UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CONTADURÍA Y
ADMINISTRACIÓN

"ANÁLISIS COMPARATIVO ENTRE ESQUEMAS DE COMERCIO ELECTRÓNICO BASADOS EN TARJETAS DE CRÉDITO"

TESIS PROFESIONAL QUE PARA OBTENER EL
TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

MACIEL MÉNDEZ MOHAMMED GIOVANNI

ASESOR:

M. EN C. LEOBARDO HERNÁNDEZ AUDELO

MÉXICO, D.F. 2000

RESUMEN

La tecnología como agente de cambio, viene jugando desde hace tiempo un papel muy importante para mejorar la calidad de vida de las personas. Esta influencia se ha incrementado conforme el uso de la tecnología gana terreno dentro de la vida cotidiana de las comunidades actuales, llegando incluso a convertirse en algo indispensable, convirtiéndose en muchos casos en un elemento de primera necesidad.

Anteriormente las tecnologías de aparición reciente estaban disponibles a precios considerablemente altos, siendo necesario esperar un período de tiempo significativo, antes de que estuvieran al alcance de la mayoría de las personas. En la actualidad esta situación está cambiando, permitiendo que las nuevas tecnologías puedan adquirirse a precios muy accesibles desde su lanzamiento al mercado. Un ejemplo de este cambio lo ofrecen las computadoras. Cuando estos equipos comenzaron a comercializarse, hace algunas décadas, sus precios elevados provocaban que sólo una porción muy reducida de la población mundial pudiera adquirir alguno, por lo que eran instituciones como universidades, compañías de gran tamaño y centros de investigación las que tenían acceso a equipo de este tipo. Sin embargo, hoy en día, un gran porcentaje de la población mundial, que se incrementa a diario, posee o utiliza alguna computadora; ya sea en su casa, escuela, trabajo, etc.

Este número elevado de usuarios de computadoras distribuidas alrededor del planeta junto con el abaratamiento en costos y los avances de la tecnología de cómputo y telecomunicaciones, son tres de los principales factores que han permitido la formación de redes de computadoras de un creciente tamaño y capacidad de transmisión. Estas *redes de computadoras*[1] están formadas por varias computadoras independientes y conectadas a través de redes de telecomunicaciones, cuya función principal consiste en permitir el intercambio de recursos entre los equipos que las forman.

Esta independencia de los equipos que forman una red en particular, provoca en muchos casos que tales equipos sean de diferente marca, modelo, etc., razón por la cual, se requiere de *protocolos de comunicación* para que los diferentes equipos logren entenderse y comunicarse entre sí. Estos protocolos consisten en una serie de pasos ordenados y preestablecidos, que dos o más partes acuerdan para desempeñar alguna tarea específica.

Dentro de un protocolo, cada paso involucra mensajes que se intercambian entre los equipos que intervienen en él, y que guían el comportamiento del mismo. Los mensajes más comunes son, entre otros: los de inicio, cancelación o finalización del protocolo. Sin embargo, cada protocolo establece mensajes específicos de acuerdo a su función. Un aspecto de gran importancia dentro de los protocolos es el orden de los pasos que lo

[1] En este trabajo, las *cursivas* se utilizan para identificar conceptos utilizados por primera vez

forman, el cual debe estar estrictamente establecido ya que un equipo necesita saber cuando solicitar o enviar información a otro, o por ejemplo, cuando el envío de información ha terminado [2] (pp. 127).

Actualmente la red de computadoras que conecta al mayor número de equipos alrededor de todo el mundo es la *Red Internacional* (*"International Network"*), conocida como *Internet* o *Red de amplitud mundial* (*"World Wide Web"*), también conocido como web.

Al inicio de Internet, cuando dos equipos conectados intercambiaban información, la tecnología disponible permitía que la información se desplegara únicamente en forma de texto. Conforme la tecnología avanzó se añadieron al texto imágenes, voz y video. Hoy en día al uso simultáneo de estos elementos, se le denomina *Multimedia*

Este veloz desarrollo de la tecnología de cómputo y de redes de computadoras está cambiando la forma en que se realizaban muchas transacciones, incluyendo aquellas de naturaleza comercial o financiera, permitiendo que dichas transacciones se puedan efectuar de forma electrónica. Estas nuevas posibilidades no han sido ignoradas por aquellas instituciones financieras y comerciales que a través de la experiencia propia o de la competencia, están conscientes de que incorporar nuevas tecnologías en sus procesos operativos puede representar una ventaja competitiva dentro de los esquemas de libre comercio, que se viven desde hace algunos años en casi todos los países del mundo; situación por lo que dichas entidades buscan con gran interés nuevos esquemas, que les permitan ofrecer a sus clientes la mayor parte de las siguientes características:

a) Ofrecer servicios las 24 horas del día
b) Aprovechar las características que ofrece el web tales como: video, imágenes, texto, audio, etc., para publicitar productos y servicios
c) Permitir que el cliente pueda adquirir algún bien o servicio sin que tenga que salir de su casa o hacer largas filas.
d) Proporcionar al usuario la posibilidad de pagar con su tarjeta de crédito y/o dinero electrónico
e) Reducir el tiempo de las transacciones a sólo algunos segundos
f) Garantizar al usuario o cliente que los datos involucrados en una transacción comercial que viajan por la red, lo hagan protegidos contra lectura, modificación, destrucción o falsificación por parte de personas o entidades no autorizadas. Entre estos datos se incluyen: números de tarjeta, números de identificación personal (NIP's), etc.; además de los datos relacionados con las características de los bienes o productos que se adquieren, tales como la descripción, cantidad, costos, etc.
g) Asegurar al usuario que está realizando la transacción con quien él realmente desea

Estas características, entre otras más, resultan de gran interés y rentabilidad, por lo que un gran número de instituciones y gobiernos del mundo entero están apoyando en mayor o menor grado el desarrollo de los esquemas que las proporcionen. Como una

consecuencia de este apoyo e interés, se espera que en un futuro cercano, el uso de este tipo de esquemas de manera cotidiana.

Este uso frecuente se comienza a percibir sobre todo en los EUA y en algunos países de Europa en los que las compras por internet han comenzado a realizarse desde hace ya algunos años, incrementándose drásticamente en el último par de ellos. Sin embargo, en nuestro país la situación es diferente, ya que la compra de bienes o la contratación de servicios por medio de internet es apenas incipiente. A este respecto es en el ultimo año cuando han comenzado a aparecer las primeros sitios nacionales realmente comerciales en nuestro país en los que en un principio sólo se proporcionaban catálogos electrónicos de sus productos o servicios, para paulatinamente ir incorporando esquemas más avanzados como por ejemplo el pago electrónico de los bienes o servicios adquiridos.

Este avance paulatino ha respondido entre otras razones al nivel de la cultura tecnológica del grueso de la población de nuestro país, a la falta de legislación con respectos a las transacciones comerciales de naturaleza electrónica y a la desconfianza que han mostrado los usuarios de internet al momento de enviar los datos de sus tarjetas a través de internet.

Estas expectativas e incertidumbres representan dos de las motivaciones principales para la realización de este trabajo en el que se realiza un estudio de los diferentes esquemas de Comercio Electrónico (CE), se presentan los protocolos básicos y se realiza un análisis comparativo de algunos de los principales esquemas de CE como son: SSL, iKP, SEPP, y SET, tomando como base de la comparación las técnicas criptográficas que utilizan, su interacción con las instituciones financieras, el costo de cada transacción, complejidad en instalación y uso, y la manera en que proporcionan servicios de seguridad tales como autenticación, confidencialidad, e integridad entre otros.

Se presentan, en tablas comparativas, los resultados obtenidos de este análisis, resaltando las propiedades, ventajas y desventajas de cada uno de ellos con respecto a los demás.

En este sentido el presente trabajo pretende servir como un punto de inicio en la adquisición de conocimientos acerca del concepto general de CE, sus niveles y categorías, así como de las principales características de los cuatro esquemas considerados en el análisis comparativo con respecto a sus niveles de seguridad, de tal modo que se busca proporcionar un acercamiento completo y sencillo que sirva como base de tomas decisiones acerca de la elección adecuada de alguno de estos esquemas para los individuos u organizaciones que les interese incursionar en los niveles avanzados del CE.

CONTENIDO

Capítulo 1

INTRODUCCIÓN

1.1 Antecedentes

Los seres humanos han efectuado transacciones comerciales desde la formación de las primeras sociedades, utilizando diversos métodos a través de los años para tal fin; iniciando con el trueque, pasando por la invención del dinero, hasta llegar a la reciente aparición de una nueva modalidad denominada *Comercio Electrónico*. Esta aparición fue posible gracias a los avances tecnológicos que desde hace un par de décadas se han alcanzado en materia de cómputo, telecomunicaciones, redes de computadoras e informática, principalmente.

Estos avances han abierto mercados enormes en un espacio virtual, libre en muchas ocasiones de distancias y fronteras físicas, y posibilitado por la gran cantidad de equipos conectados a una sola red, como por ejemplo internet; en cuyo auge el CE ha encontrado el terreno ideal para surgir de manera alterna a otras formas de comercio más o menos novedosas, basándose en ocasiones en esquemas de pago ya existentes como el dinero, los cheques o las tarjetas de crédito.

Como su nombre lo indica el CE es aquella actividad que permite realizar transacciones de tipo comercial mediante recursos y medios electrónicos. Dentro del alcance de este trabajo, se considera al término *Transacciones Electrónicas de Tipo Comercial* (TETC) como un sinónimo de CE debido a que este último abarca a todas aquellas transacciones de carácter comercial que se efectúan por medio electrónicos.

Como consecuencia de la naturaleza altamente confidencial de ciertos datos como el número de tarjeta o el nombre y dirección del comprador o vendedor, la información involucrada en las transacciones de CE requieren de una protección suficiente y adecuada para evitar fraudes perpetrados por comerciantes, compradores, o cualquier otra entidad ya sea que esté involucrada directa o indirectamente en la transacción. El número y tipo de estas prácticas fraudulentas es muy amplio y suele incluir: el retiro de fondos de cuentas bancarias sin autorización para ello, cargo del monto de alguna compra a una entidad ajena a dicha transacción, entre otros muchos. Estos riesgos convierten a la seguridad de dicha información en un aspecto fundamental del CE, razón por la cual y debido a que como se estableció el CE se efectúa por medio de computadoras conectadas en red, se requiere el uso de ciertos protocolos. Desafortunadamente la mayoría de estos protocolos, incluyendo

al *Protocolo de Control de Transmisiones/Protocolo Internet (TCP/IP)*[1], ofrecen esquemas de seguridad muy limitados y por lo tanto deficientes, ya que fueron diseñados a finales de los años sesenta y principios de los ochenta, una época en que la preocupación radicaba en compartir información y no en ser seguros. Esta falta de seguridad provoca que la información que viaja de una computadora a otra por medio de estas redes esté expuesta a múltiples amenazas. Estos peligros a los que se enfrenta la información adquieren gran relevancia en el contexto del CE precisamente por la confidencialidad de cierta parte de esta información y del hecho de que se involucra dinero, razones por las cuales se deben de establecer mecanismos que protejan de manera adecuada dicha información. Los conceptos asociados a dicha seguridad se definen a continuación.

La *información* puede ser definida como un estímulo que tiene algún significado en un contexto en particular para quien la recibe. Algunos tipos de información si no es que todos, pueden ser expresados en forma de datos, y ser enviados o transmitidos a otro receptor. En el contexto de este trabajo, la información puede ser entendida como un conjunto de datos relacionados entre sí, almacenados y procesados precisamente como datos para posteriormente ser mostrados como datos en alguna forma que permita que sean percibidos como información [2].

La *seguridad de la información* consiste en todas aquellas actividades y recursos destinados a proteger la información. Esta protección debe garantizar que la información esté en el lugar y en el momento precisos en que se necesite, impidiendo su lectura, modificación, destrucción o falsificación por personas o entidades no autorizadas, independientemente de si la información está almacenada en una máquina o de que viaje por una red de telecomunicaciones [6] (pp. 3-6).

Conforme la tecnología ha evolucionado, los métodos y herramientas para proteger la información también han evolucionado. Hace algunos años cuando la información consistía únicamente de palabras en documentos tangibles, protegerla era simple, bastando con colocar dichos documentos en algún archivero con cerradura y restringir el acceso a dicho archivero. En la actualidad, por el contrario, mucha de la información que se genera son bits almacenados, o que viajan a través de redes de telecomunicaciones. Proteger y asegurar la información en este último caso no es una labor tan sencilla.

En un pasado más reciente, cuando los equipos de cómputo trabajaban de forma independiente unos de otros y no podían comunicarse entre sí, los accesos o modificaciones a la información por partes no autorizadas, resultaban menos viables y, por lo tanto, dañinos. Sin embargo, es a partir de la conexión de las computadoras por medio de redes como Internet, con sus deficiencias de seguridad inherentes (que como ya se mencionó muchas de los cuales radican en el diseño de los protocolos de redes), que proteger la información se ha complicado considerablemente. De estas circunstancias surge la innegable necesidad de herramientas automatizadas para proteger archivos y todo tipo de información. Esta necesidad es especialmente evidente en el caso de sistemas abiertos, en los que varios equipos pueden compartir recursos entre sí por medio de redes públicas de voz y datos. La denominación genérica para el conjunto de herramientas diseñadas para

[1] Este protocolo es el utilizado para la comunicación en Internet
[2] www.wathis.com

proteger datos durante su almacenamiento y transmisión, y frustrar los intentos de posibles intrusos es *seguridad en cómputo* [1] (pp. 1-1).

Con el fin de ejemplificar la importancia y complejidad de la seguridad de la información hoy en día, basta imaginar un escenario en que una persona no autorizada obtuviera de alguna forma acceso a la información de la base de datos de cierto banco. Esta persona obtendría acceso a información tan confidencial como: el nombre, las direcciones, los teléfonos, los números de cuenta, los estados de cuenta, etc. de los tarjeta-habientes. Con estos datos la persona estaría en capacidad de: transferir a su cuenta fondos de otras cuentas, proporcionar datos de otros tarjeta-habientes para efectuar compras o transacciones en su beneficio, conocer el historial médico de los mismos; tener conocimiento de lo que compran, a dónde viajan, dónde se hospedan, con quién interactúan y el contenido de sus comunicaciones; todo esto gracias a la integración de bases de datos de otras corporaciones con la del banco, a través de redes de telecomunicaciones.

Es por todo lo anterior que conforme las comunicaciones interpersonales, el trabajo y las transacciones de tipo comercial comienzan a efectuarse en el web, la preocupación por brindar la seguridad adecuada a la información involucrada en tales comunicaciones se incrementa día con día. En respuesta a esta preocupación, se han implementado ciertos métodos de seguridad conocidos como *servicios de seguridad.* La descripción detallada de estos servicios junto con la de sus antagónicos, los ataques contra la seguridad, se describen a continuación.

1.2 Servicios de seguridad y ataques contra la seguridad

1.2.1 Servicios de seguridad

Para proporcionar la protección adecuada a la información existen los *servicios de seguridad*, cuya adecuada implementación garantiza el prevenir y proteger al equipo de cómputo y a la información contra ataques a los mismos, y que pueden consistir de uno o más mecanismos de seguridad, los cuales son diseñados para detectar, prevenir o recuperarse de un ataque. Tales servicios de seguridad son los siguientes [1] (pp 4-5):

Confidencialidad

Este servicio garantiza que la información en un sistema de archivos y la transmitida sea accesada para lectura, sólo por las partes autorizadas. En el contexto específico de las TETC, la confidencialidad consiste en restringir ciertas piezas de información relacionadas a la transacción, por ejemplo el número de la tarjeta del comprador. En ocasiones la confidencialidad es conocida también como *privacia* [1](pp 10), [2](pp 5) y [9](pp).

Integridad

Implica que la información propia y la transmitida por un sistema, pueda ser modificada sólo por las partes y/o maneras autorizadas. En el contexto de las TETC,

la integridad está estrechamente vinculada a la *autorización*, entendiéndose autorización no en el sentido de un filtro de acceso, sino como una autorización formal y explícita ya sea de parte del comprador y comerciante que garantice por una parte que el retiro de dinero de la cuenta de algún comprador sólo pueda efectuarse con su previo consentimiento, y por la otra que el depósito de cierta cantidad en la cuenta de algún vendedor sólo se pueda realizar con el consentimiento de éste[1](pp 11), [2](pp 5) y [9].

No-repudio

Permite que ni la parte que envía, ni la parte que recibe la información sean capaces de negar que lo enviaron o que lo recibieron. Este servicio, que es uno de los principales en el contexto de las TETC se implementa por medio de firmas digitales[1](pp 11), [9] y [2](pp 5).

Disponibilidad

Consiste en que un recurso de cómputo o información esté disponible cuando sea requerido por las partes autorizadas, garantizando que el acceso a tales recursos no les pueda ser negado. [1](pp 12) y [2](pp 5)

Autenticación

Servicio que se presenta en dos modalidades: por una parte la autenticación de *origen del mensaje* en la que la identidad de un mensaje se identifica correctamente con la certeza de que el origen del mensaje no es falso, y la *autenticación de parte* o *identificación*, la cual garantiza por un lado que la identidad de una entidad en particular sea verdadera, y por el otro garantiza que ningún intruso pueda hacerse pasar por otra entidad distinta. En el contexto del CE, ambas modalidades de la autenticación adquieren relevancia por el hecho de garantizar a cada una de las entidades participantes en una transacción, que la entidad con la que están negociando es realmente quien dice ser, o que el origen de algún mensaje como alguna oferta, pedido o autorización de pago proviene realmente de quien dice venir [1](pp 10).

Control de Acceso

Servicio que limita el acceso a los recursos de algún equipo o sistema en particular, obligando a toda entidad que desee obtener acceso dichos recursos a que se identifique o autentique previamente antes de que se le otorguen el acceso solicitado [1](pp 11-12).

1.2.2 Ataques a la seguridad

Por su parte, los *ataques contra la seguridad* se definen como cualquier acción que comprometa la seguridad del equipo de cómputo o de la información, ya sea que dicha acción se haya realizado en forma intencional o no [1] (pp. I-4) y [2] (pp. 3). Cuando el

usuario de un sistema, ocasiona algún daño a la información o al equipo por ignorancia o descuido, se considera que el ataque fue *accidental*. Pero cuando el daño se realiza teniendo como objetivo dañar o realizar algún acceso, modificación, etc. al equipo o a la información, entonces el ataque se considera *intencional*.

Los ejecutores de los ataques intencionales son llamados *atacantes, intrusos, adversarios, oponentes o enemigos*; y aunque con frecuencia, resultan ser personas que utilizan sus conocimientos en cómputo para dañar información, destruirla, robarla, etc.; genéricamente un intruso puede ser cualquier persona, programa o sistema de cómputo. [2] (pp. 4,11-13)

Una clasificación de los ataques con respecto al nivel de acceso que se obtiene sobre la información es la siguiente:

Pasivos

Aquellos en los que el intruso tiene acceso a la información pero sólo para leerla. Por ejemplo cuando se puede acceder al contenido de un mensaje o cuando se puede analizar el tráfico de una red a través de escuchar en el canal de comunicaciones [1](pp I-8) y [2](pp 395).

Activos

En este ataque, el atacante obtiene acceso a la información de tal modo que puede modificarla, agregarle o eliminarle partes. Casualmente, este tipo de ataques toman como base a los pasivos, ya que a través de estos últimos el atacante puede supervisar el tráfico de la red buscando elementos, como contraseñas, passwords o llaves, que posteriormente posibiliten un ataque activo [1](pp I-9) y [2](pp 395)

Otra clasificación de los ataques, esta vez con relación al servicio de seguridad en especifico que se busca contrarrestar es la siguiente [1] (pp.7-9) :

Intercepción

Ataca a la confidencialidad, interceptando un mensaje durante su transmisión y obteniendo acceso a su contenido sin tener autorización para ello [1](pp I-7) y [2](pp 4).

Interrupción

Ataca a la disponibilidad de los datos o recursos de cómputo. Por ejemplo a través de cortar la comunicación entre dos nodos de una red o destruir un disco duro [1](pp I-7) y [2](pp 4).

Fabricación

Ataca a la autenticación permitiendo que una entidad no autorizada inserte partes falsas al mensaje transmitido. Por ejemplo cuando se le agregan registros a un archivo[1](pp 1-7) y [2](pp 4).

Modificación

Ataca a la integridad, pues permite que un mensaje además de ser interceptado sea modificado por una entidad no autorizada antes de que llegue de forma integra a su destino. Como ejemplos tenemos: el cambio de valores en ciertos datos, la modificación del código de ciertos programas etc. [1](pp 1-7) y [2](pp 4).

Esta clasificación puede apreciarse de forma gráfica en la figura 1-1.

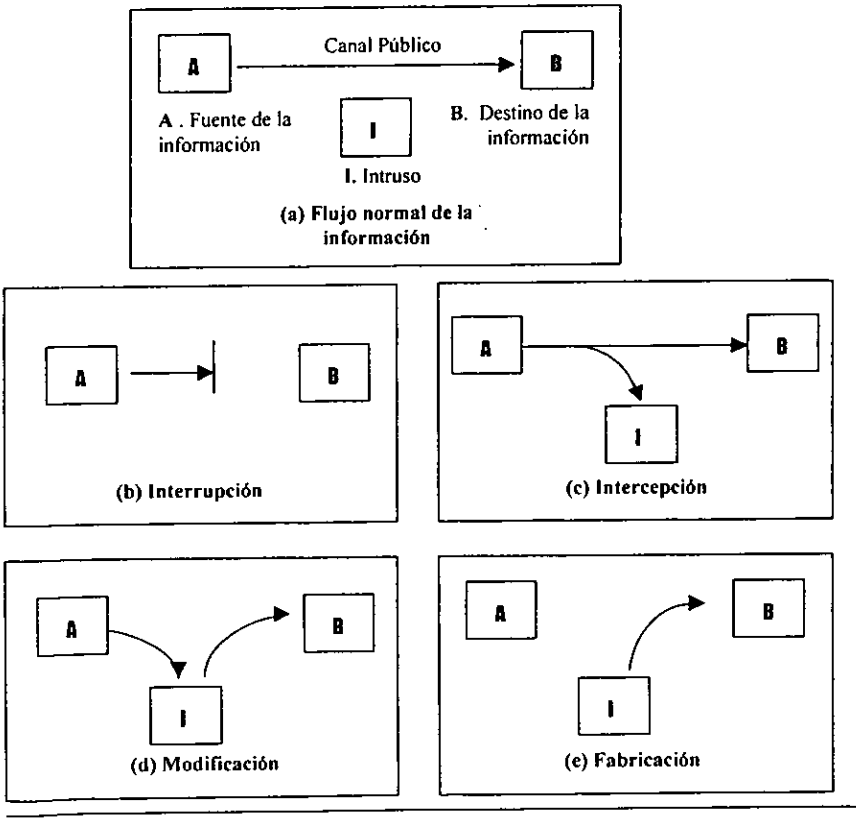

Fig. 1-1 Ataques a la seguridad

Para finalizar con los ataques contra la seguridad, a continuación se describen dos de los ataques más frecuentes a los que se ven expuestos los esquemas de CE:

Ataques por diccionario

Consiste en intentar conjeturar una llave, un password o un texto en claro comparando un espacio finito de opciones (por ejemplo las palabras de un diccionario) contra el valor hash de una llave, de un password o un texto cifrado dado; verificando para cada una de las comparaciones efectuadas si la opción en cuestión coincidió o no con el elemento a conjeturar [13](pp 4).

Ataques tipo réplica o por reflexión

Este tipo de ataque conocido también como ataque "replay" y cuya protección es frecuentemente descuidada, no tiene como fin romper el algoritmo de cifrado utilizado, sino, registrar mensajes válidos y utilizarlos en otras sesiones o contextos. Un ejemplo clásico es el registro de mensajes de un cajero automático, en el que un intruso puede registrar los intercambios, protegidos criptográficamente, que se efectúan durante un retiro de efectivo, y posteriormente, enviarlos nuevamente para efectuar retiros ilegales [13](pp 4).

