite trabajar, conseguir entretención, comprar, vender, etc. Es un mercado electrónico que cada vez crece más y que cada vez se usa más por parte de las empresas ya que es el futuro del mercado.

Creo que el Comercio Electrónico es muy similar al común y corriente que conozco, pero tiene la ventaja de que es más rápido y no hay que pasearse por varios lugares para encontrar lo que uno está buscando.
Por lo visto es seguro ya que se requiere descifrar la clave del cliente y la del servidor para poder extraer la información personal de las personas envueltas en la venta del producto.

El método de encriptación parece ser muy eficiente ya que es bastante difícil desencriptar un mensaje oculto y sobre todo si los involucrados se preocupan de la confidencialidad de los datos personales, ya sea cambiando seguidamente las claves o cambiando el lugar donde se guardan éstas.

Los avances tecnológicos permiten reforzar la seguridad de la información mediante dispositivos externos que no dependen del poder de cómputo del equipo Host.

Glosario

Glosario

Autenticación: Todas las partes involucradas en la transacción económica (el cliente, el comerciante y los bancos, emisor y adquiriente) pueden verificar mutuamente sus identidades mediante certificados digitales. De esta forma, el comerciante puede asegurarse de la identidad del titular de la tarjeta y el cliente, de la identidad del comerciante.

Autoridad de Certificación: Servicio ofrecido por su banco (o la entidad delegada) para firmar digitalmente claves públicas que le son remitidas por un navegador o el software del servidor del comerciante.

Banco Adquiriente: Forma relación con el comerciante, procesando las transacciones con tarjeta y las autorizaciones de pago.

Banco Emisor: Emite la tarjeta del cliente, extiende su crédito y es responsable de la facturación, recolección y servicio al consumidor. En el artículo 46 de la Ley de Comercio Minorista se establece que cuando el importe de una compra hubiese sido cargado utilizando el número de una tarjeta de crédito, sin que ésta hubiese sido presentada directamente o identificada electrónicamente (por ejemplo por un hacker que robó el número en Internet), su titular podrá exigir la inmediata anulación del cargo.

Carrito de la Compra: Elemento de un catálogo en línea que mantiene una relación de los artículos que ha decidido comprar. Al terminar la compra, se pasa por la caja virtual y se paga el conjunto usando SET.

Certificados de Autenticidad: Como se ha visto la integridad de los datos y la autenticidad de quien envía los mensajes es garantizada por la firma electrónica, sin embargo existe la posibilidad de suplantar la identidad del emisor, alterando intencionalmente su clave pública.

Certificado Digital: Clave pública que ha sido firmada por una autoridad de certificación confiable (como por ejemplo su banco) para identificar a los comerciantes y compradores cuando hagan uso de esta clave. Contiene además datos personales de identificación del usuario. Estos certificados se usan para la protección de la información de pago.

Clave Privada: Clave que debe permanecer secreta, ya que permite descifrar los mensajes recibidos cifrados con la clave pública, así como firmar mensajes. Ver Criptografía de Clave Pública.

Clave Pública: Clave que otras personas pueden conocer para enviar

mensajes cifrados a su propietario o para verificar la firma de mensajes firmados por él. Ver Criptografía de Clave Pública.

Comerciante: Vende productos, servicios o información y acepta el pago electrónico. La parte débil en las transacciones electrónicas es el comerciante, a quien corresponde probar que su abono está justificado (a no ser que responda el banco o entidad financiera titular de la tarjeta, todo depende del contrato que tenga con el comerciante).

Confidencialidad: La información de pago se cifra para que no pueda ser espiada mientras viaja por las redes de comunicaciones. Solamente el número de tarjeta de crédito es cifrado por SET, de manera que ni siquiera el comerciante llegará a verlo, para prevenir fraudes. Si se quiere cifrar el resto de datos de la compra, como por ejemplo qué artículos se han comprado o a qué dirección deben enviarse, debe recurrirse a un protocolo de nivel inferior como SSL.

Criptografía: Es la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos y cifras. La palabra criptografía se limita a veces a la utilización de cifras, es decir, métodos de transponer las letras de mensajes (no cifrados) normales o métodos que implican la sustitución de otras letras o símbolos por las letras originales del mensaje, así como diferentes combinaciones de tales métodos, todos ellos conforme a sistemas predeterminados.

Criptografía de Clave Pública: Utiliza dos claves, una pública (conocida por todos) y otra privada (sólo conocida por el propietario), matemáticamente relacionadas, de manera que mensajes cifrados con una de ellas sólo pueden ser descifrados si se conoce la otra.

DNI: Es el documento público que acredita la auténtica personalidad de su titular, constituyendo el justificante completo de la identidad de la persona. Será imprescindible para justificar por sí mismo y oficialmente la personalidad de su titular, y servirá para acreditar, salvo prueba en contrario, la nacionalidad española de su titular y los datos personales que en él se consignan.