Como se puede apreciar, la función de los servicios de seguridad en el contexto del CE, como una manera efectiva de evitar ataques a la información confidencial, repudio de mensajes enviados o recibidos, etc., resulta de una gran importancia, por lo que en el siguiente apartado se analizarán a detalle, los conceptos de criptografía y *técnicas criptográficas*; conceptos de gran importancia para la implementación de los servicios de seguridad.

1.3 Modelo de comunicación

Como inicio de este apartado, se presenta en la figura 1-2 el modelo de comunicación, ubicado en una red de computadoras, el cual presenta en términos generales muchos de los elementos que se analizarán más adelante.

En este modelo un mensaje se transmite de una entidad A a otra B a través de algún medio de transmisión como por ejemplo una red de computadoras. Ambas entidades deben cooperar para que la comunicación se realice. Un canal de información se establece al definir una ruta o camino a través de la red que vaya desde la entidad fuente hasta la entidad destino.

Como anteriormente se ha establecido, los aspectos de seguridad toman relevancia cuando se desea o necesita proteger la información transmitida de un intruso I que puede representar una amenaza a la confidencialidad, autenticación, etc. Una de las prácticas más comunes para brindar esta protección ya sea a nivel local o durante la transmisión de la información consiste en la transformación de la misma. Una de las herramientas más

efectivas para dicha transformación es la criptología, la cual será definida a continuación junto con sus conceptos asociados.

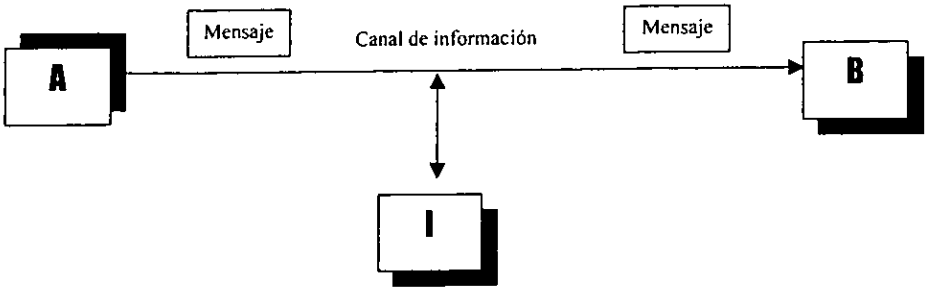

Fig. 1-2 Modelo de comunicación

1.4 Criptologia : Criptografía y Criptoanálisis

La criptología es la ciencia que se encarga del ocultamiento de la información para su protección; esta a su vez se divide en la *criptografía*, constituida por un conjunto de técnicas cuyo objetivo consiste en el ocultamiento de la información; información que como se ha visto, será eventualmente intercambiada entre dos o más partes en forma de mensajes [2](pp 20), y el *criptoanálisis*, que consiste en el proceso de averiguar la información, el secreto o ambos. La estrategia de ataque usada por el *criptoanalista* depende de la naturaleza del esquema criptográfico usado y de la información de que se dispone [13](pp 2).

Con respecto a la criptografía, algunos de los elementos básicos que se presentan en los procesos donde se involucra esta son: el *texto en claro* que se refiere al mensaje original que se encuentra de forma legible, el cual es transformado, por medio de un proceso de *cifrado* o *encripción*, en un texto aparentemente aleatorio y sin sentido, conocido como *texto cifrado*. El proceso inverso que transforma un texto cifrado en texto en claro, se llama *descifrado* [2](pp 20). En este sentido, el cifrado proporciona confidencialidad de la información y adicionalmente permite alcanzar integridad, debido a que los datos que no pueden ser leídos, tampoco pueden ser modificados en una forma significativa. [2] (pp. 13)

De manera formal el *proceso de cifrado* consiste de un algoritmo y de una *llave*. La llave es independiente del texto en claro y determina de un modo particular la forma en que los datos serán transformados al ser cifrados, por lo que un algoritmo producirá salidas distintas, dependiendo de la llave utilizada. Las llaves frecuentemente son cadenas de caracteres que suelen generarse ya sea aleatoriamente o con base en ciertos datos particulares (como el Registro Federal de Causantes, el número de afiliación al Seguro Social, etc.) [1](pp.2).

Un aspecto que resulta importante de mencionar con respecto a la llave es su longitud. Existen algoritmos de cifrado los cuales requieren que la longitud sea fija; hay

otros que aceptan llaves de longitud variable, pero lo realmente importante de dicha longitud es que mientras mayor sea, más seguro será el cifrado ya que el número de posibles llaves se incrementa, complicando de esta forma un ataque por diccionario [5] (pp. 40,41). Finalmente es importante mencionar con respecto de las llaves que aunque una buena cantidad de los algoritmos de cifrado utilizan una o más de ellas, hay otros que no requieren de ninguna para su funcionamiento [2] (pp. 22).

A continuación se analizan tres de las técnicas criptográficas de mayor uso: criptografía de llave simétrica, criptografía de llave asimétrica y funciones hash, cada una con características particulares tanto en su funcionamiento, como en el número de llaves que utilizan; así como también los conceptos relacionados a las técnicas criptográficas tales como firmas digitales y certificados de llave pública, entre otros.

1.4.1 Criptografía de llave secreta

Esta técnica conocida también como *criptografía de llave secreta* o *criptografía convencional*, permite el cifrado de información con el uso de una sola llave. Esta llave única es utilizada tanto para cifrar como para descifrar los datos.

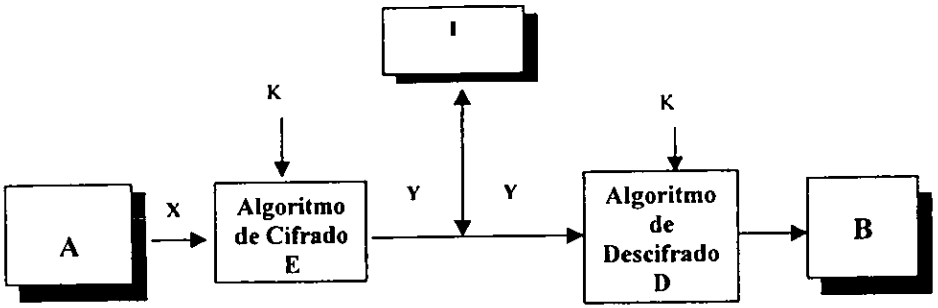

Fig.1-3 Representación gráfica de cifrado de Llave Simétrica

Supóngase que la entidad A, que puede ser una persona, proceso, etc., origina el texto en claro $X=[x_1, x_2,...x_m]$, donde los m elementos de X son letras en algún alfabeto finito, en el que el mensaje a cifrar estará escrito. Tradicionalmente el alfabeto tiene 26 letras (de la A al Z). Para la llave se tiene a $K = [k_1, k_2,...k_m]$. Con X y K como entradas al algoritmo de cifrado E, se obtiene el texto cifrado $Y = [Y_1, Y_2,...Y_m]$, lo que se denota de la siguiente forma:

$$Y = E_k(X)$$

que significa: cifrado del texto en claro X utilizando como llave de cifrado a K y a E como algoritmo de cifrado.

Para el caso contrario, es decir, para descifrar se tiene que:

$$X = D_k(Y)$$

que significa: si el texto cifrado Y, y la llave K (que resulta ser la misma que se usó para cifrar) son entradas del algoritmo de descifrado D, entonces se obtiene el texto original X [1] (pp. 2,3).

Lo anterior puede apreciarse de forma gráfica en la figura 1-3

La seguridad de este esquema reside en la llave y en el hecho de que ésta permanezca secreta, de tal modo que el algoritmo puede ser publicado y analizado sin que por ello el cifrado pierda seguridad [2] (pp. 2).

Por otra parte, la naturaleza de este tipo de cifrado requiere que las partes que desean comunicarse de forma segura, acuerden una llave antes de establecer comunicación. Este acuerdo debe realizarse a través de un canal de comunicación seguro, lo que implica muchas veces que tenga que ser de forma personal, por lo que en el supuesto en que un comprador que radique en México quisiera realizar una transacción electrónica de forma segura con un comerciante que opere en Japón, siendo la forma elegida por ambos para tal acuerdo una entrevista cara a cara para acordar la llave, tendrían obviamente que salvar la gran distancia geográfica que los separa; representando así un problema que en casos como el anterior resulta difícil si no es que imposible de solucionar.

Resulta importante mencionar que como la llave que se utiliza para cifrar es la misma que se usa para descifrar, en el caso en que la llave llegue a ser conocida por alguien aparte de quienes la acordaron (un intruso por ejemplo), ese alguien puede leer todos los mensajes que sean cifrados, y producir mensajes cifrados con dicha llave, perdiéndose así toda la seguridad que brinda este esquema. Por lo tanto, es recomendable que las llaves sean reemplazadas cada cierto tiempo o cuando se tenga la sospecha de que la llave pudo haber sido conocida por alguna entidad diferente a las entidades que la usan para comunicarse.

Otro problema que se desprende del hecho de que éste esquema utilice una única llave, es que cada parte que quiera comunicarse en forma segura con otras, requerirá una llave por cada entidad con la que quiera comunicarse. Esto significa que si un comerciante tuviera 1,500 clientes necesitaría 1,500 llaves para poder comunicarse en forma segura con cada uno. De acuerdo a lo anterior resulta obvia la gran dificultad que representaría la administración del total de las llaves [3] (pp.3 ,4).

Para resolver algunos de estos problemas inherentes al uso de una sola llave, en 1976 surgió como alternativa la *criptografía asimétrica o de llave pública*, propuesta por Whitfield Diffie y Martin Hellman, la cual utiliza un par de llaves [2] (pp.33). Este esquema se analiza a continuación.

1.4.2 Criptografía de llave pública

Conocida también como *criptografía de llave pública,* requiere ya no sólo una llave, sino un par de ellas: una *pública* y otra *privada.* Este esquema se apoya en funciones matemáticas para relacionar cada una de las llaves, efectuando el cifrado con la llave pública y el descifrado con la privada si se desea obtener confidencialidad, y el orden inverso si se desea autenticación y no repudio. [1] (pp. 107).

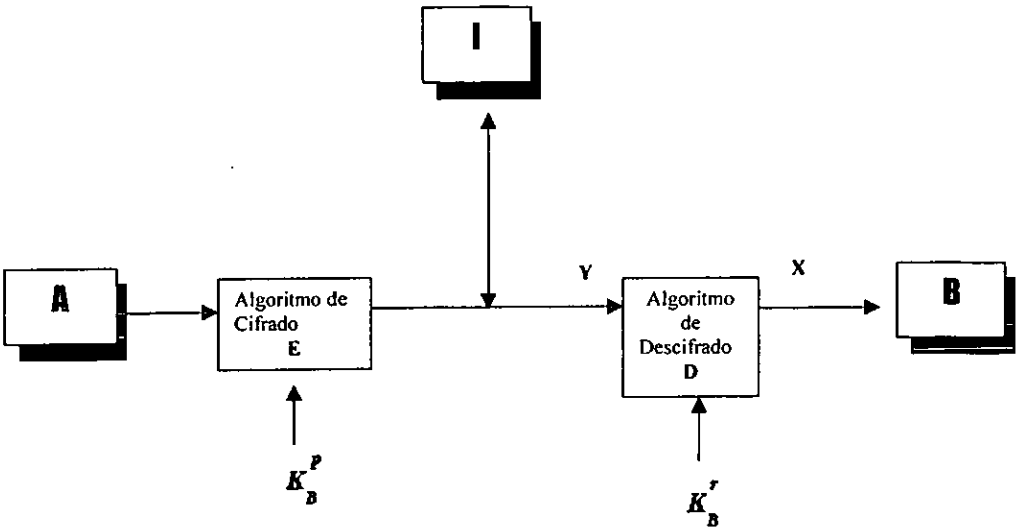

Fig 1-4 Representación gráfica de cifrado de Llave Asimétrica

En este esquema de cifrado, cada entidad que interviene en la comunicación debe poseer un par de llaves. Una de estas llaves es la privada, con ella se cifran los mensajes y debe ser conocida únicamente por su dueño, sin ser revelada jamás. La otra llave, la pública, es publicada y distribuida ampliamente, con el fin de que la llave pueda obtenerse de diversas fuentes, permitiendo que la llave pública de una entidad en particular, obtenida de cierta fuente, pueda ser comparada contra la llave pública, de la misma entidad, obtenida de otro sitio, corroborando así su autenticidad y previniendo falsificaciones.

Para ejemplificar cómo funciona este esquema se puede plantear el siguiente escenario: supóngase que un comprador desea enviar, a través de una red de telecomunicaciones pública, el pedido de una compra a un comerciante con el que nunca ha efectuado una compra y desea además que el contenido del pedido sea conocido sólo por el comerciante. Para tales fines el cliente debe obtener, de alguna forma la llave pública del comerciante (la obtención de la llave pública del comerciante resulta ser en la práctica una tarea sencilla). Una vez que el comprador posee la llave pública, debe cifrar el pedido con ella y enviarlo al comerciante.

Posteriormente cuando el comerciante reciba el pedido cifrado, lo descifrará con su llave privada, obteniendo de este modo el pedido como texto en claro. En el caso opuesto, en que el pedido no fuera cifrado con la llave pública del comerciante, le resultaría tan imposible conocer el contenido del pedido como a cualquier intruso que intentara descifrarlo con una llave distinta a la que fue usada para cifrarlo.

Asúmase el mismo escenario establecido en el apartado para el cifrado de llave simétrica, en el que una entidad **A** que genera un mensaje en texto en claro X destinado a **B**. Sin embargo en este esquema, **B** debe generar un par de llaves: la pública denotada por

$$K_B^r$$

que debe ser puesta en un lugar público accesible a la entidad **A**, y la privada denotada como

la cual debe permanecer secreta para todos exceptuando a **B**.

$$K_B^p$$

Se tiene entonces que con el mensaje X y la llave pública de **B**, como entradas al algoritmo de cifrado E, la entidad **A** obtiene el texto cifrado $Y = [Y_1, Y_2, \ldots Y_m]$, por lo tanto:

$$Y = E_{K_B^p}(X)$$

Como **B** tiene la llave privada correspondiente, cuando reciba el texto cifrado podrá descifrarlo de la siguiente forma:

$$X = D_{K_B^r}(Y)$$

Lo anterior puede apreciarse de forma gráfica en la figura 1-4

La criptografía de llave pública, por otra parte, intenta resolver algunos de los problemas que presenta la criptografía de llave secreta, como los de distribución y administración de llaves; y aunque no lo logra de forma total, aporta algunas soluciones. Por ejemplo, en el supuesto en que un comerciante quisiera mantener transacciones electrónicas seguras con 1,500 clientes, requiere solamente un par de llaves (una privada y otra pública) para poder lograrlo, pues bastaría con que cada uno de los 1500 clientes cifrará su pedido con la llave pública del comerciante para que solamente él pudiera tener acceso a dicha información de una forma legible usando su llave privada para descifrarla. Además, evita el problema de tener que acordar previamente una llave como sucede en el

esquema de criptografía de llave secreta, debido a que el comerciante únicamente debe hacer pública su llave para que cada cliente la obtenga, independientemente de la distancia geográfica que los separe [2] (pp.33).

A pesar de lo anterior no se puede considerar a la criptografía de llave pública como un reemplazo a la de llave secreta, debido entre otras cosas a que la generación de llaves en la primera es más costosa, hablando en términos de recursos de cómputo, que en la segunda, puesto que es alrededor de 1000 veces más lenta que la criptografía de llave secreta [2](pp. 162). Para aprovechar las mejores características de ambos esquemas por lo general se utilizan en forma combinada. Por ejemplo, la criptografía de llave pública se utiliza al inicio de una transacción electrónica para que un cliente envíe cifrada, con la llave pública del comerciante, una llave secreta que haya generado previamente. Una vez que el comerciante recibe la llave cifrada la puede recuperar, descifrándola con su llave privada. De esta forma se evita el problema de tener que acordar previamente una llave. A partir de este momento toda la información que se intercambien el cliente y el comerciante durante la transacción será cifrada y descifrada con la llave secreta que ahora comparten dentro de un esquema de cifrado de llave secreta .

Por ultimo, es importante mencionar que debe establecerse claramente la diferencia entre los términos: *llave secreta* y *llave privada.* La primera siempre se referirá a la llave única que se utiliza tanto para cifrar como para descifrar dentro del esquema de criptografía de llave secreta, y la segunda se refiere a la llave con que se realiza el cifrado en el esquema de criptografía de llave pública [5] (pp. 48,49).

1.4.3 Funciones hash

Existe una tercera y última técnica criptográfica conocida como *compendio de mensaje, funciones hash* o *transformaciones unidireccionales.* Estas funciones reciben como entrada una cadena de longitud arbitraria y regresan como salida otra de longitud fija, frecuentemente de menor longitud que la original; a esta salida se le nombra *valor hash* [7] (pp 28).

La naturaleza de estas funciones, hace que sea prácticamente imposible que dos mensajes distintos generen un valor hash idéntico al aplicárseles una misma función hash. Es por esta característica que a estas funciones se les utiliza para comprobar que un mensaje que viajó de una entidad a otra o que radica en forma local, no haya sido modificado por partes no autorizadas durante su transmisión o su almacenamiento, proporcionando por lo tanto integridad para dicha información. Su operación no requiere de llaves y dado que el valor hash calculado de un mensaje no tiene una forma legible y no muestra elementos de relación con el mensaje original, las funciones hash ofrecen la seguridad de que un intruso no puede obtener el mensaje original a través de analizar el valor hash de dicho mensaje [5] (pp. 53).

Supóngase entonces, que un valor hash h, es generado por una función H de la forma:

$$\mathbf{h = H(}m\mathbf{)}$$

Donde *m* es un mensaje de longitud arbitraria, y *h* es el valor hash de longitud fija, resultado de aplicar la función H al mensaje *m*: **H(*m*)**. Una vez generado, el valor hash es anexado al mensaje que lo originó. Cuando el receptor recibe el valor hash junto con el mensaje, podrá verificar la integridad de éste último calculando su valor hash y comparándolo contra el valor hash que le fue enviado; si coinciden, la entidad receptora puede estar segura de que el mensaje no fue modificado durante su transmisión [1] (pp.174).

Otro escenario posible es el siguiente: supóngase que un comerciante desea enviar un mensaje para verificar que el cliente **A** (con el que se encuentra realizando una transacción) posea los suficientes fondos como para pagarle. Este comerciante debe calcular el valor hash de la orden de compra, y enviarlo junto con la orden, al banco donde **A** le haya indicado previamente. Cuando el banco de **A** reciba los datos enviados por el comerciante, calculará por su cuenta el valor hash de la orden de compra, comparará el valor hash calculado contra el recibido. Si coinciden y si el cliente posee los fondos suficientes como para pagar, el banco le hará saber al comerciante que puede llevar a cabo la venta; de lo contrario, si el valor hash calculado por el banco no coincide con en recibido, el banco sabrá que la orden de .compra fue modificada durante su transmisión, el alguno de sus datos (por ejemplo el monto), indicándole al comerciante que la transacción no puede efectuarse.

Nota: En el esquema anterior se asume que tanto el banco como el comerciante conocen y utilizan la misma función hash.

Hasta este punto, se han revisado tres técnicas criptográficas que otorgan confidencialidad y/o integridad como su principal función. Una variación en el esquema de la criptografía de llave pública proporciona además autenticación y no-repudio. Está técnica es conocida como firmas digitales y se analiza a continuación.

1.5 Firmas digitales

Las firmas digitales son un mecanismo que permite crear el mismo esquema de las firmas tradicionales, en el que se logra relacionar la identidad de alguien a un documento tangible, por ejemplo un cheque, pero en una forma electrónica, prescindiendo de la existencia del elemento tangible.

Se define como *firma digital* al resultado de cifrar un mensaje utilizando un esquema de cifrado asimétrico, de manera que la persona que posea el mensaje inicial y la llave pública del firmante, pueda determinar de forma fiable si dicho cifrado se hizo utilizando la llave privada correspondiente. Además las firmas digitales permiten conocer si el mensaje ha sido alterado a partir del momento en que fue firmado [2](pp. 35,36), [6](pp.209) y [1](pp.214).

Una firma digital se logra a través de invertir el esquema de cifrado de llave pública; es decir, el cifrado de los datos se realiza con la llave privada, llamado *proceso de firma*, y el descifrado con la llave pública, conocido como *verificación de la firma*.

Para ejemplificar lo anterior, supóngase que la entidad A prepara un mensaje X que será enviado a la entidad **B**, cifrándolo con su propia llave privada:

$$Y = E_{K_A^r}(X)$$

Posteriormente envía el texto cifrado a **B**. La entidad **B** por su parte, puede descifrarlo gracias a que la llave pública de **A** es accesible para él, puesto que está en algún lugar público, calculando entonces:

$$X = D_{K_A^p}(Y)$$

Dado que el mensaje fue cifrado usando la llave privada de **A**, **B** puede estar seguro de que sólo **A** pudo generar la firma, pues sólo **A** tiene acceso a su propia llave privada. De esta manera se consigue la autenticación. Cabe mencionar que este esquema no proporciona confidencialidad, ya que cualquiera que puede acceder a la llave pública de **A** está en condiciones de descifrar el mensaje enviado a **B**.

Lo anterior puede apreciarse de forma gráfica en la figura. 1-5

Resulta importante aclarar que cuando la firma digital de un mensaje es enviada, también debe enviarse el mensaje junto con ella, ya que la firma digital de un mensaje no es el mensaje mismo, sino una pieza de información asociada a él. Es por lo anterior que la firma digital de cierta entidad, por ejemplo **A**, para un mensaje *m*, sólo puede ser generada por alguien que tenga acceso a la llave privada de **A** (que en el caso más recomendable resulta ser sola y únicamente **A**) y al mensaje firmado, obteniéndose de esta manera, no-repudio y autenticación [1] (pp. 114).

Con respecto al no-repudio, gracias a que las firmas digitales permiten relacionar un documento con la entidad que lo firma, se obtiene la seguridad de que sólo esa entidad es el firmante, garantizando de este modo que dicha entidad, no pueda negar haber firmado el documento.

Por parte de la integridad del mensaje, dado que la firma digital depende del contenido de *m*, si éste es alterado, entonces la firma digital ya no corresponderá al mensaje firmado. Esto asegura que sí la entidad receptora descifra el documento firmado con la llave pública de **A**, y obtiene el mismo mensaje que recibió junto con la firma podrá estar plenamente convencido de que el mensaje no fue alterado durante su transmisión, garantizado así la detección oportuna de cualquier alteración a la integridad del mensaje firmado [5] (pp.52) y [2] (pp.140-142).

Como se sabe hasta ahora, la llave pública, por ejemplo de **A**, se utiliza para confirmar que una firma digital haya sido generada por dicha entidad, pero ¿qué pasaría con la autenticidad de una firma en el caso en que la identidad de **A** fuera falsa, es decir, que **A** no fuera la persona que dice ser al por ejemplo, no trabajar en donde dice trabajar, o no vivir donde dice vivir?. Lo que sucedería es que la firma no tendría validez puesto que aunque el receptor de la firma podría estar seguro de que **A** generó la firma, no puede estar

seguro, de que por ejemplo A tenga la autoridad como para firmar el mensaje que le envió. Por esto resulta imprescindible contar con un medio por el cual cualquier persona que reciba un documento firmado, pueda tener la certeza de que la firma es auténtica, es decir que la llave privada que generó la firma pertenezca realmente por ejemplo a A y no a alguien más que intente hacerse pasar por esta entidad.

Una forma de lograrlo es que la llave pública de A sea entregada a la otra parte a través de un canal seguro, pero esto como se ha visto no es práctico. Otro medio que resulta funcionar de mejor manera es el conocido como *certificado de llave pública*, el cual se detalla a continuación [2] (pp.135).

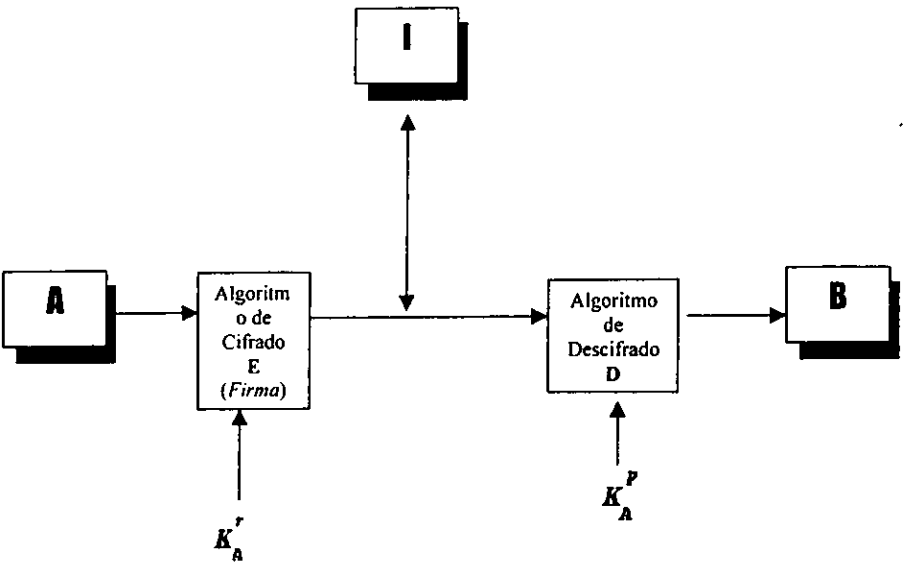

Fig 1-5 Representación gráfica de Firma Digital

1.5.1 Certificados de llave pública

Se define como *certificado de llave pública* aquel documento digital que identifica a la autoridad certificadora que lo ha emitido y a la entidad dueña de la llave pública certificada. Este documento contiene tanto la llave pública del dueño de la llave como la firma digital de la autoridad que emitió el certificado [7] (pp. 38).

Dicho de otra forma, un certificado es la llave pública de alguien, por ejemplo de A, la cual es cifrada con la llave privada de una entidad confiable.

La emisión de certificados y la generación de llaves privadas para firmas digitales, frecuentemente es desempeñada por múltiples entidades que están jerarquizadas de una manera tal, que las de nivel inferior obtienen su capacidad de certificación de otras entidades de nivel superior. Finalmente en la cúspide de la jerarquía suele hallarse una *autoridad certificadora central*, que puede pertenecer al Estado o a la Iniciativa Privada.

Una *autoridad certificadora central* (ACC) es aquella entidad que da testimonio de la pertenencia de una determinada llave pública a un usuario o a otro certificador de nivel jerárquico inferior, cuya identidad ha sido verificada. A las entidades certificadoras de jerarquía intermedia e inferior se les llama simplemente *autoridades certificadoras* (AC).

Las autoridades certificadoras tienen la función de emitir, suspender, cancelar y revocar certificados, así como de dar a conocer la situación actual de un certificado en particular [7](pp. 38).

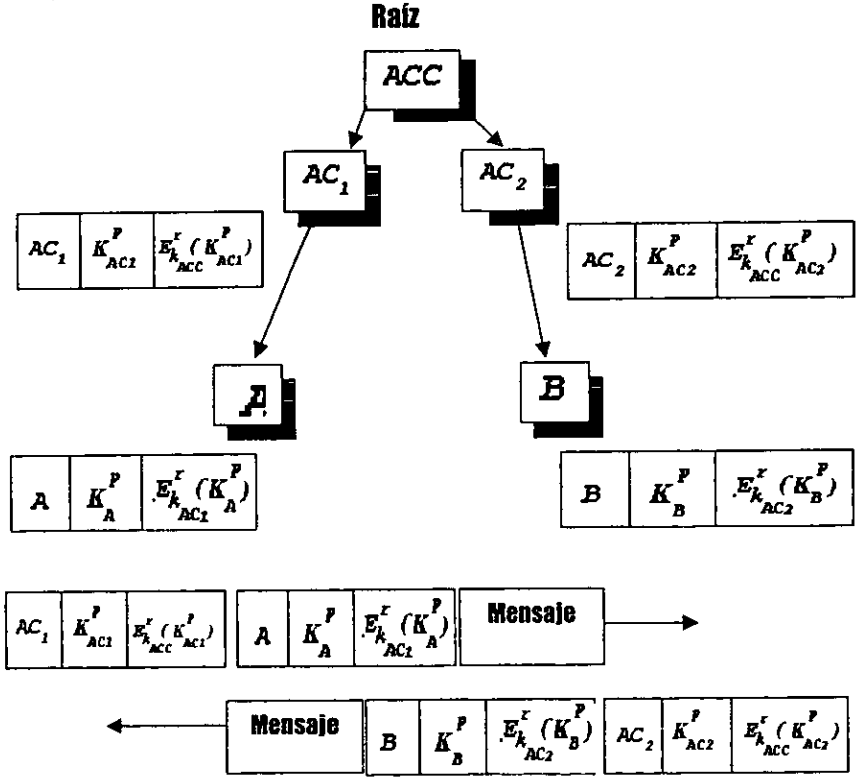

Fig. 1-6 Flujos de una jerarquía de certificación

Para ejemplificar la función de una AC hágase una analogía con la firma de un contrato de tipo mercantil ante un notario. El notario en este caso es una persona que tiene una mayor jerarquía de confianza que los firmantes y que funge como una AC, pues conoce el contrato y las leyes que lo rigen, además debe haber comprobado, previo a la firma del contrato, la autenticidad de la entidad de los firmantes y de lo que asientan en el contrato. Por último el notario está autorizado por una institución legal a fungir como tal. En este caso la función del notario es certificar que el contrato y las firmas de los participantes son válidos. De una manera similar en la que el notario certifica las firmas y el contrato, un certificado de llave pública es generado o emitido por una AC, la cual establece que la llave y la identidad del dueño de la llave son auténticas.

Como se acaba de describir, un certificado de llave pública se basa en una *jerarquía de confianza*. Una jerarquía de confianza es aquella en la que se requiere de una tercera parte, en este caso una AC, para que haga constar que el dueño de la llave pública es realmente quien dice ser. La AC verifica la identidad del dueño de la llave, antes de emitir el certificado, a través de documentos oficiales tales como cartillas militares, licencias de manejo, credenciales de elector, etc., que le son solicitados al dueño de la llave pública en el momento que la presenta para que sea certificada. [7](pp. 39).

Es por lo anterior que en forma general un certificado de llave pública contiene:

1. La identidad del dueño de la llave pública
2. La llave pública misma
3. El valor hash de la llave (opcional)
4. La llave pública de la autoridad certificadora

La figura 1-6 muestra una jerarquía de certificación simple, donde la entidad **A** ha sido certificada por la autoridad certificadora **AC1** y la entidad **B** por la **AC2**. Tanto **AC1** como **AC2** dependen de la autoridad certificadora central **ACC**, la cual les ha emitido a cada una su certificado respectivo. Además, cada entidad que participa en esta jerarquía posee la llave pública de **ACC**. Cuando **A** envía un mensaje a **B** envía además su propio certificado, el cual está firmado por **AC1**, y el certificado de **AC1** firmado por **ACC**. Cuando **B** recibe este mensaje utiliza la llave pública de **ACC** para verificar la llave pública de **AC1**, que a su vez es utilizada para validar llave pública de **A**, y esta última para autenticar el mensaje, recorriendo de esta manera la cadena de confianza de los certificados.

En algunos casos en los que la jerarquía de certificación es de una extensión considerable, incluir los certificados con cada mensaje puede resultar ineficiente. Esto puede solucionarse si cada usuario posee una copia de los certificados que ha recibido, de tal manera que la entidad emisora en lugar de incluir los certificados en el mensaje, debe incluir el valor hash de los certificados, valor que es conocido como sello. La entidad receptora debe comparar este sello con el valor hash de cada certificado, del que posee una copia, y en los casos en que no haya coincidencia, deberá solicitar una copia al emisor del mensaje.

Existen ciertos casos en los que la cancelación de los certificados se debe realizar cuando:

a) El dueño de la llave pública deja de representar a la entidad que indica el certificado

b) El dueño de la llave pública tiene sospecha que la seguridad de la llave privada puede estar comprometida
c) La llave privada asociada a la llave pública del certificado ha sido extraviada o destruida

Como se puede notar, la seguridad de los certificados de llave pública se basa en lo confiable que resulte ser el desempeño de las AC, por lo que la función de dicha entidad no resulta trivial en ningún momento y debe contar con medidas de seguridad extremadamente eficientes, para que la información sensible que maneja no se vea amenazada.

Con respecto a la necesidad de una tercera parte confiable, esta representa frecuentemente un costo para los usuarios del web que en ocasiones puede ser alto, además de que dicha autoridad puede llegar a representar un cuello de botella para el flujo de las transacciones sobre todo en situaciones en el que el flujo de la red es muy alto [2] (pp 16-17,135-140).

Para finalizar con los aspectos criptográficos asociados a las firmas digitales, a continuación se describe otra técnica llamada *firma blindada.*

1.5.2 Firmas Blindadas

Generar una *firma blindada* o *blindar un mensaje* puede equipararse a poner un mensaje en un sobre junto con una pieza de papel carbón situación en la que nadie puede leer el mensaje a través del sobre. Una firma digital es efectuada a través de firmar desde el exterior del sobre. La firma se hará a través del papel carbón hacia el mensaje. Cuando el mensaje es extraído del sobre, estará firmado y de esta manera la entidad que lo haya firmado, no habrá sido capaz de conocer el contenido de lo que firmó [7] (pp 48-49). Este método ha sido usado para la implementación de protocolos de votación y dinero digital.

A continuación se muestran los pasos básicos para que una entidad **V**, usando las firmas blindadas, logre que otra entidad **C** firme un mensaje sin que conozca su contenido.

1. **V** toma el mensaje y los multiplica por un valor aleatorio, llamado *factor de blindaje*, blindando así el mensaje de tal manera que el contenido no pueda ser conocido.
2. **V** manda el mensaje blindado a **C**
3. **C** firma digitalmente el documento y lo envía de regreso a **V**
4. **V** divide el mensaje blindado y firmado entre el factor de blindaje, obteniendo así el mensaje original con la firma de **C**

Para que este esquema funcione, la función de firma y la de multiplicación deben ser conmutativas, lo que significa que cualquiera de ellas pueda efectuarse antes o después de la otra sin restricción alguna. Las propiedades de las firmas blindadas son las siguientes:

1. La firma en el documento después de habérsele retirado el blindaje es una firma digital válida, la cual tiene las mismas propiedades de cualquier firma digital.

2. No existe manera de probar que la firma digital fue creada usando un protocolo de firma blindada

Matemáticamente el protocolo de firma blindada en un escenario en el que una entidad V desea que otra entidad C genere una firma blindada sobre un mensaje *M*, donde se asume que la entidad C posee una llave pública K_c^p y una llave privada K_c^r funciona de la siguiente manera:

1. V: elige el factor de blindaje, *k*, como un número aleatorio entre 1 y *n* (el cual es el módulo utilizado para la generación previa del par de llaves de C), y blinda a *M* como sigue:

$$T = (Mk)^{k_c^p} \bmod n$$

2. V envía *T* a *C:*

$$C \longrightarrow V: \qquad T$$

3. C firma *T* :

$$E_{k_c^r}(T) = (Mk^{k_c^p})^{k_c^r} \bmod n = M^{k_c^r} k \bmod n$$

4. V : quita el blindaje de $(Mk^{k_c^p})^{k_c^r}$ calculando:

$$S = \frac{(Mk^{k_c^p})^{k_c^r} \bmod n}{k} = \frac{M^{k_c^r} k \bmod n}{k}$$

5. El resultado es:

$$S = M^{k_c^r} k \bmod n$$

Es decir, el resultado final es el mensaje firmado con la llave privada de C. En resumen, este esquema requiere que C firme el mensaje sin conocer su contenido, lo que se logra frecuentemente demostrándole por medios probabilísticos que lo que firma es realmente lo que V le dice. Las firmas blindadas se aplican generalmente usando una llave de propósito particular que es utilizada para firmar un tipo específico de documento [7] (pp 49-50).

1.5.3 Firmas Duales

Como en su oportunidad se explicó, las firmas digitales se utilizan para relacionar la identidad de alguna entidad con el contenido de algún mensaje en particular. Con el fin de verificar el mensaje, el receptor requiere adicionalmente ser capaz de conocer el contenido del mensaje. En protocolos que involucran al menos tres entidades, como por ejemplo en una transacción de CE que use tarjeta de crédito, se utiliza en ocasiones una técnica conocida como firmas duales.

Las *firmas duales* permiten asociar la identidad de alguna entidad con un mensaje en específico sin que esto implique necesariamente que el receptor pueda conocer el contenido del mensaje. Como su nombre lo indica las firmas duales son utilizadas cuando dos mensajes relacionados deben ser enviados a dos entidades diferentes. Siempre que un pago es efectuado es posible realizar una separación entre los detalles financieros necesarios para efectos del pago mismo y de los detalles de lo que se compra o en una palabra del pedido. Lo anterior puede ser separado en dos mensajes diferentes.

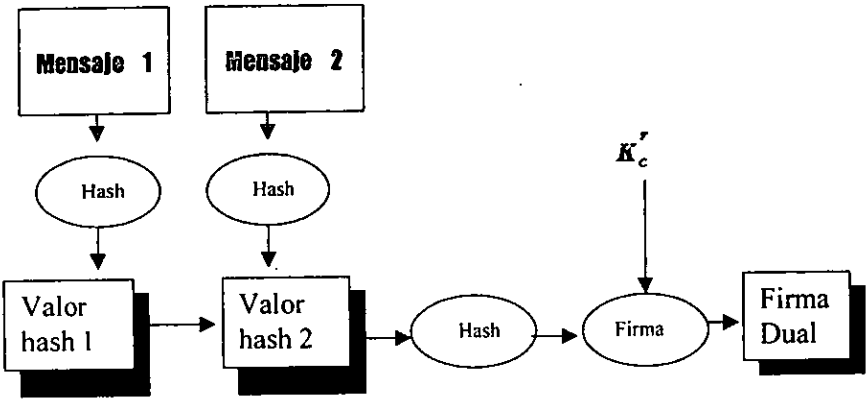

Figura 1-7 Representación gráfica de la generación de una firma

La figura 1-7 muestra de forma gráfica la manera en que se construye una firma dual. En un inicio se calcula un valor hash de cada uno de los dos mensajes relacionados de manera independiente. Después los dos valores hash son concatenados y se calcula el valor hash del resultado de la concatenación. Este tercer valor hash es firmado con la llave privada del emisor.

Tomando como base la figura 1-7 se plantea un escenario en el que un comprador C desea enviar a un comerciante V un mensaje1 y a una entidad financiera B un mensaje2, de tal manera que se le asegure tanto a V como a B que un segundo mensaje relacionado existe. C debe enviar a V el mensaje1, el valor hash 2 y la firma dual, mientras que a B debe enviarle el mensaje 2, el valor hash 1 y la firma dual. Cuando V recibe lo enviado por C, debe calcular el valor hash del mensaje 1 concatenar dicho valor hash con el valor hash

2, calcular el valor hash de esta concatenación y verificar que el resultado final coincida con la firma dual. De esta forma aunque V pude conocer únicamente el contenido del mensaje 1, puede confiar existe un segundo mensaje que fue utilizado para calcular el valor hash 2 y que la firma dual relaciona ambos mensajes. B por su parte se encuentra en una posición similar ya que únicamente puede conocer el contenido del mensaje 2, pero puede verificar que la firma dual lo relaciona con el mensaje 1. Un beneficio adicional de las firmas duales consiste en el hecho de que el emisor requiere calcular únicamente una firma dual por cada par de mensajes, lo que ahorra ciertos recursos de cómputo.

El uso de esta técnica en esquemas de CE, será mostrado en capítulos posteriores.

Finalmente un último concepto importante de definir asociado a la criptografía son ciertos números generados aleatoriamente que se utilizan como elementos criptográficos que se usan una única vez, conocidos en la literatura como *nonces* y que en este trabajo llamaremos *núnicos*, los cuales se describen a continuación.

1.6 Elementos criptográficos aleatorios (núnicos)

Un núnico es una cierta cantidad o número en cada mensaje que será usado únicamente para ese mensaje en particular. Un núnico puede ser utilizado como [1] (pp. 96):

1. *Un entero*, que proporciona esquemas de autenticación recíproca, en la que tanto el emisor como el receptor se autentican, donde los núnicos se usan para evitar ataques tipo reflexión.
2. *Timestamp* o *instantánea*, que consisten en un núnico asociado de manera única a un mensaje en particular de tal modo que la posibilidad de que otro mensaje tenga asociado el mismo núnico sea extremadamente pequeña, Existen timestamps que incluyen una hora y fecha, y son usados para limitar el período de validez del mensaje al que esta asociado la timestamp, por ejemplo el caso en el que ciertas entidades participantes en un protocolo, acuerden que el mensaje sea válido únicamente por un período establecido a partir del timestamp correspondiente. [7] (pp. 48) y (2) (pp 168).
3. *Llaves de sesión*, que se usarán en esquemas de criptografía simétrica.
4. *Llaves* utilizadas en esquemas de criptografía de llave pública.

La mayoría de los esquemas de CE que se describen en el capítulo 4, hacen un uso considerable de núnicos, en varias de sus modalidades, para evitar principalmente los ataques por reflexión.

Hasta este momento se han revisado los conceptos más importantes con relación a la seguridad de la información. También se han analizado tres de las técnicas de cifrado más importantes en la actualidad: el cifrado asimétrico, el cifrado de llave pública y las funciones hash. Además, se ha descrito la forma en que estos esquemas implementan los servicios de seguridad, tan importantes para poder realizar transacciones electrónicas de

tipo comercial en forma segura, apoyándose también en las firmas digitales y los certificados de llave pública, por lo que en este punto se cuenta ya con los suficientes conocimientos como para poder comprender el funcionamiento de los diferentes esquemas que permiten realizar transacciones de CE. Sin embargo, antes de adentrarse en ellos a lo largo de este trabajo, el contenido de los capítulos que lo integran será descrito a continuación en forma resumida.

1.7 Estructura de este trabajo

La modalidad electrónica del comercio ha tenido cada vez una mayor difusión gracias a que cada día es mayor el número de personas que utilizan Internet. Una parte importante de estos usuarios, que se incrementa rápidamente, está aceptando y haciendo uso de algún esquema de CE. El capítulo **2** define inicialmente los conceptos principales asociados al CE además de las entidades que están involucradas, abarcando la forma en que participa cada una. Posteriormente se mencionan las ventajas y desventajas que presenta esta nueva modalidad sobre el comercio tradicional, para finalizar con la especificación de los requerimientos de un esquema general de CE en los niveles básicos.

De la misma forma que el comercio tradicional tiene múltiples formas de efectuarse (trueque, crédito, abonos, etc.), el CE presenta una serie de modalidades que difieren en ciertos aspectos entre sí. Los esquemas que implementan estas modalidades son muy variados y frecuentemente podemos encontrar la existencia de más de un esquema para cada tipo de transacción. Es por lo anterior que existe una gran gama de protocolos que satisfacen a cada tipo especifico, requiriendo por lo tanto diversos recursos para su funcionamiento además de presentar diversas ventajas y desventajas en cada caso en particular. Con respecto a los métodos de pago dentro de esta gran variedad de esquemas, se puede decir que la mayoría se basan en métodos a los cuales la mayor parte de la gente está acostumbrada. El uso del dinero como medio de pago se ha dado desde tiempos muy antiguos, por lo que utilizarlo como medio para comprar, vender o adquirir bienes y/o servicios le resulta a la gente totalmente familiar. Hay esquemas dedicados a implementar el uso de dinero electrónico para realizar transacciones en forma electrónica y que conservan aquellas ventajas que siempre ha proporcionado el dinero tradicional como: sencillez de uso, alta disponibilidad, anonimato para quien lo usa, etc.; además de ofrecer la familiaridad con que la gente hace uso de él.

Por otra parte, la aparición de las tarjetas de crédito ha tenido una relevancia notable dentro del mundo financiero y comercial debido a su facilidad de uso, el alcance mundial que ofrecen, lo prácticas que resultan al poder contar con cantidades de crédito sin tener que cargar con dinero alguno; además de la incorporación de sistemas de cómputo para realizar lo que se ha denominado *la banca electrónica* en la que surgieron los ahora familiares cajeros automáticos, en los que el retiro o depósito de efectivo se efectúa a través de únicamente la tarjeta de crédito y de un numero personal, en sólo segundos y cuya disponibilidad abarca las 24 horas del día. Son muchas las características por las que las tarjetas de crédito resultan ser un elemento ideal para utilizarse como medio de pago en algunos esquemas de transacciones electrónicas. El capítulo **3** se dedica a describir en forma general los esquemas que existen, tanto convencionales como electrónicos, tomando

como base los medios de pago que utiliza cada esquema, mencionando las características principales de cada uno

El capítulo **4** describe algunos de los esquemas de CE basados tanto en dinero electrónico como en tarjetas de crédito que en la actualidad son de uso muy frecuente en Internet enfatizando la descripción de cómo estos esquemas alcanzan la confidencialidad, integridad, y autenticación a través de técnicas criptográficas. Estos sistemas son:

a) **SSL** ("Secure Socket Layer"). La seguridad de las aplicaciones para web gira en torno a dos protocolos, SHTTP ("Secure HyperText Transfer Protocol") y SSL, Este último permite la autenticación para servidores web y navegadores. Además, proporciona confidencialidad e integridad para los datos que son transmitidos durante transacciones efectuadas entre los servidores web y navegadores. Es importante mencionar que a pesar de que no fue desarrollado pensando en su uso conjunto con tarjetas de crédito, su estructura permite que las incorpore como medio de pago. Hoy día la versión 3.0 de SSL está incluido en la mayoría de los navegadores.

b) **iKP** ("i-Key Protocol"). Es una familia de protocolos diseñados específicamente para permitir TETC usando tarjetas de crédito como forma de pago. Su funcionamiento se basa en el uso de criptografía de llave pública y cada uno de los protocolos que integran la familia se diferencian entre ellos por el número de participantes del protocolo que poseen su propio par de llaves.

c) **SEPP** ("Secure Electronic Payment Protocol"). Basado en 3KP, el cual es el integrante de la familia *i*KP en el que todas las entidades participantes poseen un par de llaves, por lo que conserva muchas de las características de este, sin embargo como un elemento extra para la definición del protocolo, SEPP define un sistema de administración de certificados CMS, que consiste de una o más autoridades certificadoras que proporcionan servicios de emisión y distribución de certificados de llave pública a compradores, vendedores e instituciones financieras.

d) **SET** ("Secure Electronic Transaction"). Desarrollado conjuntamente por IBM, VISA, MASTERCARD y otros, utiliza a DES ("Data Encription Standard") y RSA ("Rivest Shamir Adelman") como algoritmos principales de cifrado y a SHA ("Secure Hash Algorithm") como función hash. Por sus características técnicas y de origen, se espera que SET se convierta en el método estándar para efectuar pagos electrónicos en Internet

La existencia de un gran número de esquemas para efectuar CE, implica que cada esquema logre proporcionar autenticación, intregridad, confidencialidad y otros servicios de seguridad por diversos medios; resultando interesante para aquellas personas o corporaciones que están interesadas en realizar compras o ventas por medio de Internet, saber cual o cuales esquemas resultan más convenientes para sus características y mercados específicos. En este sentido, el capítulo **5** desarrolla un estudio comparativo entre los esquemas de Comercio Electrónico basados en tarjetas de crédito, descritos en el capítulo 4, tomando en consideración los siguientes elementos de comparación:

1. Entidades participantes
2. Entidades que se autentican durante el protocolo

3. Algoritmos de cifrado que utiliza o soporta cada esquema
4. El tamaño de las llaves que utiliza cada uno de los algoritmos utilizados
5. El número total de llaves requeridas tanto para cifrado de llave secreta como para cifrado de llave pública
6. Número de procesos de cifrado de llave pública
7. El número de firmas digitales
8. El número de núnicos generados
9. El número total de mensajes intercambiados durante el protocolo
10. Los requerimientos de seguridad que satisface cada esquema
11. Las principales ventajas
12. Las principales desventajas

Para finalizar, en el capítulo 6, se describen los resultados y conclusiones obtenidas de la realización de este trabajo.