Financiación: Recibes un préstamo gratis por la duración del periodo de gracia**,** normalmente unos 20 a 25 días. No obstante hay que tener claro cómo eliminar las deudas con tarjetas de crédito.

Firma Digital: Sirven para asegurar la integridad y la autenticidad de los mensajes. Representan el equivalente digital de la firma convencional dibujada a mano.

Firma Dual: Aplicación novedosa de las firmas digitales introducida por SET. Consiste en firmar los mensajes de manera que tanto el comerciante como el banco puedan verificar su integridad y autenticidad, pero sin acceder a los contenidos destinados a la otra parte.

Firmas Electrónicas: Las relaciones matemáticas entre la clave pública y la privada del algoritmo asimétrico utilizado para enviar un mensaje, se llama firma electrónica (digital signatures). Quien envía un mensaje, cifra su contenido con su clave privada y quien lo recibe, lo descifra con su clave pública, determinando así la autenticidad del origen del mensaje y garantizando que el envío de la firma electrónica es de quien dice serlo.

Los Hackers: Son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección. Su motivación abarca desde el espionaje industrial hasta el mero desafío personal. Internet, con sus grandes facilidades de conectividad, permite a un usuario experto intentar el acceso remoto a cualquier máquina conectada, de forma anónima.

Integridad: Garantiza que la información intercambiada, como el número de tarjeta, no podrá ser alterada de manera accidental o maliciosa durante su transporte a través de redes telemáticas. Para lograrlo se utilizan algoritmos de firma digital, capaces de detectar el cambio de un solo bit.

Intimidad: El banco emisor de la tarjeta de crédito no puede acceder a información sobre los pedidos del titular, por lo que queda incapacitado para elaborar perfiles de hábitos de compra de sus clientes.

Logo SET: Es el sello que le indica que el comerciante está usando software que ha superado con éxito el test de Certificación de Software SET.

Monedero Digital: Constituye el remedo digital de la cartera o monedero donde almacena sus tarjetas de crédito y su identificación personal. En el monedero digital, toda esta información se encuentra protegida por una contraseña que usted establece. Es el encargado de efectuar diligentemente todos los pasos del protocolo SET una vez ha pulsado el botón de Pagar.

No repudio para resolución de disputas: La mayor ventaja de SET frente a otros sistemas seguros es la adición al estándar de certificados digitales (X.509v3), que asocian la identidad del titular y del comerciante con entidades financieras y los sistemas de pago. Estos certificados previenen fraudes para los que otros sistemas no ofrecen protección, como el repudio de una transacción (negar que uno realizó tal transacción), proporcionando a los compradores y vendedores la misma confianza que las compras.

Pasarela de Pagos: Mecanismo mediante el cual se autoriza y procesan las transacciones del comerciante (autorización, revocación, liquidación, etc.). La pasarela puede pertenecer a una entidad financiera (adquiriente) o a un operador de medios de pago.

Puntos de Tarjetas: Hay tarjetas de puntos con los que acumulas puntos canjeables por otros artículos (billetes de avión, gasolina etc.). Hay otras que te devuelven un % del dinero gastado.

Procesador (redes de medios de pago): Proporciona servicios adicionales operando la infraestructura de telecomunicaciones sobre las que se realizan las transacciones.

Seguros de compra: Muchas tarjetas tienen un seguro asociado que te garantizan contra el robo del producto. Cuando contratas un vuelo o un viaje con la tarjeta, puedes beneficiarte de un seguro de viaje.

SET: El protocolo SET (Secure Electronic Transaction) es un estándar desarrollado por Visa y MasterCard para dotar de máxima seguridad a los pagos en línea por Internet y otras redes abiertas.

Software de la Autoridad de Certificación: Las entidades financieras que decidan soportar el estándar SET necesitarán este software para que sus respectivos clientes (titulares de tarjetas y comerciantes que aceptan pago con tarjeta) puedan participar en el juego. Permite registrar a los usuarios y emitir certificados digitales para ellos, que aseguren la confianza entre las partes. Además, tanto los clientes como los comerciantes necesitan certificados para garantizar la identidad de los participantes.

Software de Cartera del Titular: Aplicación 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.

Software de Punto de venta del Comerciante: Para que el sitio web del comerciante acepte pagos con SET necesitará instalar una aplicación de Terminal de Punto de Venta (POST) compatible con SET en su servidor, que acepte los pedidos y procese los pagos con el banco. Para obtener un listado de empresas que comercializan aplicaciones POST que hayan sido certificadas.

Software del Servidor de la pasarela de Pagos: Realiza el procesamiento automatizado de los pagos. La pasarela recibe peticiones de autorización/liquidación/reconciliación de pagos de los sistemas del comerciante (POST) en Internet y las encamina hacia los sistemas de pago propietarios (sistemas de autorización tradicionales).