Capítulo 2

COMERCIO ELECTRÓNICO (CE)

2.1 Antecedentes

En la actualidad, la mayoría de los países del mundo, incluido México, funcionan económicamente bajo un régimen capitalista. En estos países, una serie de factores tales como la formación de grandes ciudades que albergan enormes cantidades de habitantes y el comportamiento consumista de estos, provocan un incremento en la demanda de bienes y servicios, necesarios para la satisfacción tanto de las necesidades individuales como colectivas de instituciones y gobiernos.

Esta situación se ha complicado, a la vez que enriquecido, con la aparición de los mercados globales, posibilitados por la interconexión de entidades de todo el mundo por medio de redes de telecomunicaciones que abren un sin fin de posibilidades acompañadas de múltiples problemas que requieren solución. Este panorama hace evidente la trascendencia que en aspectos políticos, sociales y económicos representa la producción y comercialización de bienes. y servicios suficientes y adecuados para responder a las grandes demandas actuales. Por esto, las empresas comerciales y de servicios, se ven en la continua necesidad de buscar medios que les permitan reducir sus costos de operación, aumentar sus ganancias y ser más competitivos.

Frecuentemente este aumento en la productividad se ha logrado a través de mejorar los esquemas existentes de producción, venta, comercialización, etc. o desarrollando nuevos que aporten mejoras o innovaciones útiles para tal fin. A este respecto, una de las prácticas que ha resultado ser de las más eficientes consiste en incorporar la *Tecnología de la Información* (TI), en los procesos productivos y de servicios de las organizaciones. El término TI aglutina todas las formas de tecnología que son utilizadas para crear, almacenar. y hacer uso de las diferentes formas de información (datos de negocios, archivos de audio, imágenes, archivos de video, presentaciones multimedia, incluyendo además a formas aún no concebidas). De hecho este concepto abarca tanto la tecnología telefónica como la de cómputo.[1]

[1] http://www.whatis.com

Ésta integración de las computadoras en el desempeño de las actividades cotidianas no ha sido casual y tampoco sencilla, pues a pesar de que se ha realizado de forma veloz, no por ello ha sido fácil. La dificultad radica principalmente en la resistencia al cambio que se presenta por parte de las personas. Sin embargo, a pesar de esta resistencia, muchas de las funciones de las empresas como por ejemplo la nómina, los sistemas de cuentas de los bancos, los expedientes de personal, el manejo de créditos, la facturación, etc.; se han automatizado por medio de la TI; logrando en muchos casos, disminuir costos, reducir tiempos, aumentar la calidad de productos y servicios, etc.

Aunque el éxito de la TI en los negocios es notable, no ha parado ahí, sino que ha llegado hasta el consumidor de bienes y servicios promedio (amas de casa, profesionales, estudiantes, artistas, etc.). Estos consumidores han identificado las ventajas que se obtienen del uso de la TI, disfrutando de productos y servicios de mejor calidad; acostumbrándose rápidamente a ellos, convirtiéndose así en consumidores más exigentes que esperan productos y servicios de alta calidad, demandando también, períodos de tiempo más cortos para su realización o entrega. Sin embargo, más allá del éxito que goza la TI entre compradores y productores, su inclusión en el mundo actual, está representando un cambio de la economía en general.

En el comienzo, cuando la TI no jugaba un papel tan importante como hoy día, en la antigua economía el flujo de la información era físico: dinero en efectivo, cheques, facturas, reuniones personales, documentos tangibles, fotografías tradicionales, anuncios distribuidos por correo convencional, etc. Por el contrario, en la nueva economía, la información en todas sus formas es digital, reducida a bits almacenados en computadoras, o en el mejor de los casos viajando a la velocidad de la luz a través de redes por medio de fibra óptica [8] (pp. 6-8).

Entre los múltiples cambios y evoluciones que está originando esta economía digital, aparece el CE que tiene como fines los mismos que el comercio tradicional y abarca todos los procesos que el comercio tradicional abarca: presentación de ofertas y promociones, negociación y entrega de bienes, reclamaciones y servicios de postventa. Todos los procesos se siguen haciendo, pero ahora se cuenta con recursos y medios que antes no existían; oportunidades y riesgos nuevos.

Con respecto a las nuevas oportunidades, el CE permite un incremento en la capacidad de los proveedores de bienes y servicios, de la competitividad global de las entidades comerciales y de servicios, y de las expectativas de los consumidores con respecto a la calidad, costo y servicio. En respuesta a estos cambios se están disolviendo y reinventando las estructuras jerárquicas de las empresas, buscando mayor flexibilidad, dinamismo y especialización; además se están derribando las barreras tanto entre las divisiones internas de las empresas, como las existentes entre las empresas y sus proveedores y clientes. Los procesos comerciales que efectuaban las empresas u organizaciones comerciales y de servicios se están rediseñando de tal manera que los límites y fronteras tanto de tipo geográfico como entre organizaciones están siendo sobrepasadas de forma tan dinámica y versátil como nunca antes.

Gracias a la rápida evolución del CE, resulta favorecida la aparición de un gran número de negocios, mercados y *comunidades digitales*. Estas últimas constituidas por individuos y organismos que mantienen relaciones de diversas índoles por medio de redes como Internet. Un ejemplo de estas comunidades consiste en la asociación de empresas que

integran sus competencias para ofrecer productos y servicios que estarían fuera de la capacidad de dichas empresas si trabajaran de forma aislada. Dentro de estas comunidades es común que las empresas acudan a distribuidores de todo el mundo especializados en la ejecución de pedidos o el transporte y entrega de bienes físicos. Finalmente compradores, vendedores e intermediarios están formando mercados específicos para industrias concretas en Internet, trabajando tanto en ámbitos ya existentes de mercados tradicionales como en nichos de mercado inexplorados [8] (pp. 9-12).

Sin embargo, por muy novedoso que pueda parecer el concepto de CE, la gente ha comprado bienes o contratado servicios, en mayor o menor medida de forma electrónica por años. Por ejemplo el *shareware,* que consiste en una muestra de software con funcionalidad incompleta que puede ser obtenida de forma gratuita o por un precio muy bajo a través de la red por un período de tiempo limitado, ha estado disponible por muchos años bajo la filosofía hacia el cliente de "Pruébelo, y si le convence, cómprelo". De forma similar, la gente ha ofrecido otros productos y servicios, frecuentemente con precios especiales para los usuarios de Internet. En la mayoría de estos casos, aunque la compra se realizaba a través de Internet, el pago era enviado por correo tradicional a una dirección física (usualmente en forma de cheque) [6](pp.190).

Los escenarios anteriormente descritos demuestran que el CE no es un sueño futurista, sino que está ocurriendo actualmente; en algunos casos con resultados muy satisfactorios. Y aunque son USA, Japón y Europa los que liderean el camino, el CE es en esencia global, tanto en concepto como en realización, por lo que sé esta llevando a cabo en muchas partes alrededor de todo el mundo.

En este capítulo, se describen en forma detallada los elementos más importantes que involucra el concepto de CE, tales como: entidades participantes, niveles, categorías, ventajas y desventajas del CE, además de los requerimientos elementales para un esquema básico del mismo.

2.2 Definiciones

Dentro del alcance de este trabajo se considerará al CE como: la compraventa de bienes y/o la contratación de servicios, a través del uso de equipos y herramientas (hardware y software) de telecomunicaciones y cómputo, en lugar de hacerlo por medio de intercambio o contacto físico directo [4] (pp.1).

Otra definición establece que el CE[2] designa al conjunto de transacciones comerciales que se realizan parcial o completamente a través de una red abierta (como Internet) o sobre una red privada (aquella cuyas instalaciones y recursos pertencecen a compañías específicas, siendo por lo tanto accesibles sólo para los equipos de dichas compañías). Más precisamente, el CE involucra a todas las operaciones comerciales tales como la publicidad en línea, la *TEF* (Transferencia Electrónica de Fondos[3], que consiste en mover dinero de una cuenta a otra de forma electrónica), *pago electrónico* (aquel que se realiza a través de

[2] http://www.cominfo.cl/faq/faq6.html

[3] http://www.par-ent.com/

medios y herramientas electrónicas [7] (pp. 1-5)), *EDI* ("Electronic Data Interchange"), una de las formas más usadas de intercambio de datos a través de redes de computadoras privadas, etc.; las cuales permiten la concreción de una operación de compraventa y que tienen en común el emplear medios electrónicos.

Como definición adicional de CE, se tiene la siguiente[4]: "El Comercio Electrónico abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más *mensajes de datos*, es decir, toda aquella información generada, enviada, recibida, almacenada o comunicada por medios electrónicos; o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de factoraje financiero *o "factoring"*; de arrendamiento financiero *o "leasing"*; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiamiento de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera".

Una constante en las tres anteriores definiciones son los bienes y servicios que se compran o venden por medio del CE; y puesto que estos bienes y servicios son los objetos básicos del comercio, es conveniente su definición formal:

Se entiende por *bien* toda aquella entidad física que es identificable de otras y que además es entregada a la entidad que la haya adquirido [4] (pp.4).

Por su parte, un *servicio* será definido como aquel acto que es desempeñado por alguna entidad, a cambio de recibir un pago determinado [4] (pp.4).

Finalmente, para la adecuada comprensión de diversos elementos que serán definidos y utilizados en el transcurso de éste trabajo, es importante establecer la diferencia entre un producto físico y uno digital. Un *producto digital* se define como todo aquel bien o servicio que puede ser entregado o desempeñado completamente a través de una red de telecomunicaciones, gracias a su naturaleza digital; mientras que un *producto físico* involucra actividades de logística, tales como transportación de los bienes, o de la persona que prestará el servicio hasta el lugar donde serán entregados o donde el servicio será desempeñado. Por ejemplo un disco compacto de audio, es un producto físico mientras que un archivo de audio obtenido de la red es un producto digital. En este sentido, los esquemas de CE actuales pueden soportar la mayoría de los procesos involucrados en la compra de bienes y el desempeño de servicios físicos, con la excepción de la entrega o desempeño de los mismos. En el caso de los bienes y servicios digitales, éstos pueden ser entregados usando las infraestructuras de telecomunicaciones existentes [4] (pp. 6).

Una vez definidos los conceptos principales relacionados al CE, a continuación se analizará el modelo básico del mismo.

[4] Esta definición fue establecida por el Estado colombiano en su Proyecto de Ley No. 21, por medio del cual se define y reglamenta el acceso y uso del CE, en su capítulo I, artículo 1°. El documento completo puede encontrarse en la siguiente dirección: http://www.qmw.ac.uk/~tl6345/colombia_sp.htm

2.3 Modelo básico de CE

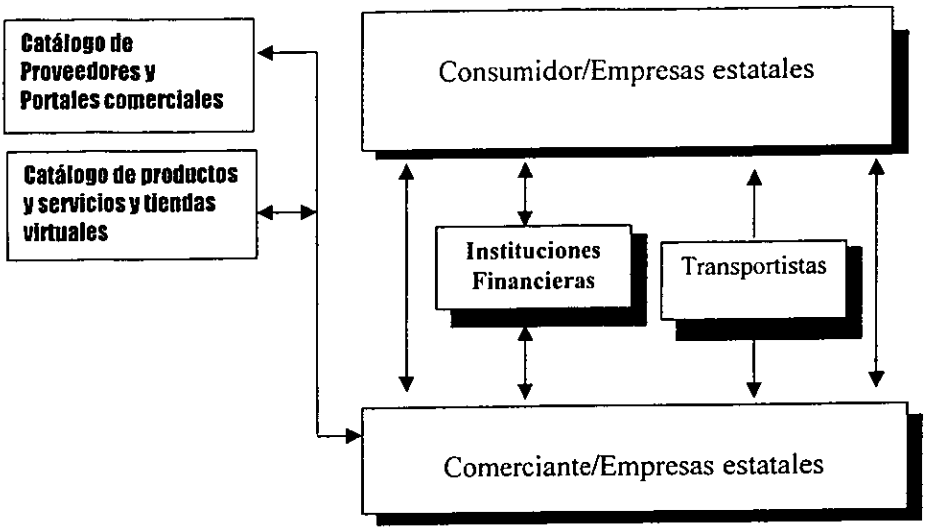

Figura 2-2 Representación gráfica del modelo básico de CE (caso ideal)

2.3.1 Entidades Participantes

Desde un inicio, los esquemas básicos del comercio, han involucrado dos entidades para realizar una transacción. La primera de ellas se define como aquella entidad que desea satisfacer ciertas necesidades, y que cuenta con medios para obtener los bienes y/o servicios que las satisfagan. A esta entidad se le conoce como *consumidor*, *cliente*, o *comprador*. La segunda entidad es aquella que tiene la capacidad de producir los bienes o de prestar los servicios que el consumidor necesita para satisfacer sus necesidades, cobrando algún valor por ello, y se le nombra *comerciante*, *proveedor*, *vendedor* o *empresa*. [5]

En el contexto específico del CE, un consumidor se considera como aquella entidad que compran bienes o contratan servicios a través de herramientas y medios electrónicos como Internet. Establece además comunicación con los comerciantes, por medio de equipos electrónicos, por ejemplo computadoras personales; y a través del uso de software

[5] http://www.activamente.com.mx/boletin/boletin_002b.html

especializado. Un ejemplo de este tipo de software es conocido como *navegador* o *"browser"*, y ha sido diseñado específicamente para visitar los documentos electrónicos que permiten que los datos, imágenes, etc. sean presentados en Internet. Estos documentos son conocidos como páginas web y en ellas están montados los catálogos electrónicos de productos y servicios de las empresas en Internet. Cuando un conjunto de ellas pertenece a un individuo u organización en particular que efectúa CE a cualquier nivel, reciben el nombre de sitio web, "website" o *tienda virtual*. Otra modalidad de este tipo de documentos la constituyen los sitios que se asemejan a un centro comercial en el que se tiene acceso a las páginas de varias empresas y no de una sola; este tipo de páginas se conoce frecuentemente como "*mall virtual* ", *catálogo de proveedores* o *portal comercial*. Bajo este esquema, cuando un posible comprador "navega" por Internet, a través de la tienda virtual de alguna empresa en particular o de algún portal, es como si diera un paseo ya sea por una tienda o fábrica convencional o por un centro comercial y fuera visitando los diversos locales con la opción de comprar en ellos.

Es importante incluir dentro de esta entidad a las *empresas estatales* e *instituciones públicas*, que consisten en entidades que son establecidas y controladas por el gobierno de cada país en específico, y representa a las instituciones gubernamentales que adquieren o venden bienes, o contratan y desempeñan servicios, por lo que pueden considerarse como consumidores o comerciantes según sea el caso. Como ejemplos de este tipo de entidad en México se tiene a la Secretaría de Contraloría y Desarrollo Administrativo (SECODAM), la Secretaria de Comercio y Fomento Industrial (SECOFI), etc.

En cuanto al vendedor dentro del contexto del CE, es aquel individuo u organización que ofrece y/o vende productos y servicios a través de páginas en el web. Esta entidad debe contar con sistemas de cómputo específicos para poder realizar la promoción y venta de sus productos o servicios, a través del web. Idealmente estos sistemas deben garantizar que la información involucrada en la compraventa cuente con protección adecuada.

Aunque tanto el comerciante, como el consumidor son las entidades básicas y aquellas que se presentan más comúnmente en una transacción de CE, es frecuente que participen algunas entidades adicionales como por ejemplo las *instituciones financieras y los transportistas*. Las instituciones financieras con frecuencia son representadas por bancos, y son las encargadas de respaldar las transacciones comerciales a través del web en términos financieros. Esto implica, por ejemplo, que si el comprador desea pagar con una tarjeta de crédito, debe disponer de una cuenta en alguna institución financiera (al igual que el comerciante), de forma que los fondos requeridos para la compra o adquisición del bien o servicio puedan ser transferidos de una cuenta a otra. Es importante aclarar que la institución financiera del comerciante no tiene que ser la misma que la del comprador. Otro punto a resaltar es el hecho de esta entidad no se presenta en forma constante en todos los esquemas de CE, encontrándosele con mayor frecuencia en aquellos esquemas que basan el pago de la transacción en tarjetas de crédito. Por su parte los *transportistas* se definen como aquellas empresas u organizaciones que se dedican a la entrega de mensajes y paquetería, tales como: "FederalExpress", "Estafeta", "DHL", etc. y que en la mayoría de los casos, mantienen contratos con los comerciantes para encargarse de la distribución y entrega de los productos adquiridos por los consumidores de forma electrónica, siendo estos productos de naturaleza física, situación que para este caso en particular impide que el CE pueda prescindir de intermediarios, con los incrementos en costos y tiempo de

entrega que esto supone; entidad que no se presenta en el caso de las transacciones que involucran bienes de naturaleza digital.

Una vez revisado el modelo básico de CE, a continuación se describen las operaciones y procesos que éste involucra de manera general.

2.4 Operaciones y Transacciones que involucra el CE

A pesar de la naturaleza global del CE conferida por Internet, al ser la red principal en la que se efectúa, el CE no es una tecnología única ni tampoco uniforme, sino que se caracteriza por su diversidad, lo que suele implicar un amplio rango de operaciones y transacciones comerciales, entre las que se encuentran [4]:

a) Establecimiento del contacto inicial entre un cliente potencial y un proveedor.
b) Soporte pre y post venta (detalles de los productos y servicios disponibles, guía técnica del uso del producto, respuestas a preguntas de adecuación, etc.)
c) Ventas
d) Pago electrónico, usando TEF, tarjetas de crédito, entre otros
e) Distribución, incluyendo tanto administración de distribución y reparto para productos físicos, como distribución o transferencia de los productos que se pueden repartir de forma electrónica
f) *Asociaciones virtuales*, que consisten en grupos de empresas independientes que integran sus competencias de manera que puedan ofrecer productos o servicios que van más allá de la capacidad de cada una de ellas individualmente.
g) Acceso a información comercial
h) Contratación pública

Sin embargo, aunque el concepto general de CE involucra inicialmente la compraventa de bienes y/o servicios, abarca además ciertas transacciones que no tienen un carácter puramente comercial. Algunos ejemplos de estas transacciones son las siguientes:

a) Inscripciones escolares
b) Trámites administrativos
c) Servicios electrónicos otorgados por agencias de gobierno
d) Trámites de registros y licencias

Todas las operaciones y procesos del CE descritos anteriormente, pueden o no presentarse, dependiendo de las categorías y niveles del CE de que se trate. Estas categorías y niveles del CE se describen a continuación.

2.5 Categorías del CE

De acuerdo a las entidades o agentes implicados en alguna TETC, el CE puede dividirse en cuatro categorías diferentes [4] [6] :

a) Empresa-Empresa

En esta categoría las empresas efectúan negocios entre sí, por lo que en ella se ubican aquellas TETC efectuadas entre organizaciones que tienen tratos de naturaleza comercial, de forma constante, permitiendo que la cantidad de transacciones y de información involucrada sea lo suficientemente alta como para que las empresas establezcan redes privadas para comunicarse entre sí, asegurando de este modo que los datos compartidos viajen de forma segura y veloz. Un ejemplo de esta categoría lo ofrece una compañía que para ordenar pedidos a proveedores, recibir los cobros y realizar los pagos, usa una red privada. Esta categoría ha sido efectuada hace bastantes años, a través del uso de EDI.

b) Empresa-Consumidor

Esta categoría implica que las empresas se dirijan a los clientes finales para comercializar sus productos por medio de una red pública, por lo que su auge ha llegado con el de Internet. Hoy día existen galerías o sitios comerciales sobre Internet ofreciendo todo tipo de bienes consumibles, desde dulces y vinos, hasta equipo de cómputo y vehículos a motor. Esta categoría es la que nos ocupa en particular en este trabajo.

c) Empresa-Estado

Esta tercer categoría del CE, abarca todas las transacciones entre las empresas y las organizaciones gubernamentales. Por ejemplo, en México las convocatorias que realizan las dependencias de gobierno para adquirir o contratar bienes o servicios, se realizan a través del sistema *compraNET®* [7], el cual permite que los proveedores interesados consulten las bases de las convocatorias, realicen sus propuestas técnicas y económicas, paguen los derechos por concursar y conozcan si les fue adjudicada la licitación; todo lo anterior de forma electrónica a través de Internet.

d) Consumidor-Estado

Por último, esta categoría aún no termina de emerger. Sin embargo, a la vez que maduran las categorías empresa-consumidor y empresa-administración, los gobiernos podrán extender las interacciones electrónicas con los consumidores, a diversas áreas, como por ejemplo los pagos de pensiones, el pago de impuestos prediales, contribuciones fiscales, servicios públicos entre otros.

[6] http://www.ver.ucc.mx/pccolon/html/isuec09.htm

[7] Para más detalles del sistema compraNET, dirigirse a: http://compranet.gob.mx

2.6 Niveles del CE

Desde un comienzo, los individuos u organizaciones que deseen realizar negocios en la red deben decidir el grado de complejidad que quieren asumir. Esta complejidad puede ir desde anunciarse en Internet y aceptar pedidos en línea, apoyándose en los mecanismos de pago tradicionales (giro bancario, cheque, etc.), hasta implementar un sistema de pagos a través de la red, es decir un *SEP* [8], en cuyo caso debe invertir más recursos en adquisición de equipo y de personal capacitado para poder hacer uso de las tecnologías que permiten este tipo de pagos.
De lo anterior se desprende, la siguiente clasificación de las TETC tomando en consideración la complejidad de los procesos que involucran y el grado de automatización de los mismos [9].

Niveles básicos

Estos niveles son los que conciernen a la presencia básica de alguna entidad dentro de las redes de información, entendiéndose esto como la simple promoción de los productos y servicios de las empresas a través de catálogos electrónicos; incluyendo en ocasiones servicios de soporte pre y postventa, pero sin involucrar mecanismos de pago. Dentro de estos niveles, es frecuente que la interacción entre los consumidores y los comerciantes se realice por medio de fax o de correo electrónico. Dos de las características principales que presentan estos niveles es la sencillez y bajos costos de implementación que se obtienen usando las tecnologías disponibles hoy en día.

Niveles avanzados

Estos niveles además de abarcar a los niveles básicos, involucran mecanismos tales como : pagos electrónicos, tiendas virtuales (sección 2.9), entrega de productos de naturaleza electrónica, entre otros. Involucran también problemas complejos de índole más legal o cultural que tecnológica, debido a las diferentes legislaciones que rigen las relaciones comerciales y a los diversos patrones de consumo de cada país en particular. Las consecuencias que se desprenden de estas diferencias pueden variar dependiendo de si la transacción requiere de operaciones nacionales o internacionales. Esta variación se origina, entre otras razones, por el hecho de que las operaciones de carácter internacional resultan ser más complejas que las que solo implican operaciones nacionales debido a la incompatibilidad entre las legislaciones de cada país, originada por las diferencias entre la tasación de impuestos, las leyes contractuales, las formas de pago y las diferentes prácticas financieras.

Otra de las problemáticas principales que se presenta en estos niveles radica en el hecho de que no hay soluciones estándar que resuelvan de forma eficiente y completa las necesidades específicas de cada organismo o empresa, por lo que las organizaciones se ven

[8] Un *SEP (Sistema Electrónico de Pagos)*, es un tipo de sistemas que permiten que el pago de alguna transacción, se efectúe de forma electrónica

[9] http://www.sopde.es/cajon/comercio/home.html (pp.4-5)

forzadas a desarrollar sus propios sistemas a medida, provocando que en la actualidad las empresas grandes y ricas sean las pioneras en el desarrollo e implantación de sistemas que permitan la realización de TETC a niveles avanzados. Sin embargo a partir de la experiencia de dichas empresas se irán extrayendo, en forma gradual, soluciones comunes que permitan que estos procesos formen parte de las tecnologías más usuales, como ha ido ocurriendo con los procesos de los niveles básicos.

Por lo tanto, se puede concluir que el CE no se circunscribe sólo a las modalidades electrónicas de pago, pues aunque el mercado digital adquiere real relevancia cuando los niveles avanzados se generalizan, los niveles básicos resultan ser también pasos importantes, toda vez que cumplen con una función comercial no despreciable. Es por esto, que aunque no se realice propiamente ninguna transacción electrónica, modifican de cierta forma las condiciones de comercio al servir de punto de partida de una transacción.

Como ya se ha mencionado, en este trabajo se considera a las TETC como un sinónimo de CE. Sin embargo, por razones de claridad, en el siguiente apartado se utilizará principalmente el termino de TETC.

2.7 Fases de una TETC

Después de revisar las categorías y niveles en los que puede desarrollarse una TETC, es importante definir las fases en las que estas se dividen, pues a pesar de que en el mundo real cada una de estas fases son fácilmente identificables entre sí, existen ciertas circunstancias en las que dos o más de estas fases se mezclan u ocurren en una secuencia distinta. A continuación cada una de estas fases es descrita, mostrándose de forma gráfica en la figura 2-2.

1. *Fase pre-contractual*

   En el inicio de una TETC el comprador busca información acerca de bienes y servicios, de sus precios, características técnicas, término y condiciones aplicables a su compra o adquisición, además de información acerca de los proveedores que los venden o los proporcionan.
   El vendedor por su parte busca a posibles compradores de sus bienes o servicios. Esto es identificado generalmente como el mercadeo o publicidad.

2. *Fase contractual*

   Durante esta fase se establece una relación formal entre el comprador y el comerciante, incluyendo los términos y condiciones bajo las que realizará la transacción.
   Si la TETC se ubica en los niveles avanzados del CE, esta fase incluirá el establecimiento de los esquemas de cifrado, llaves de sesión y demás aspectos relacionados con la seguridad de la información confidencial que será intercambiada y generada durante la transacción.

3. *Fase de pedido*

Incluye la generación y procesamiento de órdenes de compra por parte del comprador, es decir una oferta o pedido, y su aceptación por parte del comerciante. Es también en esta fase donde frecuentemente los compradores envían los datos asociados a su institución financiera, tales como el número de cuenta en caso de un pago electrónico usando tarjetas de crédito.
Algunos esquemas de CE permiten fases para realizar correcciones, re-negociaciones y cancelaciones.

4. *Fase de Acuerdo*

Durante esta fase los bienes o servicios son pagados. Entre las actividades que se incluyen están la facturación, autorización de pago y el pago mismo, entre otros.
En el caso de las formas avanzadas del CE, durante esta fase se incluyen todos aquellos procesos que involucran las diferentes formas electrónicas de pago (capítulo 3), por lo que es en esta fase, donde las instituciones financieras entran realmente en acción al gestionar la autorización de pago frecuentemente comunicándose entre ellas por medio de redes privadas de carácter financiero.

5. *Fase de logística*

Esta fase se encarga de la entrega de los bienes y/o el desempeño de servicios. Además algunas actividades de post-entrega pueden realizarse como inspecciones, o devoluciones.
En ocasiones, resulta conveniente para las organizaciones contratar los servicios de empresas especializadas en entrega y envíos, debido a lo importante que resulta el hecho de que el comprador reciba en tiempos y condiciones adecuadas los productos o servicios adquiridos.

6. *Fase de Post-Proceso*

Después de que la transacción ha sido realizada en términos generales, ciertas actividades adicionales pueden ser efectuadas. Comúnmente, la información generada por las transacciones es recopilada y presentada en forma de reportes, en algunos casos puede existir la obligación de almacenarla, para intercambiarla con asociaciones de industrias o con organismos de estadística nacionales. Además, la venta pudo haber generado una relación adicional entre el comerciante y el comprador, con relación al servicio, mantenimiento, actualización y reemplazo eventual de bienes o componentes de los mismos.

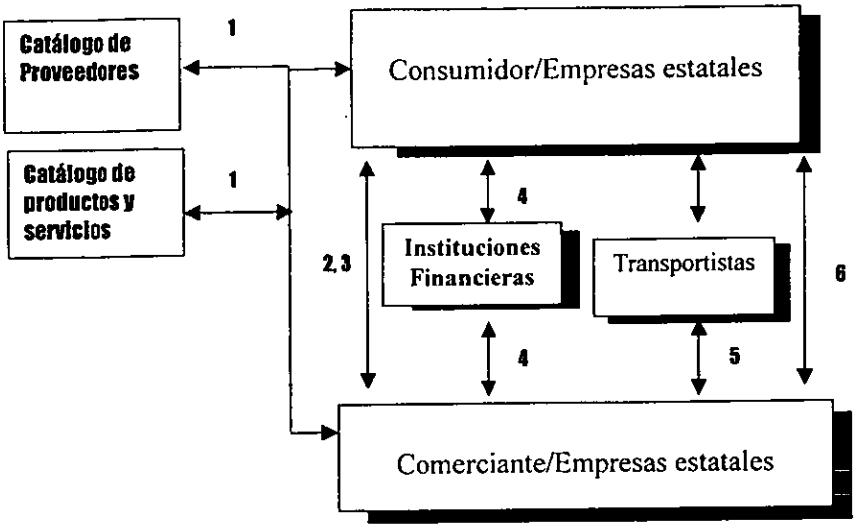

Figura 2-2 Representación gráfica de las fases que integran una TETC (caso ideal)

Como toda tecnología, el CE presenta aspectos positivos y negativos. En este sentido algunos de los aspectos más sobresalientes tanto buenos como malos, que en forma general presenta el CE son detallados a continuación.

2.8 Ventajas y desventajas del CE

Ventajas

Entre las ventajas que el CE ofrece con relación al comercio tradicional tenemos las siguientes [10]:

a) *Presencia global de los comerciantes y sus productos*

[10] http://www.spode.es/cajon/comercio/home.html

El CE no está limitado por fronteras geográficas o nacionales, sino por la cobertura de las redes de computadoras. Debido a que las redes más importantes, como Internet, son de ámbito global, el CE permite, incluso a los proveedores más pequeños, alcanzar una presencia global y efectuar negocios en todo el mundo.
El beneficio correspondiente para el consumidor es la *elección global,* ya que está en la posibilidad de elegir de entre todos los proveedores potenciales de un determinado producto o servicio, sin tener en cuenta su localización geográfica.

b) *Posibilidad de compra/venta las 24 horas del día los 365 días del año*

Asociada a la presencia global se tiene la posibilidad de que los productos sean presentados por medio de Internet las 24 horas del día los 365 días del año, implicando la posibilidad de compra en este mismo rango. Esta flexibilidad de horario frente a la limitación en los horarios de apertura de los comercios tradicionales o ante el incremento de precios en los horarios nocturnos representa una ventaja considerable, ofreciendo al cliente un amplio rango de tiempo para realizar compras o contratar servicios. A pesar de esta mayor flexibilidad no se debe olvidar que aunque la compra puede realizarse en un lapso de tiempo considerablemente reducido, la entrega del producto adquirido toma un tiempo mayor, sobre todo en aquellos casos en que la empresa u organización con la que se realizó el trato esta fuera de la ciudad o país del domicilio en el que se entregará los productos

c) *Aumento en la competitividad/calidad del servicio*

Gracias al uso de la tecnología que el CE involucra, los comerciantes pueden ofrecer mejor soporte pre y postventa, a través de incrementar los niveles de información a cerca de los productos promocionados, las guías de uso, además de dar una rápida respuesta a las demandas de los clientes.
El beneficio correspondiente para el consumidor es una mejora en la calidad del servicio, que entre otras cosas tiene la posibilidad de un acercamiento dinámico y ameno al catálogo de productos y servicios de las empresas mediante las características de interactividad y multimedia del web, impidiendo de esta manera que esta nueva forma de promocionar los productos y servicios pueda equipararse con los catálogos tradicionales utilizados desde hace varias décadas.

d) *Productos y servicios personalizados*

Por medio de diversos mecanismos, el CE puede permitir a las empresas, obtener información detallada de las necesidades de cada cliente en particular y ajustar automáticamente sus productos y servicios de acuerdo a ciertas necesidades y características específicas. Dicha información puede ser obtenida directamente de los consumidores, mediante páginas que muestren formas de captura de datos relacionados con hábitos y preferencias de compra, o mediante el uso de "*cookies*", las cuales consisten de pequeñas cadenas de información almacenadas en las computadoras de los compradores, bajo su permiso, que permiten conocer hábitos de acceso a las

páginas web o la frecuencia de estos por parte de cada usuario en particular. Estos esquemas pueden proporcionan información suficiente para el desarrollo de productos a medida comparables a los ofrecidos por especialistas pero a precios de mercado masivo.
Un ejemplo sencillo de lo anterior se da cuando un posible cliente visita un sitio web de alguna empresa en particular, y se le anima a proporcionar sus datos personales, de contacto y la información que solicita sobre productos o sobre la empresa. Todos estos datos son utilizados para conocer los gustos, preferencias, etc. del posible comprador y, preparar con base a los mismos, la información solicitada de la manera más adecuada para el cliente.
En este sentido, algo de lo que se a vecina en un futuro muy próximo, es la aparición de la figura del *prosumer* (mezcla de productor y consumidor), del cual se pretende que sea capaz de diseñar en línea (mediante Internet) y de manera exacta el producto que desee, eligiendo su color, características técnicas, extras que requiera, etc. Las compañías que desarrollen correctamente este concepto prácticamente estarán creando un mercado cautivo, pues se espera que los productos logrados bajo este esquema sean exactamente los deseados por el cliente, eliminando de esta manera la mayoría de los motivos de queja originadas por características no deseadas de los productos.

e) *Cadenas de entrega y distribución más cortas o inexistentes*

En la actualidad bajo los esquemas del comercio tradicional, hay ocasiones en las que las entidades que venden los productos al comprador final son los mismos que los entregan, sin embargo, no siempre es así. En este sentido el CE también permite el contacto directo entre el fabricante y los consumidores, evitando en buena medida los incrementos en el costo final de venta de los productos o servicios, originados por las ganancias de las entidades intermediarias tan comunes en los esquemas de comercio tradicional. Sin embargo como en todo existen las excepciones que en este caso las constituyen los portales comerciales, en los que frecuentemente una empresa en particular se limita a promocionar y vender productos de las empresas fabricantes por lo que de alguna manera dicho portal juega el papel de intermediario entre el consumidor y los fabricantes. Adicionalmente a estos portales se consideran como intermediarios a las compañías de mensajería y paquetería encargadas en la mayoría de los casos de la entrega de los productos de naturaleza física, por lo que a pesar de que el trato sea directo entre el comprador y el fabricante, esto no implica que la entrega de bienes o el desempeño de servicios sea en todos los casos también directo.
A este respecto, hay muchos ejemplos habituales en los que los bienes son vendidos directamente por los fabricantes a los consumidores, evitando los retardos postales, los almacenamientos intermedios, el aumento de costos debido a la ganancia de los intermediarios y los retrasos de distribución. De hecho, aunque la distribución directa ya es posible usando catálogos en papel o por medio de compras por teléfono o correo convencional, el CE contribuye además a permitir que esta distribución directa sea práctica en términos de precio y tiempo especialmente en los casos de los bienes y servicios de naturaleza digital. Un ejemplo extremo de este escenario se presenta, como se acaba de mencionar, con los productos y servicios que pueden ser distribuidos en forma electrónica, en los que la cadena de distribución puede suprimirse

completamente. Esto tiene implicaciones masivas en la industria del ocio (películas, vídeo, música, revistas, periódicos), para las industrias de la información y la educación (incluyendo todas las formas de publicidad) y para las empresas de desarrollo y distribución de software.
En este caso el beneficio por parte del consumidor es la posibilidad de obtener rápidamente el producto que necesita, sin estar limitado a los "stocks" actuales (sólo en caso de los bienes y servicios digitales) de los distribuidores locales. Además, como otra faceta de lo mismo, en empresas de mensajería se comienzan a implantar sistemas que permiten al cliente efectuar un seguimiento directo y en tiempo real del estado de su envío, hora probable de llegada, si se ha recibido ya o no, etc. y en general todos los datos pertinentes para el seguimiento personal, por parte del cliente, de todo lo referente al producto adquirido.

f) *Reducción de costos de transacción y disminución de precios.*

Esta es una de las mayores contribuciones del CE, pues mientras que el costo de una transacción comercial que implica interacción humana puede medirse en dólares, el costo de llevar a cabo una transacción similar electrónicamente pueden ser de sólo algunos pesos. De aquí que, algunos procesos comerciales que implican interacciones rutinarias, como por ejemplo una rápida y barata actualización de la información que las empresas desean ofrecer a sus clientes como: catálogos, nuevas sucursales, etc., pueden reducirse de costo substancialmente, lo que llega a representar disminuciones considerables de precio de operación que se reflejan en los precios de venta para los clientes. Sin embargo, hay que considerar que en ocasiones, el comprar en países diferentes al de residencia, implica costos y tiempos de entrega más elevados; existiendo también la posibilidad de que el producto pueda conseguirse en forma local a través de comercio tradicional a precio y en periodos de tiempo considerablemente más bajos.

g) Generación de nuevas oportunidades de negocios

Además de redefinir los mercados para productos y servicios ya existentes, el CE también proporciona productos y servicios completamente nuevos. Los ejemplos incluyen servicios sobre redes, servicios de directorios en algún servidor externo (espacio en disco), o servicios de contactos, esto es, establecer los contactos iniciales entre los clientes y proveedores potenciales y muchos otros tipos de servicios de información en línea.

h) Bajo nivel de riesgo

Gracias a que la tecnología necesaria para la implantación del CE no es difícil de conseguir, además de que la seguridad que se le brinda a la información involucrada en transacciones de CE está basada (como se explicó en el capitulo 1) en técnicas criptográficas y de que se encuentra en un proceso de continua mejora y abaratamiento, el CE ofrece bajos niveles de riesgo, los cuales en ocasiones están por debajo de los presentados por medios tradicionales de comercio. Lo anterior se consigue por medio

de la implementación de servicios de seguridad que permiten un nivel de riesgos bajo gracias a técnicas como el cifrado, las firmas y sobres digitales entre otras descritas en el capitulo 1 de este trabajo.

i) Publicidad no agresiva

Por último, esta ventaja radica en el hecho de que la publicidad ofrecida en Internet no es agresiva, puesto que es el cliente el que acude a ella y no viceversa, como en los medios de comunicación tradicionales.

Las anteriores ventajas sólo son una muestra del total que presenta el CE. Sin embargo éste también presenta una serie de desventajas, algunas de las cuales se listan a continuación.

Desventajas [11]

a) *La intangibilidad del producto promocionado*

Esta situación se muestra como uno de los mayores frenos para la compra de productos por este medio. El comprador tiende a no fiarse de un producto que no puede tocar, y cuya publicidad se basa en potentes herramientas informáticas capaces de disimular o de obviar cualquier elemento negativo de este.

b) *La idiosincrasia, costumbres, e idioma de una cierta población o país.*

Como ejemplo de esto, se tiene el caso de un fuerte rechazo hacia el hecho de que adquirir un bien o contratar algún servicio se limite al simple acto de compra o contratación, sin que implique una serie de relaciones e interacciones sociales, siendo sustituidas estas por un frío e impersonal pedido por teléfono o por Internet. Este es un hecho del que pueden dar fe empresas que han intentado introducir a ciertos países como España la venta por catálogo, y que prácticamente han desaparecido poco tiempo después de constituirse.

c) *La escasa confianza en la seguridad de la transmisión de información por Internet*

Esta que es una de las mayores resistencias por parte de los empresarios a la hora de adoptar un sistema de CE y ha sido fomentada por los medios de comunicación y sus noticias sensacionalistas sobre el pirateo informático. Este es un aspecto psicológico que debe ser superado mediante la demostración fehaciente de los avances logrados en este campo por las nuevas herramientas de software, ya que éste constituye un campo que merece una muy especial atención por parte de los programadores y de las autoridades mundiales con campo de actuación en la seguridad sobre Internet. A este respecto desde hace ya varios años diversas entidades como desarrolladores, empresas e investigadores se han ocupado de la implementación de técnicas que ofrezcan niveles

[11] http://www.sevsigloxxi.org/ActEmpr/comercelec.htm#Introducción

de seguridad adecuados y suficientes para la información involucrada, dando como resultado una serie de esquemas que basándose en la mayoría de los casos en técnicas criptográficas tales como: el cifrado de información, firmas digitales, funciones hash, entre otras, proporcionan la seguridad requerida para información tan confidencial como el número y nombre del comprador que es frecuentemente intercambiada durante una transacción de CE. La descripción detallada de cada una de estas técnicas ha sido establecida en el capitulo 1 de este trabajo, mientras que un análisis detallado de cuatro de los esquemas de CE mas utilizados actualmente es desarrollado en el capítulo 3 y 4 del mismo.

d) *Los requerimientos e infraestructura necesaria*

Una serie de desventajas importantes del CE surge de los requerimientos y la infraestructura necesaria para la realización del mismo, entre los que se incluyen: equipos de cómputo, redes de comunicaciones, legislación tanto legal como económica, sistemas políticos entre otros que afectan en mayor o menor medida el desempeño e implantación de esquemas de CE dependiendo del país o región en cuestión.

e) Necesidad de servicios de empresas de entrega paquetería

Esta otra desventaja que presenta el CE, se observa sobre todo en sus niveles avanzados, y está asociada a la necesidad de los servicios de empresas dedicadas a la distribución y entrega de productos y paquetes, servicios que incrementan los costos y tiempos de entrega de los productos adquiridos de naturaleza comercial.

Se espera que un futuro, las ventajas ofrecidas por el CE, superen a las desventajas; de hecho esta especulación contará con múltiples oportunidades de ser comprobada a corto y mediano plazo gracias a la gran cantidad de empresas que están implementando algún sistema de este tipo. Sin embargo, en la mayoría de las ocasiones, mientras mayor sea el número de cualidades positivas que presente un sistema de CE, mayores serán los recursos que requiera, teniendo por ejemplo que los costos de implementar sistemas de CE a niveles básicos son con frecuencia de bajos a moderados, mientras que efectuar CE a niveles avanzados implica costos elevados. A continuación, se describen los requerimientos para un esquema general de CE.

2.9 Requerimientos básicos para un esquema general de CE

Dependiendo del grado en que se realiza el CE son los recursos necesarios para que un comerciante pueda disponer de sistemas que le permitan efectuar TETC. A continuación se listan los requerimientos mínimos, para que un comerciante establezca un sitio comercial en Internet, para efectuar CE en sus niveles más básicos:

1. Equipo

Se debe contar con al menos una PC o estación de trabajo que cuente con la configuración (memoria, espacio en disco, procesador, etc.) suficiente para que pueda funcionar como servidor web, de tal modo que atienda a las solicitudes provenientes de las máquinas de los posibles compradores.

2. Conexión a Internet

Esta conexión se obtiene frecuentemente a través de los servicios de alguna empresa dedicada a tal fin, empresas conocidas comúnmente como ISP's ("Internet Service Provider").

3. *Herramientas y lenguajes de programación* tales como:

a) Editores de páginas HTML y de imágenes
b) Lenguajes de programación que permitan realizar ciertas transacciones por medio de las páginas web. Entre estos lenguajes se cuentan: Java, PERL, C, entre otros.
c) Herramientas informáticas que permitan manipular e interactuar con objetos multimedia, bases de datos, etc.

4. Recursos humanos

Se debe disponer del personal necesario para que desarrolle las páginas HTML, las imágenes para el diseño gráfico, y en general que configure y ponga en funcionamiento el sitio web.

Con este conjunto de recursos, se pueden construir desde simples sitios web, hasta catálogos electrónicos. Sin embargo, en el caso de CE a niveles más avanzados, una de las formas más comunes en que se llevan a cabo las transacciones electrónicas es por medio de una *tienda virtual*, que como se mencionó anteriormente consiste en una serie de páginas web, que dependiendo el grado en que la organización pretenda realizar el CE, contendrá diversos elementos, los cuáles van desde los simples y baratos hasta los sofisticados y costosos. Entre estos elementos se cuentan:

1. *Catálogos electrónicos*, que muestren los productos y servicios que vende la empresa.

2. *Carrito de compras* o *"merchant server"*, el cual consiste en un software que procesa la sesión de compra en la tienda virtual. Aparte de las funciones que incluye para administrar las selecciones del cliente, el carrito de compra calcula: totales e impuestos, considerando casos específicos como descuentos, ofertas, etc. Este software debe ser fácilmente accedido por el cliente para agregar, eliminar, y cambiar productos del pedido en cuestión.

3. Creación de la *trastienda* o *"backoffice"*, la cual consiste en aquellos sistemas que a nivel local se encargan de las operaciones de facturación, inventarios, etc. para que se

puedan visualizar los pedidos realizados y el detalle de los mismos, producir informes y generar estadísticas.

4. *Medios de pago utilizados.* Una de las características más relevantes en las formas avanzadas del CE, es la posibilidad de que el cliente realice los pagos en tiempo real de manera electrónica. Las opciones más frecuentes para este tipo de pago son analizadas a detalle en el capítulo 3.

5. *Logística de envío de productos a los clientes*, que permita la entrega adecuada, oportuna y en buenas condiciones de los productos, frecuentemente realizado por los transportistas.

6. *Integración con los sistemas de la empresa;* los cuales cumplen con funciones vitales tales como: gestión de pedidos, generación de facturas y gestión de las actividades de entradas y salidas del almacén. Con objeto de minimizar los gastos de administración y gestión, y dependiendo de los sistemas informáticos, se puede llevar a cabo una integración de la tienda virtual con los mismos.

Hoy día las tiendas virtuales, son una de las formas más utilizadas y rentables para efectuar compras y ventas por Internet; así mismo, la mejor forma de conocer y entender lo que es una tienda virtual es entrar en una. Uno de los sitios comerciales más reconocidos en la red es "Amazon", cuya tienda de libros está en http://www.amazon.com, y que reporta ventas millonarias, teniendo como su centro de operaciones un espacio muy reducido gracias a que no maneja inventarios de mercancías.

Hasta aquí, se han revisado los elementos más importantes que involucra el concepto de CE. En el capítulo siguiente se abordarán los diferentes esquemas de pago que se pueden utilizar para una TETC.

Capítulo 3

COMERCIO ELECTRÓNICO ACTUAL (Esquemas de Pago)

Existen evidencias de que la mayoría de las TETC realizadas alrededor del mundo se efectúan, al menos parcialmente, de forma electrónica. Una parte de estas transacciones pertenece a los niveles básicos del CE y son efectuadas por teléfono o fax utilizando esquemas de pago convencionales tales como: efectivo, cheque y giro, entre otros. La otra parte, que se ubica dentro de los niveles avanzados, utiliza las versiones electrónicas de los esquemas tradicionales del dinero y los cheques, proporcionando también en ciertos casos la posibilidad de efectuar pagos electrónicos utilizando tarjetas de crédito.