SSL: El protocolo Secure Socket Layer (SSL), desarrollado por Netscape, permite la creación de un canal cifrado entre el servidor Web y el navegador, por el cual se puede transmitir información de forma segura en uno y otro sentido.

Titular de la tarjeta: Posee la tarjeta emitida por el banco emisor y realiza y paga las compras.

Verificación Inmediata: Proporciona al comerciante una verificación inmediata, antes de completarse la compra, de la disponibilidad de crédito y de la identidad del cliente. De esta forma, el comerciante puede cumplimentar los pedidos sin riesgo de que posteriormente se invalide la transacción.

Bibliografía

Bibliografía

- ✓ León O. R., Lizama P. L.: Monedero Electrónico Seguro. Universidad Juárez Autónoma de Tabasco, México (2005)
- ✓ Lizama P. L., Gómez R.: Autenticación Biométrica On Card en el Protocolo de Kerberos.
- ✓ Memoria del Segundo Congresos Iberoamericano de Seguridad Informática. México (2003) 249-266
- ✓ The source for Developers – A Sun Developers Network Sites.
- ✓ http://wireless.java.sun/Javacard/articles/Javacard02/. An Introduction to Java Card
- ✓ Technology – Part 2, The Java Card Applet. Sun Microsystems.

- ✓ CryptoflexTM Cards Programmer's Guide. Cyberflex Access SoftwareDevelopment Kit 4.3. (2002) C300474_rev1.
- ✓ CyberflexTM Access Software Development Kit Release 3C. Cyberflex Access Programmer 's Guide. (2000) C300451.
- ✓ Java Card Applet Developer's Guide. SUN Microsystems. Rev 1.10, July 17, (1998)
- ✓ Stallings, J.: Cryptography and Network Security, Prentice Hall.U.S.A., 3th Ed. (1998)
- ✓ Jerdoney R., et al.: Implementation of a Provably Secure, Smartcard-based Key
- ✓ Distribution Protocol. CITI Technical Report. (1998) 4
- ✓ Giampaolo B.: Modelling Security Protocols Based on Smart Cards. Computer
- ✓ Laboratory, University of Cambridge.
- ✓ Ferrari J., *et al.*
- ✓ Smart Cards: A Case Study. International Technical Support Organization.
- ✓ http://www.redbooks.ibm.com

Páginas de Internet

- ✓ http://www.creaciondempresas.com/serv_gratuitos/albanova/ecommerce/art4.asp
- ✓ HTTP://WWW.VIRTUAL.UNAL.EDU.CO/CURSOS/SEDES/MANIZALES/4060038/LECCIONES/MODULO%201/CAPITULO%206/PROTOCOLOS.HTM#ARRIBA
- ✓ http://www.wikilearning.com/curso_gratis/curso_de_criptografia_basica_para_principiantes-protocolos_de_seguridad/4306-9
- ✓ http://www.monografias.com/trabajos11/comele/comele.shtml
- ✓ http://www.economia.com.mx/el_uso_correcto_de_su_tarjeta_de_credito.htm

- ✓ http://www.economia.com.mx/decalogo_para_el_uso_de_la_tarjeta_de_credito.htm
- ✓ http://www.las-tarjetas-credito.com/
- ✓ http://www.las-tarjetas-credito.com/Definicion_de_tarjeta_de_credito_Para_que_sirven.html
- ✓ http://www.las-tarjetas-credito.com/Claves_de_tarjetas_de_credito_Como_sacar_el_mejor_rendimiento.html
- ✓ http://www.las-tarjetas-credito.com/Como_se_usan_las_tarjetas_de_credito_No_cometa_errores.html
- ✓ http://www.las-tarjetas-credito.com/Solicitar_Tarjetas_de_Credito_La_mejor_Guia.html
- ✓ http://www.las-tarjetas-credito.com/Manejo_de_tarjetas_de_credito_Consejos_practicos.html
- ✓ http://www.las-tarjetas-credito.com/Que_son_tarjetas_de_credito_Principales_Ventajas.html
- ✓ http://www.las-tarjetas-credito.com/Principales_problemas_con_tarjetas_de_credito.html
- ✓ http://www.las-tarjetas-credito.com/Tarjetas_de_creditos_Aprenda_a_utilizarlas.html
- ✓ http://www.las-tarjetas-credito.com/Clases_de_tarjetas_de_credito.html
- ✓ http://www.monografias.com/trabajos11/comele/comele.shtml
- ✓ http://grasia.fdi.ucm.es/jpavon/agentes/tema43.pdf
- ✓ http://www.creaciondempresas.com/serv_gratuitos/albanova/ecommerce/art4.asp
- ✓ http://www.idg.es/iworld/impart.asp?id=103068
- ✓ http://www.morales-vazquez.com/pdfs/ssl.pdf
- ✓ http://www.arrendamientos.biz/dni.html