Desde finales de los años 70's y principios de los 80's, el estudio y desarrollo de diferentes técnicas para efectuar pagos a través de redes de computadoras de manera segura ha mantenido ocupados a un buen número de investigadores, incluidos aquellos de la rama de la criptografía, que como ya se ha visto es una de las técnicas que permiten la realización de transacciones de CE de manera segura. Sin embargo, es a partir del auge de Internet que el desarrollo de técnicas que protejan a la información involucrada en una transacción efectuada en internet se ha vuelto una necesidad urgente de satisfacer. Esta urgencia ha originado por una parte, el surgimiento de nuevas compañías que pretenden ofrecer diversos esquemas que permitan el pago de manera electrónica de manera segura, y por la otra, alianzas entre las compañías existentes que dirigen sus esfuerzos en la búsqueda del liderazgo en esta nueva área del comercio, circunstancias que han impulsado el desarrollo de múltiples propuestas para efectuar pagos a través de redes de computadoras; propuestas desarrolladas en universidades, centros de investigación, así como en organizaciones comerciales y en el sector financiero [7] (pp.5-16).

En este capítulo se analizan tanto los esquemas de pago convencionales como sus versiones electrónicas, utilizados en el CE.

3.1 Características de esquemas de pago actuales para CE

La forma más primitiva de pago involucra el *trueque*, es decir, el intercambio directo de bienes y servicios, que a pesar de ser utilizado aun en algunas sociedades primitivas, presenta un gran problema conocido como *la doble coincidencia de deseos*. Para describir

este problema considérese un escenario en el que cierta entidad desea intercambiar, por ejemplo, una computadora por un piano. Para que esta entidad pueda realizar el intercambio, debe encontrar a otra entidad que posea el piano y que además esté dispuesta a intercambiarlo por la computadora. Para eliminar este tipo de complicaciones, a través del tiempo, el trueque ha sido reemplazado por diferentes formas de dinero [7] (pp 5).

La forma más antigua de dinero fue conocida como *mercancía-efectivo*, el cual consistía en diversas especias y metales tales como: maíz, sal, oro, plata, etc.; cuyo valor permanecía constante en una zona geográfica bastante amplia, siendo utilizadas como medio de pago. El oro y la plata fueron los elementos más comúnmente utilizados como dinero mercancía, particularmente después de la revolución industrial en el siglo XVIII. gracias a propiedades tales como la transportabilidad y la divisibilidad [7] (pp 5).

La siguiente etapa en el desarrollo del dinero, consistió en el uso de elementos de prueba o constancia, tales como notas de papel, que representaban una cierta cantidad de dinero y que eran respaldadas por depósitos de oro y plata pertenecientes a la entidad que los emitía. Este tipo de comprobante fue conocido como *mercancía estándar* [7] (pp 6).

Más tarde, cuando las economías alcanzaban una gran estabilidad y confiabilidad, se originó el *efectivo confiable*, donde el respaldo hacia las notas de papel resultaba innecesario, bastando que los gobiernos declarasen su validez para que esta fuera ampliamente aceptada [7] (pp 6).

Actualmente, el pago en efectivo es la forma más popular para pagar bienes y servicios. Sin embargo, debido a que muchas de las cantidades que se manejan hoy en día son enormes y que la seguridad del efectivo se ha convertido en un aspecto muy complejo por sí mismo, se puede observar un incremento en el número de personas que está evitando tener su capital en esta forma y usa los servicios de una institución financiera para que se encargue de guardarlo. Este fenómeno, permite la realización de diversos esquemas de pago basados en cuentas bancarias. A continuación este tipo de esquemas, junto con los pagos efectuados por medio de efectivo, son analizados, mencionando las características principales de sus versiones electrónicas.

3.2 Esquemas de pago convencionales

En los últimos años, se han generalizado principalmente cuatro esquemas de pago: el efectivo, el cheque, el giro y las tarjetas de crédito, los cuales se describen a continuación.

3.2.1 Pagos en efectivo

Entre los esquemas de pago convencionales, el efectivo es una de las formas más simples y efectivas gracias a características tales como:

a) Facilidad para transferirlo de una persona a otra
b) Garantía de pago, gracias a que el dinero no presenta riesgos asociados a la anulación del pago; por ejemplo por falta de fondos.
c) Facilidad de transportación, en su presentación en papel, puesto que grandes cantidades pueden ser transportadas en pequeñas bolsas o carteras

d) No se debe pagar ningún valor extra por hacer uso del efectivo, lo que hace del dinero un medio ideal para efectuar transacciones de un valor muy reducido
e) Además, el uso del dinero no crea rastros que permitan relacionarlo con la entidad que lo haya utilizado, otorgando por lo tanto anonimato.

Resulta importante aclarar que el dinero en sí mismo no es gratis, ya que para costear su producción y reemplazo en el caso en que el desgaste del papel o metal así lo requiera, los gobiernos de cada país utilizan cierta parte de los impuestos que pagan los ciudadanos para tales fines. A pesar de esto, el efectivo es usado como medio de pago en cerca del 80 % de todas las transacciones efectuadas, convirtiéndose así en el mecanismo más utilizado actualmente[7] (pp. 7).

3.2.2 Pagos a través de bancos

Una de las alternativas al uso del efectivo son los esquemas de pago que ofrecen los bancos. Un ejemplo de estos esquemas es una compraventa en el que tanto el comerciante como el comprador disponen de una cuenta en un mismo banco, esquema bajo el cual, el pago de la transacción puede efectuarse transfiriendo fondos de una de las cuentas a la otra. Este mecanismo, aunque esencial, hoy día es la base de una amplia variedad de esquemas de pago facilitados por la industria de servicios financieros; cada uno con características propias, algunos de los cuales se analizan a continuación.

3.2.2.1 Pagos por medio de cheques

Una de las formas más comunes de pago por medio de cuentas bancarias es el cheque, esquema que además de ser ampliamente conocido, es el más utilizado en los EUA. Los cheques resultan de mucha utilidad en aquellos casos en los que tanto el comerciante como el vendedor poseen cuentas en diferentes bancos. El proceso que se sigue en estos casos es descrito a continuación, mostrándose de forma gráfica en la figura 3-1.

Inicialmente un comprador C expide un cheque al comerciante V como pago de alguna compra o servicio. V por su parte, presenta el cheque en su banco, conocido como *banco recaudador* o *"collecting bank"* (debido a que recibe o recauda los cheques presentados para cobro). Entonces el banco de V deposita en la cuenta de éste último, la cantidad estipulada en el cheque; cabe aclarar que esta disponibilidad inmediata de los fondos no ocurre en todos los casos. Posteriormente el cheque depositado por V se envía, junto con todos los demás cheques cobrados en el transcurso del día, al departamento de cobros del banco, donde son clasificados de acuerdo al banco en el que fueron recaudados. Al día siguiente, estos cheques son enviados al *centro de cobro,* ubicado generalmente en un banco central, donde una serie de bancos se reúnen para intercambiarlos. Durante esta reunión, el cheque cobrado por V se entrega al banco de C. Con el cheque en su poder, este último verifica que la cuenta de C tenga los suficientes fondos como para pagar el monto del cheque y retirar de la cuenta la cantidad indicada en el mismo [7] (pp 7-9).

En caso de que la cuenta contenga los suficientes fondos como para que el cheque sea cobrado normalmente, los bancos participantes en el intercambio de cheques, calcularán la

cantidad que deben pagar a los otros bancos, y viceversa. Finalmente, las cantidades resultantes de esta conciliación, serán depositadas o retiradas, según corresponda, de la cuenta de cada banco que es administrada, a su vez, por el banco central.

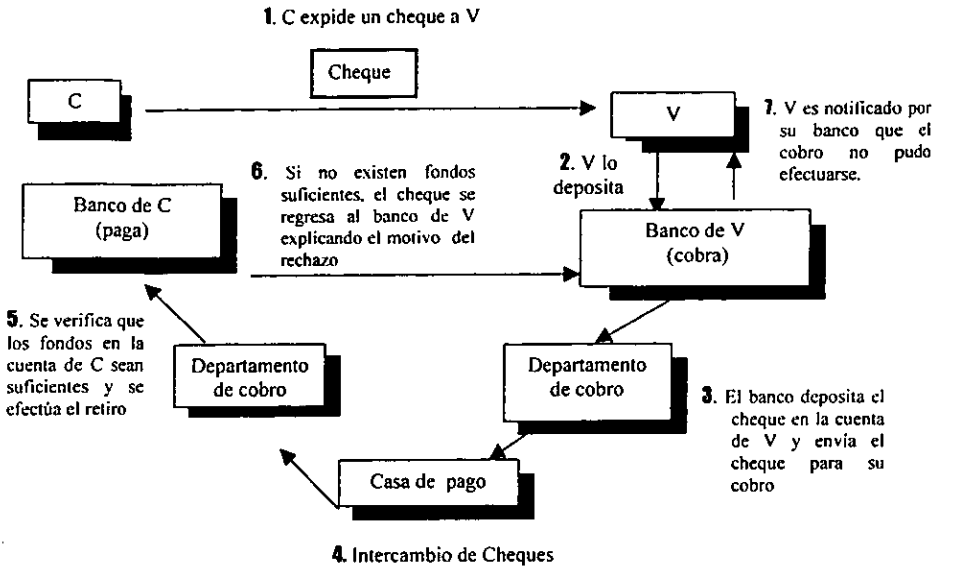

Fig. 3-1 Representación gráfica del proceso de cobro de un cheque

En ocasiones se presentan circunstancias adversas tales como: que no existan fondos suficientes en la cuenta de C, que la firma no coincida con la muestra almacenada por el banco, etc. En este caso, el cheque es enviado de regreso al banco recaudador con las indicaciones necesarias para explicar la razón por la cual no pudo cobrarse satisfactoriamente. Estos casos son conocidos como *elementos rechazados* y representan unos de los mayores problemas del uso de cheques tanto porque V debe pagar una cierta cantidad al banco recaudador por haber depositado un cheque sin fondos, como por los gastos inherentes al manejo del rechazo mismo. Este tipo de desventajas junto con las falsificaciones de firmas y otros tipos de fraudes que involucran el uso de cheques, son algunas de las razones principales debido a las cuales, el número de transacciones liquidadas por este medio esté declinado con los años. Para tratar de evitar este tipo de fraudes se han implementado ciertos mecanismos tales como los *cheques certificados*, que consisten en un cheque convencional, pero que está respaldado y garantizado por una institución financiera, por lo que siempre pueden cobrarse de forma satisfactoria. Otro

mecanismo que persigue el mismo objetivo es conocido como giro o transferencia de crédito, el cual es descrito en el siguiente apartado.

3.2.2.2 Pagos a través de giro o transferencia de crédito

Como una opción adicional a los cheques certificados, el problema de los elementos rechazados puede evitarse usando *una transferencia de crédito o giro de pago*, la cual consiste en una orden donde se indica al banco del comprador, que se transfieran los fondos necesarios al banco del comerciante, de tal manera que la transacción efectuada entre uno y otro quede liquidada. En la figura 3-2 se muestra el funcionamiento de los giros que se desarrolla de forma muy similar a los cheques, con la gran diferencia de que la transacción no puede iniciarse sin antes haber confirmado que el consumidor cuenta con los suficientes fondos como para liquidarla; evitándose de esta manera, cualquier posibilidad de rechazo de elementos, eliminándose en consecuencia los costos asociados a estos rechazos. Otra ventaja que presenta este esquema es la sencillez con que se efectúa de forma electrónica, gracias a que no es necesario transmitir el documento firmado a través de los sistemas de pago, como en el caso del cheque [7] (pp 9).

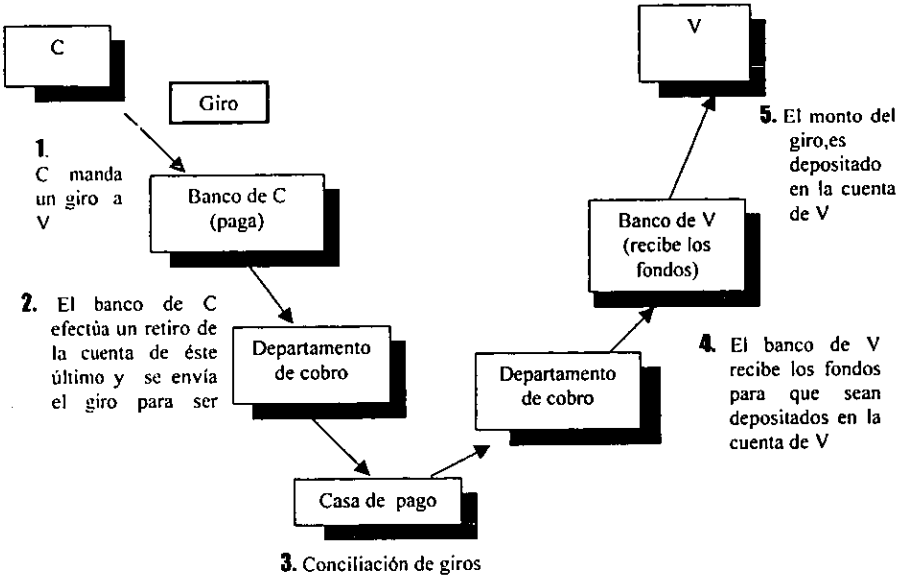

Fig. 3-2 Representación gráfica de un pago por medio de transferencia de crédito o giro

3.2.3 Pagos por medio de tarjetas de crédito

La idea de usar tarjetas de crédito como medio de pago se originó en 1915, cuando un pequeño número de hoteles y tiendas de departamentos de los Estados Unidos de Norte América, se organizaron para emitir, lo que en aquel entonces fue conocido como "placa de comprador"; posteriormente en 1947 el "FlatBush National Bank" (Banco Nacional FlatBush) emitió tarjetas a sus clientes locales. El siguiente avance se dio en 1950 por medio de la creación de la tarjeta de crédito "*Diners Club*", que fue la primera de "viaje y entretenimiento" o de crédito/débito; ocho años después haría su aparición la tarjeta "*American Express*", seguida por las tarjetas "*VISA*"[1] y "*MASTER CARD*" que a partir de ese entonces dominarían hasta nuestros días el amplio mundo de las tarjetas de crédito [7] (pp. 11).

Las tarjetas de crédito fueron desarrolladas para soportar los pagos de transacciones al menudeo, lo que implica que un tarjetahabiente puede efectuar pagos por medio de una tarjeta de crédito, únicamente a un comerciante que este registrado con la institución que haya emitido la tarjeta (comúnmente un banco), para que esta institución respalde el uso de la tarjeta, de tal modo que el comerciante esté en condiciones de aceptar pagos por medio de la misma [7] (pp 11-12).

Un banco que emite tarjetas a sus clientes es llamado *banco emisor de tarjetas* o "*card-issuing bank*". Cuando un banco emisor registra a un usuario, éste es incorporado a la institución financiera como un tarjetahabiente contando, además con una cuenta asociada a la tarjeta, para que en ella sean procesados los pagos [7] (pp 12).

En cuanto a los comerciantes que deseen aceptar pagos de sus clientes por medio de tarjetas, deben registrarse con un banco. En este caso el banco es denominado *banco de adquisición*, "*acquiring bank*", "*acquirer*" o simplemente *adquiriente*. [7] (pp 12).

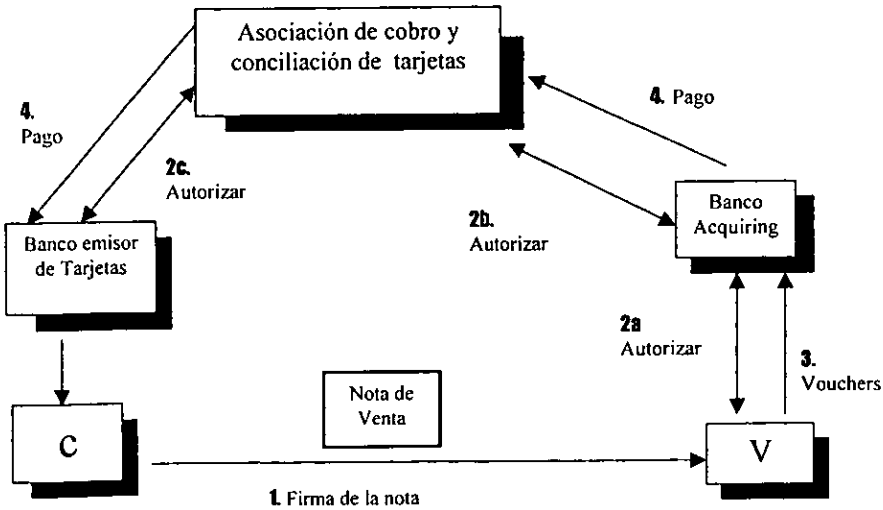

Fig. 3-3 Representación gráfica de las etapas de un pago por medio de tarjeta de crédito

[1] www.visa.com

En un pago por medio de tarjeta de crédito, mostrado en forma gráfica en la fig. 3-3, un comerciante V genera un "voucher"[2] de venta, el cual contiene: el número de tarjeta del comprador C, el monto del pago, la fecha del pago y la descripción de los bienes. Dependiendo de las políticas, se puede requerir que la transacción sea autorizada por parte de una entidad operada, por o en nombre del banco adquiriente, con el objetivo de verificar si el pago puede efectuarse. Esta verificación puede consistir desde solamente confirmar que la tarjeta no se encuentra inhabilitada, hasta una comunicación con el banco emisor, para verificar que existen fondos o crédito suficiente para efectuar el pago.

Al final del día, el comerciante entregará los vouchers de venta al banco adquiriente, el cual, a su vez los cobrará haciendo uso del sistema de cobros, que a pesar de funcionar de forma distinta a los sistemas utilizados en los cheques y giros, estará operado por o en nombre de las compañías o instituciones de tarjetas de crédito. Finalmente, la cantidad necesaria para saldar la transacción se retira de la cuenta de C, depositándola en la cuenta de V. Los detalles de la transacción realizada aparecerán de forma posterior en el estado de cuenta del siguiente mes [7] (pp 12).

Recientemente las asociaciones de empresas o instituciones de tarjetas de crédito y sus bancos asociados, han realizado esfuerzos significativos para eliminar el uso de papel al momento de efectuar transacciones por medio de tarjetas de crédito. Esto significa que los vouchers de venta con la firma del tarjetahabiente serán necesarios solo cuando surja alguna disputa con respecto a la transacción, buscando entonces que la información involucrada en este tipo de transacciones sea enteramente electrónica [7] (pp 12).

Todos los costos asociados con una transacción cuyo pago es efectuado en una tarjeta de crédito son absorbidos por el comerciante, y a pesar de que los detalles de estos costos no pueden ser vistos por el tarjetahabiente, puesto que tiene acceso solamente al monto total de la transacción por medio de su estado de cuenta, es el comerciante el que paga frecuentemente un porcentaje del costo de la transacción, y otro porcentaje muy pequeño del monto total es divido entre la asociación de tarjetas de crédito y el banco adquiriente. Por razón de estos costos, las tarjetas de crédito, no son prácticas en transacciones cuyo monto está por debajo de cierta cantidad (generalmente cerca de los 2 dólares) [7] (pp 12).

Para finalizar con la descripción de la forma en que operan las tarjetas de crédito, a continuación se muestra una clasificación de las mismas de acuerdo a la forma y tiempos en que se realiza el pago:

a) Tarjetas de crédito.

Reciben este nombre debido a que el saldo por pagar de una cuenta de cierto tarjetahabiente no necesita ser pagada forzosamente al final de mes, ya que el tarjetahabiente puede pagar un cierto interés calculado sobre el saldo, usando la tarjeta para obtener crédito. Otros esquemas son posibles, por ejemplo, si el saldo debe ser pagado forzosamente al final del período se les nombra *tarjetas de cobro* [7] (pp.61).

[2] un "voucher" es un comprobante de venta, emitido en aquellas transacciones en las que el pago se efectuó por medio de tarjetas de crédito

b) Tarjeta de débito

Son aquellas tarjetas que funcionan en un esquema en el que una tarjeta es asociada a una cuenta normal de banco para procesar la transacción en tiempo real, es decir, en el mismo período de tiempo en que la transacción se efectúa; el monto de la misma es transferido de la cuenta del comprador a la del comerciante saldando de este modo la transacción efectuada, por lo que un requisito en este esquema consiste en que la cuenta tenga los fondos suficientes para la liquidación de la transacción [7] (pp.62).

c) Monedero electrónico

Este último esquema del uso tarjetas como medio de pago, consiste en incorporar un mecanismo de almacenamiento en la tarjeta, de tal modo que el dinero almacenado en ella es de naturaleza electrónica, y proviene del retiro de fondos de la cuenta bancaria del tarjetahabiente, previo a que dicho dinero sea almacenado en el monedero [7] (pp. 13). Este tipo de tarjetas se explica a más detalle en el apartado 3.3.1

3.3 Esquemas de pago electrónico

A continuación se describen las versiones electrónicas de los esquemas de pago analizados en las secciones anteriores, mencionando su funcionamiento y características generales. Es importante aclarar, que dicha descripción tiene como único objetivo brindar un panorama completo de los esquemas de pago electrónicos que existen actualmente, por lo que los detalles de dichos esquemas están fuera del alcance de este trabajo.

3.3.1 Dinero digital

El *dinero digital* o *dinero electrónico* es el equivalente electrónico del efectivo; y aunque su concepto no es nuevo, la aplicación del mismo sí lo es. De manera general el dinero digital consiste de unidades que pueden ser consideradas como el equivalente de las monedas del efectivo tradicional. Debido a que estas unidades pueden ser generadas por cualquier entidad, deben ser respaldadas por alguna institución financiera de tal modo que por medio de este respaldo obtengan validez y por lo tanto valor. Dicho respaldo se consigue a través de la firma blindada de la institución financiera en las unidades de dinero digital. Como se precisó en la sección 1.5.2, la técnica de las firmas blindadas requiere que el firmante no pueda ver lo que está firmando, razón por la cual el comprador debe demostrar de alguna manera que lo que le esta presentando a la institución financiera es realmente lo que éste le asegura. Esta demostración se consigue por medio de un proceso repetitivo que garantice por probabilidad a la institución financiera, que la unidad de dinero digital que el comprador le presenta para que la respalde contiene las características y datos que el comprador asegura que tiene, incluyendo dentro de estos datos al monto de la unidad misma. Este proceso de demostración consiste a grandes rasgos de que un número k de copias de una unidad de dinero digital, previamente generadas y blindadas, se presente a la institución financiera que se pretende las respalde y de validez. Una vez que las k unidades están en posesión de la institución financiera, ésta debe solicitar al comprador los factores de blindaje de todas las unidades excepto una (k-1). Con estos factores de blindaje la

institución financiera retira éste último de las k-1 unidades obteniendo de este modo acceso al contenido de las mismas verificando para cada una de ellas que el contenido sea el mismo. Tras esta verificación y basándose en la probabilidad, la institución financiera asume que la unidad de dinero digital cuyo blindaje no fue retirado y cuyo contenido no fue confirmado es idéntica a las k-1,procediendo de esta forma a firmar la unidad que aún permanece blindada, otorgándole así validez. Como consecuencia de lo anterior el valor de k esta determinado por las políticas de cada institución financiera, pero por lo general deber ser un número lo suficientemente grande como para que a través del uso del proceso repetitivo anteriormente descrito la institución financiera obtenga una probabilidad muy alta de que la unidad a la que no se le retira el blindaje sea idéntica a las que si se les retiró, por lo que del mismo modo la posibilidad de que el comprador cometa un fraude al banco depende del valor k.

Para facilitar la comprensión del concepto de dinero digital, a continuación se presenta la serie de pasos necesarios para la generación y validación de una unidad de dinero digital:

1. Un comprador que desea pagar una transacción usando dinero digital debe generar k pre-unidades de dinero digital para presentárselos posteriormente al banco. Cada una de estas pre-unidades debe contener el nombre del banco, la cantidad o monto de la "moneda" o unidad y el tipo de divisa (pesos, dólares, francos etc.).
2. A cada pre-unidad generada se le asigna un número de serie lo suficientemente largo como para garantizar que a ninguna de las pre-unidades le sea asignado el mismo número, es decir, que dicho número debe de ser al menos de 64 bits de largo debido a que la probabilidad de que un número de esta longitud generado aleatoriamente se repita dos veces es alrededor de 1 en 2^{64}.
3. Una vez que a cada una de las pre-unidades le ha sido asignado un número de serie, éstas son consideradas como unidades. Los datos de las ahora unidades son pasados a un formato estándar: m_1 = (banco, cantidad, divisa), ... m_k= (banco, cantidad, divisa), donde m_1 representa a la primera de las pre-unidades generadas en el paso 1, y m_k es la última de ellas.
4. El comprador entonces debe "blindar" las unidades con el "factor de blindaje" correspondiente (ver sección 1.5.2 para el concepto de blindaje).
5. Las unidades blindadas se presentan al banco para que las firme digitalmente. El hecho de que las unidades estén blindadas evita que el banco conozca el contenido de las mismas de forma inmediata.
6. Antes de firmar, el banco elige k-1 de las mismas para verificarlas; dicha verificación requiere que el banco solicite los factores de blindaje de todas las unidades excepto una de ellas, es decir que solicita k-1 factores de blindaje.
7. El comprador proporciona al banco todos los factores de blindaje excepto el de una de ellas, lo que significa que proporciona k-1 factores de blindaje.
8. Es entonces que el banco puede retirar el blindaje de k-1 unidades para asegurarse de que el comprador no ha intentado engañarlo, por ejemplo entregando algunas unidades con un monto de $200 en lugar de $100. Si el banco no lograra verificar de forma adecuada las k-1 unidades, podría en ese momento llamar al comprador y levantarle cargos por intento de fraude.

9. En el caso en el que el banco logre verificar de forma adecuada las k-1 unidades, procede a firmar digitalmente a la unidad que permanece blindada, enviando dicha firma al comprador
10. Una vez que el comprador recibe esta firma retira el blindaje a través de multiplicarlo por su inverso.

Cuando esta serie de pasos termina exitosamente el comprador tiene en su poder una unidad de dinero que puede ser utilizada con cualquier comerciante que pueda verificar la validez de la misma a través de autenticar la firma del banco que las expidió (firmó). Si la firma es válida entonces el comerciante puede aceptar las unidades de dinero digital con toda confianza, para posteriormente presentarlas para depósito en su cuenta bancaria.

Como se expuso al inicio de esta sección, el concepto de dinero digital no es tan novedoso como suele creerse y prueba de ello es que desde inicios de la década de los 80's, algunas compañías comenzaron a experimentar con *tarjetas inteligentes* o *monederos electrónicos*, los cuales consisten en tarjetas plásticas (muy similares a las tarjetas telefónicas de prepago) que contienen un microcircuito. Este tipo de tarjetas ha ido sofisticándose con el tiempo y hoy día son programadas con cierta cantidad de dinero disponible, la cual decrece conforme la tarjeta se utiliza para realizar pagos sin necesidad de recibir cambio, o de verificar que existan monedas suficientes para efectos del pago [6] (pp. 206-208).

Otra modalidad del dinero digital es aquel que se genera y reside en una computadora. En este caso, se pueden usar monedas para pagar bienes y servicios de forma inmediata y anónima, además de la posibilidad de recibir cambio digital por sobrepago. Debido a que en este esquema, el dinero digital debe ser autorizado por un banco antes de que pueda entrar en circulación, no se requiere la verificación de fondos de una cuenta bancaria para la autorización del pago.

3.3.1.1 La importancia del anonimato que brinda el dinero digital

Uno de los beneficios más importantes que comparten el dinero convencional y su modalidad digital, consiste en el hecho de que se pueden realizar pagos de forma anónima, situación que adquiere especial importancia en un mundo cada vez más interconectado. El uso del dinero digital es virtualmente irrastreable, a menos que el número de serie de cada moneda sea monitoreando en los lugares que estas hayan sido usadas.

La mayoría de la gente no considera al beneficio del anonimato como algo importante, hasta que se encuentran con cierta información que desea ocultar a otra entidad. Por esta razón, esta característica es particularmente útil cuando el comprador no desea que se le vincule con la compra. Una de las razones por las que las personas desean evitar esta vinculación, consiste en la sencillez con que en ocasiones se puede rastrear el comportamiento de consumo de los compradores, hecho que puede ser aprovechado por criminales para determinar la capacidad de compra de cierta persona, localizando de esta manera a individuos con los suficientes recursos como para ser consideradas como posibles candidatos a víctimas de robo [6] (pp. 207). Sin embargo este mismo anonimato puede inducir a la realización de delitos tales como el lavado de dinero tan frecuente en la actualidad, o el cobro de rescates por el delito de secuestro, puesto que en ambos casos no

se puede asociar la identidad de la entidad que lava el dinero o del secuestrador que cobra un rescate gracias precisamente al anonimato que brinda el dinero digital.

3.3.1.2 Transacciones con dinero digital

El dinero digital debe ser inherentemente seguro, motivo por el cual, las formas de dinero digital deben emplear necesariamente cifrado de información, autenticación, y firmas digitales, técnicas que garantizan que el dinero digital generado es auténtico, seguro y que pueda gastarse sólo una vez.

A continuación se muestra un breve ejemplo, en forma de pasos, de una transacción usando dinero electrónico. Se asume que tanto el comprador C como el comerciante V han acordado una orden de compra [6] (pp.207,208):

1. El comprador C establece una cuenta con un banco que soporte transacciones con dinero digital.
2. C deposita cierta cantidad de dinero convencional en su cuenta
3. C solicita un retiro de dinero digital vía su computadora
4. La computadora determina la cantidad necesaria y el tipo de monedas digitales necesarias
5. La computadora genera las monedas asociándoles números de serie de forma aleatoria, blindándolas posteriormente. A este respecto, los números de serie deben ser lo suficientemente largos como para que haya una probabilidad extremadamente pequeña de que cualquier otra entidad genere el mismo número de serie, por ejemplo utilizando números de 100 dígitos. Con relación al blindaje, éste se realiza utilizando la técnica de las *firmas blindadas* descritas en la introducción de este trabajo.
6. El banco verifica los fondos en la cuenta de C y firma los números de serie blindados
7. La cantidad solicitada es retirada de la cuenta de C, y las monedas firmadas le son enviadas
8. C quita el blindaje a las monedas, dejando así, el dinero electrónico listo para su uso
9. C utiliza el dinero digital para pagar un bien o servicio a un comerciante V
10. V deposita el dinero digital en un banco que soporte transacciones digitales
11. El banco del punto anterior, verifica la autenticidad de las monedas
12. Finalmente, el monto determinado por las monedas es depositado en la cuenta de V.

3.3.2 Cheques electrónicos

De igual manera que la versión en papel, los cheques electrónicos, contienen las instrucciones para que el banco de un comprador C, efectúe el pago de una determinada cantidad a un comerciante V. El hecho de que el cheque electrónico es transmitido a través de redes de computadoras, otorga mayor flexibilidad en el manejo del mismo. Con respecto a los cheques en papel, nuevos servicios pueden ser otorgados como la capacidad de verificación de existencia de fondos; además de que la seguridad puede ser más fácilmente integrada en esquemas de TETC [7] (pp. 125,126).

La figura 3-4 muestra el concepto general de los cheques electrónicos, donde un comprador C, expide un cheque que contendrá la misma información de un cheque convencional. En este escenario, se asume que las entidades participantes poseen un par de llaves para trabajar bajo un esquema de cifrado de llave pública, asumiéndose que alguna AC en particular, ha emitido el certificado correspondiente a las llaves públicas de cada una de las entidades, y mantiene además una estructura adecuada de certificación. A través de variar la información contenida en el cheque, se pueden producir varios tipos de cheques además del convencional. Por ejemplo, si se cambia el tipo de moneda, se puede producir un cheque de viajero, o si se aplica la firma digital del banco, se obtiene un cheque certificado [7] (pp. 126).

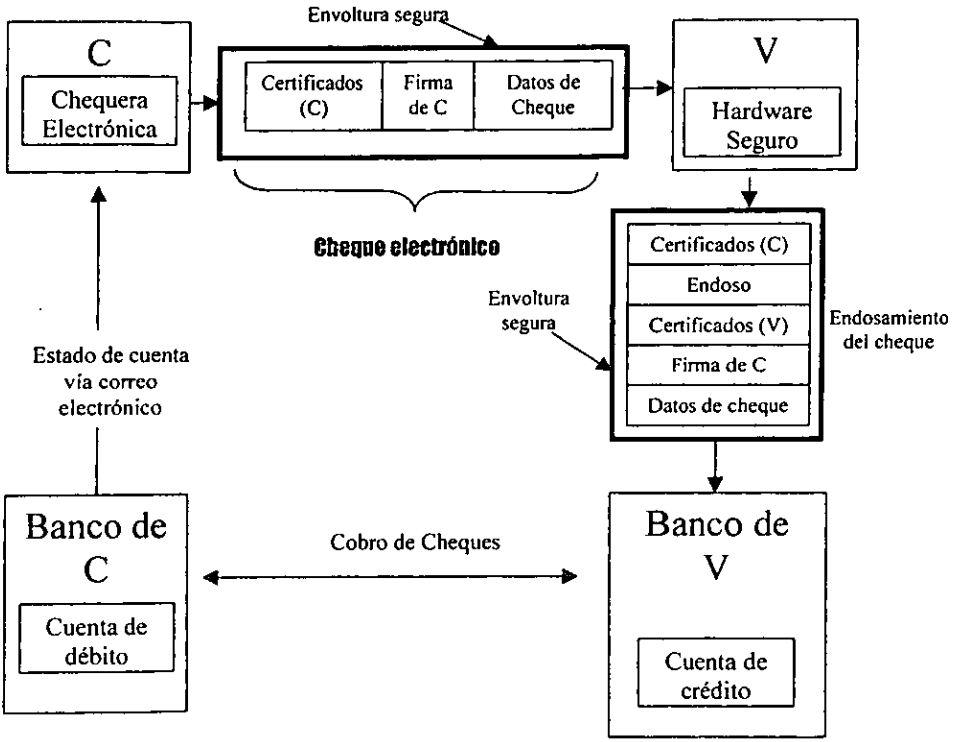

Fig. 3-4 Representación gráfica del concepto de Cheque Electrónico

En este esquema, todos las entidades capaces de expedir cheques electrónicos, deben contar con una *chequera electrónica*, la cual consiste en algún tipo de hardware que implementa mecanismos de seguridad. La función de esta chequera electrónica es

almacenar, de forma segura, llaves para un esquema de cifrado de llave secreta, certificar información y mantener el registro de los cheques que han sido firmados y endosados recientemente. En la figura 3-5 se muestra también cómo el cheque se transporta hacia el comerciante V en algún tipo de envoltura segura, pudiendo enviarse por medio de un correo electrónico seguro, o a través de un diálogo interactivo cifrado entre C y V [7] (pp. 126,127).

Una vez que V ha recibido el cheque, lo endosa haciendo uso de algún tipo de dispositivo de hardware seguro, enviándolo posteriormente a su banco. Una vez hecho esto, los bancos involucrados efectúan los mismos procesos inherentes al cobro de cheques convencionales, descritos en la sección 3.2.2.1 [7] (pp. 127).

3.3.3 TETC usando tarjetas de crédito

A continuación se describen algunas de las modalidades de pago que usan tarjetas de crédito y que se realizan en mayor o menor medida de manera electrónica.

3.3.3.1 Pagos a través de correo convencional y teléfono usando tarjetas de crédito o "Mail Order/Telephone Order" (MOTO)

Desde hace varios años a la fecha, es posible realizar pagos usando tarjetas de crédito sin que necesariamente el comprador y el comerciante estén físicamente en el mismo lugar. Las compañías de tarjetas de crédito tienen ya algún tiempo permitiendo que se ordenen productos ya sea por correo convencional o por teléfono. A este tipo de órdenes de compra se les conoce como *orden por correo/orden por teléfono* o *"mail order/ telephone order"* (MOTO), y las compañías de tarjetas de crédito han establecido reglas especiales para efectuar este tipo de transacciones [7] (pp. 63).

En este esquema, a los tarjeta-habientes se les solicita información adicional tal como: su nombre y dirección. Esta información es utilizada para verificar la identidad del tajetahabiente. Si se trata de bienes físicos, estos son entregados en la dirección asociada a la tarjeta, lográndose de esta manera una protección limitada en contra de ordenes fraudulentas. Sin embargo, desde que no existe una firma del comprador involucrada, las reglas permiten que el comprador niegue o rechace la transacción, situación que incrementa el nivel de riesgo para los vendedores [7] (pp. 64).

A pesar de que hay más posibilidades de fraude asociadas a este tipo de transacción, es una forma de pago muy popular, haciendo evidente que los beneficios que ofrecen superan suficientemente a los riesgos de fraude involucrados.

3.3.3.2 Pagos electrónicos usando tarjetas de crédito a través de redes de computadoras inseguras

Utilizar tarjetas de crédito como forma de pago a través de redes de computadoras presenta riesgos similares a los mencionados para las transacciones tipo MOTO. Los intrusos que *fisgonean* el tráfico de las redes, pueden interceptar mensajes y capturar los datos confidenciales de las tarjetas de crédito; además de cierta información relacionada a

la verificación de datos, por ejemplo: el nombre y dirección del tarjetahabiente. Gracias al formato distintivo bajo el que se definen los números de tarjetas, junto con sus dígitos verificadores incluidos, cierto tipo de programas pueden ser escritos con el fin de identificar dentro del tráfico de la red la ocurrencia de tales patrones. El flujo de datos puede consistir en una transmisión interceptada, un archivo en alguna máquina local e incluso el flujo de tecleos producidos por alguna persona desde una estación de trabajo. Esta posibilidad de identificar dichos patrones agrega un riesgo adicional asociado a los ataques por diccionario o por reflexión, explicados en el capítulo 1 de este trabajo [7] (pp 65).

Sin embargo, este tipo de pagos, ofrecen riesgos mucho más altos que los realizados por medio de transacciones MOTO, debido principalmente a la velocidad con que las transacciones son efectuadas. Y es precisamente por esta velocidad que aquellos comerciantes que efectúan TETC y que soportan pagos electrónicos usando tarjetas de crédito, se enfrentan al peligro de no detectar transacciones fraudulentas sino hasta que varias de ellas ya se han efectuado [7] (pp 65).

No obstante el incremento en los riesgos y la ausencia de esquemas de pago electrónico ampliamente aceptados, la gente está utilizando esta forma de pago de manera considerable. Por su parte, algunos compradores han intentado añadir cierta seguridad por medio de diversas prácticas como por ejemplo dividir el número de tarjeta en varios mensajes. Sin embargo estas medidas se muestran cada vez más insuficientes; insuficiencia que se ha agudizado con el vertiginoso incremento de usuarios de Internet, muchos de los cuales están efectuando pagos en línea por medio de tarjetas de crédito. Antes esta situación, surge la necesidad de esquemas que permitan realizar TETC pagando de forma electrónica usando tarjetas de crédito de una forma segura y sencilla; algunos esquemas que en mayor o menor medida logran estos objetivos son analizados en el capítulo 4 [7] (pp 65).

Hasta este punto hemos revisado los métodos de uso más común en la actualidad para efectuar pagos. Sin embargo, a pesar de que los consumidores de todos los países usan efectivo en la mayoría de sus transacciones diarias y de que la mayor parte de estas transacciones son por un valor reducido, el grado en el que cada uno de los esquemas revisados durante este capítulo son utilizados varía de acuerdo al país; esta variación responde a diversas razones, entre las que se encuentran el grado de desarrollo del país y el estado de los sistemas bancarios, teniéndose por ejemplo que en EUA la forma de pago más utilizada son los cheques, mientras que en Alemania son los giros. Otro aspecto muy importante que cambia de acuerdo a cada país es la legislación, aspecto indispensable en todo esquema de comercio formal, y que es analizado a continuación.

3.4 Marco Legal

Los sistemas de pago son cruciales para el funcionamiento óptimo de toda economía, razón por la cual los gobiernos de cada país se aseguran de regular y controlar de manera adecuada y suficiente la operación de dichos sistemas. Tradicionalmente estos sistemas han sido operados por bancos (al menos en el pasado), los cuales están sujetos a la regulación del Banco Nacional Central de cada país [7] (pp 14).

Típicamente un banco debe ser autorizado para operar. Durante el proceso para esta autorización el banco puede estar sujeto a revisión; esta última puede incluir pruebas para

asegurarse que las personas representantes del banco son confiables y adecuadas para el cargo, que el banco tiene un capital mínimo requerido y de que su servicio satisface las necesidades de algún sector de la sociedad. Estas verificaciones son efectuadas con el fin de asegurar que los consumidores están protegidos contra las consecuencias de fallas y errores responsabilidad de los bancos [7] (pp 14).

En el pasado, todos los métodos de pago tradicionales, involucraban bancos que como se ha mencionado, han estado bajo la supervisión y regulación de un banco central. Los nuevos métodos de pago electrónicos apenas comienzan a ser puntos de atención para ser supervisados por estos bancos centrales. Como se ha establecido a lo largo de este capítulo, muchos de estos nuevos métodos de pago son, salvo ciertas excepciones, extensiones electrónicas de métodos ya existentes operados por bancos, que pueden ser consideradas por las leyes a través de pequeños ajustes a las regulaciones existentes [7] (pp 15).

Por ejemplo en los EUA la *Iniciativa para la transferencia electrónica de fondos* de 1980 establecida por las Regulaciones para la Reserva Federal ("Federal Reserve Regulations") cubre una serie de transacciones bancarias, incluyendo pago electrónico de cuentas, puntos de venta electrónicos, entre otros. Esto limita la responsabilidad de los consumidores en casos de retiro de dinero no autorizados, proporciona procedimientos para la solución de errores y obliga a las instituciones a otorgar recibos de compra y estados de cuenta, lo que representa un muy buen punto de inicio para la regulación de cualquier forma de pago electrónico, a pesar de que la política que a este respecto ha sido adoptada es de "esperar y ver" [7] (pp 15).

Otra de las áreas de interés es la política monetaria. Si los gobiernos son la única entidad emisora de dinero en una economía, pueden ejercer un control sobre la cantidad de dinero en circulación. Operadores de monederos electrónicos y de otros sistemas de dinero electrónico podrán en un principio afectar este balance, disminuyendo el control que los gobiernos podrían ejercer, al emitir el dinero en forma electrónica [7] (pp 15).

Estos y muchos otros, son los temas relacionados al CE que carecen de una formalización real. Entre estos se tienen aspectos tan importantes como por ejemplo la cuestión de si se cobrarán impuestos por cada transacción efectuada electrónicamente y la necesidad de establecer medidas para evitar el lavado de dinero, entre otros. A pesar de que tales situaciones no son triviales, las autoridades de los diversos países entre ellos los Estados Unidos de Norte América y Europa, solamente han comenzado a considerarlos y en el mejor de los casos a trabajar en ellos [7] (pp.15).

Hasta aquí, se han revisado los principales métodos para realizar pagos de forma convencional, sus versiones electrónicas, y algunos aspectos legales asociados a su uso.En el siguiente capítulo se revisarán detalladamente algunos sistemas que implementan TETC y que permiten efectuar pagos electrónicos usando tarjetas de crédito.

Capítulo 4

ESQUEMAS DE COMERCIO ELECTRÓNICO BASADOS EN TARJETAS DE CRÉDITO

En el capítulo anterior se analizaron a detalle las características de los métodos de pago actuales de CE, tanto en sus versiones tradicionales como en las electrónicas. Entre estos métodos se analizaron las tarjetas de crédito, mencionando los aspectos de mayor relevancia que las convierten en uno de los esquemas más idóneos para efectuar pagos de forma electrónica.

Uno de los elementos importantes que han posicionado a las tarjetas de crédito como una de las formas de pago más utilizadas para las compras por internet es la infraestructura tecnológica y las redes de computadoras privadas de carácter financiero con la que cuentan las instituciones financieras que emiten y administran dichas tarjetas de crédito. Aunque esta infraestructura no es de uso exclusivo para las transacciones que involucran tarjetas de crédito, ha permitido en el caso de estas últimas un número considerable de transacciones electrónicas tales como: transferencias de fondos, consultas de saldos, retiro y depósito de efectivo de manera electrónica, y transacciones bancarias vía telefónica, entre otras. Al conjunto de estas transacciones se le conoce como "banca electrónica" y representa una de las razones por las que las tarjetas de crédito son opción idónea para el pago de las compras por internet.

Otro punto a favor de las tarjetas de crédito consiste en la gran aceptación de la que han sido objeto por parte de los consumidores. Aceptación que quizás encuentra su origen en lo práctico que puede resultar el hecho de contar con cierta capacidad de compra o crédito sin disponer necesariamente del efectivo para la misma. Esta característica ha logrado ganarle numerosos adeptos a las tarjetas de crédito a pesar del costo elevado que frecuentemente involucra su uso.

Estos son dos de los aspectos importantes que pueden ser mencionados cuando se desea entender el predominio del uso de tarjetas de crédito en los pagos de compras por internet con relación a otro tipo de pagos como dinero digital o cheques electrónicos.

Actualmente existe un gran número de esquemas de CE que se basan en el uso de tarjetas de crédito como medio de pago, limitándose algunos a la parte teórica o de prototipo, mientras que otros cuentan ya con implementaciones y con un uso amplio

alrededor del mundo. Sin embargo, en nuestro país el conocimiento y uso de este tipo esquemas es incipiente, situación que puede llegar a representar un punto crítico para el desarrollo del CE en el ámbito nacional.

El crecimiento de empresas y organizaciones que efectúan CE en nuestro país está generando una creciente necesidad de información y de personal capacitado con respecto a los diferentes esquemas de CE, incluidos naturalmente, aquellos que se basan en tarjetas de crédito, siendo esta necesidad una de las motivaciones principales por las que en este trabajo se analizan este tipo de esquemas.

En este capítulo se hace una descripción de cuatro diferentes esquemas de CE que usan tarjetas de crédito presentando, además, sus protocolos básicos. Esta descripción servirá como base para el análisis comparativo que se presenta en el siguiente capítulo.

4.1 Especificación del problema

A continuación se describe el planteamiento del problema motivo de este trabajo, presentándose posteriormente la notación que sirve para la presentación de los protocolos de cada uno de los esquemas analizados.

4.1.1 Planteamiento

De manera formal un esquema de CE basado en tarjetas de crédito puede ser visto como un modelo con dos o más participantes ejecutando una tarea específica o protocolo.

Para este trabajo en particular, dicho protocolo debe contemplar ciertos objetivos entre los que se incluye el proporcionar servicios de seguridad tales como integridad y confidencialidad de la información y la autenticación de los participantes, conceptos definidos en la introducción de este trabajo. Dichos servicios están íntimamente relacionados con el CE desde el punto de vista de la seguridad.

El problema pues, puede plantearse en estos términos: cómo efectuar una transacción electrónica de tipo comercial que permita el pago electrónico de la misma usando tarjetas de crédito, garantizando que los datos confidenciales viajen protegidos en su integridad y confidencialidad de una entidad a otra, probando que vienen de la entidad que dice mandarlos, que esa entidad es quien dice ser y que además dichos datos sean accesibles sólo por las partes autorizadas.

4.1.2 Notación

A partir de este capítulo, se utilizará la siguiente notación, que es una de las más comunes en la literatura sobre el tema:

C, V, B Nombres o identificadores para las entidades principales involucradas en los esquemas de pago : comprador, vendedor, e institución financiera o banco.

K_c^P Llave Pública del comprador

X	Mensaje en claro
Y	Mensaje cifrado
$h(X)$	Función hash $h( )$ aplicada a X
K_c^r	Llave Privada del comprador
$C \rightarrow V : C, msg$	C envía su propia identidad y el mensaje msg a V
N_c	Núnico generado por la entidad C.
$E_k(X)$	Cifrado de X, utilizando un criptosistema de llave secreta y empleando a K como llave secreta
$E^p_{K_c^p}(X)$	Cifrado del bloque X, utilizando un criptosistema de llave pública y empleando a K como llave pública de C
$D^p_{K_c^r}(X)$	Descifrado del bloque X, utilizando un criptosistema de llave pública y empleando a K como llave privada de C
$S^f_{k_c}(M)$	Firma digital de M, empleando a k_c^f como llave de firma de C
$V^v_{K_c^v}(M)$	Verificación de firma del M, empleando a k_c^v como llave de verificación de firma
$CERT_c$	Certificado de llave pública de la entidad C, que incluye la llave pública de C
$DESC$	Descripción de los bienes o servicios a comprar o contratar
F	Fecha de la transacción
#	Número de la Tarjeta de crédito con la que C pretende pagar la transacción
$	Monto de la transacción
LST_{acs}	Lista de algoritmos de compresión soportados
LST_{acf}	Lista de algoritmos de cifrado soportados
LST_{cert}	Lista de certificados

DIO	$N_{v_1}, B, F, N_{c_2}, N_{v_2}, N_{c_3}$	Estos elementos ofrecen información acerca de la orden de compra, entre los que se incluyen el identificador de la transacción, identificador del banco. la fecha en la que se realiza la transacción, entre otros.
DIP	$N_{c_1}, \$, h(DESC, N_{c_4})$	Estos elementos ofrecen información acerca de las instrucciones de pago, entre los que se incluye el identificador de la transacción, el monto, de la misma, el valor hash de la descripción, el cifrado de llave pública de C, entre otros.
IP	$E^{P}_{K_b}(N_{c_5}, N_{c_1}, \$, h(DESC, N_{c_4}) \; S^{f}_{K_c}(h(DIO) \oplus h(DIP), h(h(DIO), h(DIP))), E^{P}_{K_b}(\$, F_2, N_{c_5}))$	Las instrucciones de pago o IP incluyen al identificador de la transacción, el monto de la misma, la firma dual de los DIP con los DIO, y en general la información que el banco del comerciante necesita para que se efectúe el pago de la transacción.
estatus	Estado de la transacción tal como: en proceso, cancelada, finalizada, entre otros	
S/N	Código de Éxito / Fracaso de la transacción	
D_{cap}	Datos de captura de pago, que la institución financiera utiliza para identificar un pago en particular	
InfAdic	Información adicional tal como: domicilio de C y giro de la empresa de V, entre otros.	

4.2 Esquemas de CE que usan tarjetas de crédito

A continuación se describen 4 esquemas de pago electrónico, SSL, iKP, SEPP y SET, los cuales usan tarjetas de crédito, presentando para cada uno sus protocolos básicos

4.2.1 SSL ("Secure Socket Layer")

Desarrollado por "Netscape Corporation" a finales de 1994, alcanzó el nivel de estándar al año siguiente; SSL es un protocolo de propósito general cuyo objetivo consiste

en asegurar el diálogo entre aplicaciones en Internet que se comunican a través de un canal de comunicación o *socket*[1] seguro. Hoy día la versión 3.0 de SSL está incluido en la mayoría de los navegadores. Gracias a esta disponibilidad y al diseño de propósito general, SSL es actualmente uno de los esquemas más utilizados para efectuar pagos electrónicos de transacciones de CE [7] (pp 72).

Las partes involucradas en una comunicación a través de SSL se identifican mutuamente, por medio de certificados de llave pública. En SSL no se utiliza una jerarquía de confianza específica, por lo que las aplicaciones tanto del comprador C como del comerciante V deben contar, previo a la comunicación, con una lista de los certificados de las AC con la que esté trabajando cada uno.

SSL es transparente a la aplicación que lo utiliza (comúnmente un navegador), por lo que una vez que tanto C como V cuentan con una implementación de SSL, la información generada y/o involucrada en la transacción, debe viajar a través del socket seguro, de la misma manera en que viajaría por medio de un socket normal (inseguro), pero contando con cierto nivel de seguridad adicional [7] (pp 72).

4.2.1.1 Características principales SSL

Aunque SSL fue diseñado como un protocolo de propósito general, para aplicaciones cliente/servidor en Internet ofrece características de seguridad tales como: confidencialidad de los intercambios o mensajes entre el cliente y el servidor, autenticación de las partes implicadas e integridad de mensajes; servicios obtenidos por medio de cifrado de llave secreta, certificados de llave pública y funciones hash respectivamente, que le permiten funcionar como un esquema de pago electrónico. Para la negociación de los parámetros que serán utilizados para la protección de la información, SSL utiliza un saludo de seguridad con el que inicia la conexión TCP/IP entre un cliente y un servidor; dicho saludo está basado en certificados de llave pública y consiste en una serie de mensajes que son intercambiados para el acuerdo de una llave de sesión y de un algoritmo de cifrado convencional que será utilizado entre el comprador y el vendedor, razón por la que SSL soporta una gama amplia de métodos de este tipo de cifrado. Otra característica relevante de SSL consiste en el hecho de que el cifrado y la autenticación son efectuados a nivel de llamadas a bibliotecas del socket, lo que hace posible que su implementación con miras a Internet sea mucho más simple en comparación con algunos protocolos seguros para ambientes de redes tales como Kerberos [7] (pp 72-73).

4.2.1.2 Protocolo SSL

A continuación se describe de manera detallada el protocolo de SSL.

[1] Un *Socket* es un canal de comunicación o elemento de conexión en esquemas cliente/servidor. Los sockets están asociados a una dirección de host y a una dirección de puerto. La primera es la dirección de la máquina en donde se ubica el programa cliente o servidor, la segunda es el puerto de comunicación que utiliza el cliente o servidor [8] (pp. 644-645).

1. $C \longrightarrow V : N_{c_1}, N_{c_2}, LST_{acf}, LST_{acs}$

2. $V \longrightarrow C : N_v, N_{c_2}, acf, acs, CERT_v$

3. $C \longrightarrow V : E^{p}_{K_v}(K_i)$

4. C y V Generan localmente llave de sesión

5. $C \longleftrightarrow V : E_k(X)$

Fig. 4-1 Pasos del protocolo SSL

4.2.1.2.1 Explicación y análisis de SSL

1. Cuando se comienza una transacción utilizando SSL, C envía un mensaje inicial que contiene:

   a) un núnico de 28 bytes producido por un generador de números aleatorios criptográficamente fuertes [N_{C1}]
   b) una lista de métodos de cifrado y de compresión de información soportados por la aplicación de C [LST_{acf}, LST_{acs}]
   c) Adicionalmente este mensaje incluye un segundo núnico[N_{C2}], el cual establece un identificador, que será usado posteriormente para identificar a la sesión de manera única en transacciones subsecuentes [7] (pp 73)

2. Cuando la aplicación de V recibe el mensaje inicial, elige de entre la lista de algoritmos de cifrado y de compresión, el más seguro [acf] y el más eficiente [acs] respectivamente. La aplicación de V genera además un núnico que debe ser diferente e independiente del incluido en el mensaje inicial enviado por C. Este núnico [N_V], junto con el identificador de la sesión [N_{C2}] y el certificado de llave pública de V [$CERT_V$], son enviados a C como la respuesta al mensaje inicial. Con respecto al certificado de V, éste consiste en una lista en formato X.509[2] versión 3, que contiene el propio

[2] Este formato corresponde al estándar aceptado internacionalmente y emitido por la CCITT para los certificados digitales de llave pública y establece un formato y contenido particulares [12] (pp. 55).

certificado de V, además de todos los certificados que respaldan su validez, hasta llegar al certificado de la Autoridad Certificadora Central o ACC [7] (pp 74).

3. Aunque durante una transacción mediante SSL todas las entidades participantes pueden autenticarse, en este trabajo se considera uno de los casos de uso más común para efectuar pago electrónico, en el que V es la única entidad que se autentica. Asumido lo anterior y siguiendo con el intercambio de mensajes se tiene que C a través de utilizar los certificados contenidos en la lista enviada por V para seguir la línea jerárquica hasta la raíz o ACC, verifica la validez del certificado de V, autenticándolo de esta manera. Después de esta verificación C calcula un valor llamado: PreSecretoMaestro o "PreMasterSecret" [Ki], de 48 bytes; de los cuales los 2 primeros indican la versión de SSL utilizada, y los 46 bytes restantes consisten de datos generados aleatoriamente. Este PreSecreto que contiene toda la información necesaria para la generación de los elementos que proporcionarán la protección de la información en fases posteriores, es cifrado con la llave pública de V, antes de enviárselo a éste último [7] (pp 74).

$$C : \quad K_i \ \text{(Presecreto)}$$

4. Cuando V recibe este PreSecreto, lo descifra con su llave privada, y tomándolo como base genera otro valor llamado SecretoMaestro o "MasterSecret" [K] (éste cálculo es efectuado de manera idéntica por C), de la siguiente manera:

$$\begin{aligned} \text{MasterSecret} = {} & \text{MD(PreMasterSecret + SHA('A' + PreSecret } + N_c + N_v \text{))+} \\ & \text{MD(PreMasterSecret + SHA('BB' + PreSecret } + N_c + N_v \text{)) +} \\ & \text{MD(PreMasterSecret + SHA('CCC' + PreSecret + } N_c + N_v \text{))} \end{aligned}$$

Durante el proceso se combina el "PreMasterSecret" con los núnicos enviados por C y V durante los mensajes previos, utilizando tanto concatenación (+), como las funciones hash MD5 ("Message Digest 5") y el SHA ("Secure Hash Algorithm"). Una vez que el "MasterSecret" ha sido generado, un calculo similar es efectuado de manera repetitiva para generar lo que es conocido como Llave de bloque o "Keyblock", que sirve a su vez como base para la generación de la llave de sesión que se utilizará para asegurar la información intercambiada durante la transacción. Dicha repetición debe efectuarse hasta que se genere la cantidad de información suficiente que será utilizada posteriormente. Este calculo es el siguiente:

$$\begin{aligned} \text{KeyBlock} = {} & \text{MD5(MasterSecret + SHA('A' + MasterSecret } + N_c + N_v \text{)) +} \\ & \text{MD5(MasterSecret + SHA ('BB' + MasterSecret } + N_c + N_v \text{)) +} \\ & \text{MD5(MasterSecret + SHA ('CCC' + MasterSecret } + N_c + N_v \text{)) + [...]} \end{aligned}$$

Dependiendo del algoritmo de cifrado seleccionado por la aplicación de V, la longitud de la llave para cifrar o de sesión (obtenida del "Keyblock") puede variar. En el caso en que quede información del "Keyblock" sin usar, esta simplemente es desechada [7] (pp 74-75).

$$C, V : \quad K \ \text{(SecretoMaestro)}$$

5. En este punto tanto V como C poseen todos los elementos necesarios para comenzar a utilizar el criptosistema acordado, por lo que las aplicaciones de V y C tienen conocimiento de que el socket seguro ha sido establecido pudiendo omenzar a intercambiar la información de la transacción [7] (pp 76).

Cuando SSL es usado para efectuar pagos, V opera una aplicación que implementa SSL y que posee un certificado de llave pública firmado por una autoridad certificadora, que idealmente la aplicación de C considere confiable. Además cuando la aplicación de C realiza una petición a un URL en particular, y la respuesta a dicha petición es efectuada usando SSL, el inicio del URL cambia del conocido *http* ("hipertext transfer protocol" a *https* ("http secure"), lo que indica que se está utilizando SSL para asegurar la comunicación. De esta manera, la aplicación de V en un principio se autentica, después los parámetros de cifrado son establecidos y los detalles de la tarjeta de crédito de C son enviados de manera cifrada por medio de SSL a V, donde pueden ser descifrados y procesados para la gestión del pago posterior [7] (pp 77).

4.2.2 iKP ("i- Key Protocol")

*i*KP (donde i = 1,2,3 hace referencia al número de entidades participantes en una transacción que poseen un par de llaves) es una familia de protocolos diseñados para permitir transacciones electrónicas usando tarjetas de crédito. Fue desarrollado por los Laboratorios de Investigación de IBM en Zurich y por el Centro de Investigaciones de Watson en EUA. Su funcionamiento se basa en criptosistemas de llave pública, y cada uno de los protocolos que integran la familia se diferencian entre ellos por el número de participantes en el protocolo que poseen su propio par llaves, situación que define el nivel de seguridad de cada miembro de la familia. De este modo, en 1KP sólo el banco del vendedor posee un par de llaves; en 2KP tanto el banco del vendedor como este último poseen un par de llaves; y por último, en 3KP todas las entidades poseen un par de llaves. *i*KP permite diferentes rangos de autenticación y por consiguiente diferentes niveles de seguridad [7] (pp. 82,83).

4.2.2.1 Características principales iKP

Como anteriormente se expuso 3KP es el integrante de la familia iKP que proporciona el mayor nivel de seguridad en parte gracias a que en él todas las entidades participantes poseen un par de llaves, lo que proporciona no-repudio en todas los intercambios del esquema que incluyen firmas digitales. En 3KP, utilizando el criptosistema de llave pública RSA, el banco del vendedor firma y recibe datos confidenciales tales como números de tarjetas, y firma mensajes de autorización. En cuanto al banco del vendedor, este puede tener dos pares de llaves: un par para firmar y el otro para cifrar, ambos pueden estar validados por un certificado único. Por su parte el comprador puede tener un par de llaves para firmar instrucciones de pago. Finalmente, el vendedor puede poseer un par de llaves para recibir información confidencial y para firmar solicitudes de pagos y confirmaciones de compra [7] (pp. 83,95).

4.2.2.2 Protocolo *i*KP (*i*=3)

A continuación se describe de manera detallada el protocolo de 3KP.

1. $C \longrightarrow V$: N_{c_1}, C, $h(N_{c_2}, \#)$, $CERT_C$

2. $V \longrightarrow C$: V, F, N_{v_1}, N_{v_2}, $S_{k_v}^f(\$, h(N_{c_1}, DESC), h(N_{v_3}))$, $CERT_V$

3 C : Calcula $h(N_{c_1}, DESC)$ y lo compara con $h(N_{c_1}, DESC)$ enviado por V. Si coinciden, C y V están de acuerdo en el pedido

$$C \longrightarrow V : V, F, N_{v_1}, N_{v_2}, S_{k_c}^f(E_{k_b}^p(\$, h(N_{c_1}, DESC), \#, N_{c_2}))$$

4. $V \longrightarrow B$: $V, F, N_{v_1}, N_{v_2}, S_{k_v}^f(h(N_{c_1}, DESC), h(N_{c_2}, \#), h(N_{v_3}), \$))$, $CERT_V$

$S_{k_c}^f(E_{k_b}^p(\$, h(N_{c_1}, DESC), \#, N_{c_2}))$, $CERT_C$

5. B : Calcula $h(N_{c_2}, \#)$ y lo compara con $h(N_{c_2}, \#)$ enviado por V.

Compara $h(N_{c_1}, DESC)$ enviado por V con $h(N_{c_1}, DESC)$ enviado por C.

Compara $\$$ enviado por V con $\$$ enviado por C. Si coinciden B puede estar seguro de que tanto C como V están de acuerdo en los detalles de la transacción.

$$B \longrightarrow V : S_{k_b}^f(V, C, F, N_{v_1}, N_{v_2}, S/N, \$, h(N_{c_1}, DESC), h(N_{v_3}))$$

6. $V \longrightarrow C$: $S_{k_v}^f(N_{v_3})$, $S_{k_b}^f(V, C, F, N_{v_1}, N_{v_2}, S/N, \$, h(N_{c_1}, DESC))$

Fig. 4-2 Pasos del protocolo 3KP

4.2.2.2.1 Explicación y análisis de 3KP

1. *Envío inicial*

En el inicio del esquema, el consumidor C genera dos núnicos [Nc_1 y Nc_2]. Calcula el valor hash de su número de tarjeta [#] y del segundo de los núnicos generados [Nc_2], para evitar que se revele dicho número de tarjeta al vendedor V. Después de esto envía a V:

a) El primer núnico generado [Nc_1] el cual será utilizado posteriormente para evitar que B (el banco de V), conozca la descripción de los productos adquiridos,
b) Su identidad [C]
c) El valor hash recién calculado [$h(Nc_2, \#)$]
d) y su certificado [$CERT_C$]; iniciando así la transacción [7] (pp. 86,87).

2. *Procesamiento inicial y composición de la factura*

Cuando V recibe este mensaje inicial, genera tres núnicos [Nv1, Nv2 y Nv3], el primero de los cuales se asocia a la fecha en la que se realiza la transacción, con el fin de identificar de manera única a la orden de compra [F, Nv_1]. V entonces firma digitalmente el valor hash tanto de la descripción de los productos a negociar: [DESC] y del núnico (enviado por C para proteger esta descripción) [Nc_1], así como el valor hash del tercer núnico generado [Nv_3], y el monto de la transacción [$]. Entonces envía esta firma a C junto con:

a) Su identidad [V]
b) El identificador de la transacción [F, Nv_1]
c) El segundo núnico generado [Nv_2]
d) y su certificado [$CERT_V$]

Por los elementos que integran este segundo mensaje se equipara a una factura en el comercio tradicional [7] (pp. 88).

3. *Procesamiento de la factura*

Una vez que C recibe este mensaje o "factura", calcula el valor hash de la orden de compra y el núnico asociado a esta, que envió a V en el intercambio inicial [$h(Nc_1$, DESC)]. Compara este valor con el enviado por V; si coinciden se confirma que tanto él como V están de acuerdo con los detalles de la orden de compra. Después de esta verificación, C envía a V:

a) La identidad de V [V]
b) El identificador de la transacción [F, Nv_1]
c) El segundo núnico enviado por V en el paso número 2 [Nv_2]
d) y la firma de C sobre el texto cifrado (con la llave pública de B) de las instrucciones de pago. Estas instrucciones incluyen:

    1. El monto de la transacción [$]
    2. El valor hash de la descripción de los bienes por adquirir y de su núnico asociado [$h(Nc_1$, DESC)]
    3. El número de tarjeta de C [#]

4. y el núnico con el que protegió este número en el inicio de la transacción [Nc_2]; estos dos últimos elementos servirán para que B pueda verificar que el número de tarjeta de este mensaje coincida con el enviado a V en el paso 1 [7] (pp.88).

4. *Procesamiento de instrucciones de pago y generación de la solicitud de autorización de pago*

Si por alguna razón V decide no seguir adelante con la transacción, debe enviar en este momento un mensaje de cancelación a C. De lo contrario procede a verificar la firma de C sobre las instrucciones de pago descifrándolas con la llave pública de C obtenida de su certificado. Si la verificación es exitosa, genera entonces una solicitud de autorización de pago. Esta solicitud esta integrada por:

a) Su identidad [V]
b) El identificador de la transacción [F, Nv_1]
c) El segundo núnico que le envió a C en el paso 2 [Nv_2]
d) La firma de V sobre: el valor hash de la descripción de los bienes que integran el pedido y el núnico para proteger dicha descripción [h(Nc_1, DESC)], el valor hash del número de tarjeta y el núnico para proteger dicho número [h(Nc_2, #)] (valor hash que le fue enviado por C en el paso 1); el valor hash del tercer núnico enviado a C en el paso 2 [h(Nv_3)], y el monto de la transacción [$]
e) El certificado de V [$CERT_V$]
f) Las instrucciones de pago tal cual las recibió de C en el paso 3
g) y por ultimo el certificado de C [$CERT_C$] [7] (pp.88-89).

5. *Procesamiento de la solicitud de autorización del pago*

Cuando B recibe los elementos del mensaje anterior, verifica la firma de C en las instrucciones de pago y la firma de V en la solicitud. Posteriormente descrifra las instrucciones de pago con su llave privada; calcula entonces el valor hash del número de tarjeta de C y del núnico que lo protege: h(Nc_2, #), y compara este valor con el que recibió firmado por V. Compara además tanto el valor hash de la descripción de los bienes a negociar y el núnico que la protege: h(Nc_1, DESC), así como el monto de la transacción enviados por C en las instrucciones de pago, contra los que recibe firmados por V en la solicitud de pago: $. Si estas verificaciones resultan exitosas, entonces B puede asumir que C y V están de acuerdo en los detalles de la transacción, sin que el número de tarjeta de C haya sido revelado a V, ni los detalles del pedido a B. Entonces B debe comprobar la "frescura" del mensaje, verificando que la combinación del identificador de la transacción y el segundo núnico: F, Nv_1, enviado por V a C en el paso 2, no haya sido utilizada en transacciones anteriores, evitando de este modo ataques por reflexión. Es en este momento que B debe comunicarse con el banco de C, a través de las redes financieras privadas, para que éste le informe si el número de tarjeta de C es válido y si cuenta con los fondos o el crédito suficiente como para saldar la transacción; si esto se cumple la transferencia de fondos se efectúa de manera inmediata.

Una vez que B ha recibido una respuesta afirmativa o negativa del banco de C, debe enviar a V una respuesta a la solicitud de autorización de pago. Esta respuesta la integran:

a) Las identidades tanto de C como de V [C y V]
b) El identificador de la transacción [F, Nv_1]
c) El segundo núnico enviado por V a C en el paso 2 [Nv_2]
d) La respuesta que recibió B del banco de C [S/N]
e) El monto de la transacción [$]
f) El valor hash de la descripción del pedido y el núnico que la protege: [$h(Nc_1$, DESC)]
g) y finalmente el valor hash del tercer núnico enviado por V a C en el paso 2: [$h(Nv_3)$]

Esta respuesta es firmada por B y enviada a V. [7] (pp.89).

6. *Respuesta de factibilidad de pago*

Como último paso V verifica la firma de B en la respuesta a la solicitud de autorización y envía a C:

a) Su firma sobre el tercer núnico que envió a C en el paso 2 [N_{V3}]
b) y la respuesta de B tal cual la recibió

De esta manera cuando C reciba éste ultimo mensaje podrá verificar la firma de B en esta respuesta, y la firma de V sobre el tercer núnico cuyo valor hash le fue enviado por V en el paso 2, pudiendo entonces calcular el valor hash de este tercer núnico y compararlo contra el recibido; si coinciden contará con la firma de V en este tercer núnico, lo que actúa como un recibo que le asegura que V ha recibido y aceptado el pago, considerando así concluida la transacción, restándole únicamente esperar la entrega de los productos adquiridos [7] (pp.89-90, 92-93).

4.2.3 SEPP ("Secure Electrónic Payment Protocol")

Fue desarrollado por MasterCard[3] en octubre de 1995 para procesar pagos electrónicos de forma segura usando tarjetas de crédito sobre redes públicas. SEPP está basado en 3KP por lo que conserva muchas de las características de este último, incluyendo a las entidades participantes, pero considerando una entidad más: un sistema administrador de certificados. Utiliza criptografía de llave pública para asegurar que el contenido de los mensajes no sea alterado durante su transmisión del emisor al receptor. Como un elemento extra para la definición del protocolo de pago electrónico, define el antes mencionado

[3] MasterCard es una de las instituciones de banca múltiple más importantes hoy en día. Inicio operaciones en 1940 y actualmente cuanta con 30 oficinas alrededor de todo el mundo

sistema de administración de certificados llamado CMS ("Certificate Managmente System") [7] (pp. 93).

4.2.3.1 Características principales de SEPP

SEPP permite, por un lado, que el vendedor sea capaz de verificar que un comprador esté usando un número de cuenta válido; y por el otro, permite prevenir fraudes perpetrados por atacantes que intenten hacerse pasar por vendedores legítimos para obtener datos de tarjetas de los compradores. Dentro de las características principales de SEPP, se incluye el hecho de que el banco del vendedor se relaciona con el vendedor por medio de un Sistema de Gestión de Pagos, el cual funge como enlace entre el vendedor y su banco para la gestión de servicios de autorización de pago y del pago mismo. Como un elemento extra para la definición del protocolo de pago electrónico, SEPP define un sistema de administración de certificados [7] (pp.93), el cual se describe a continuación.

4.2.3.2 CMS ("Certificate Managment System")

El CMS consiste de una o más autoridades certificadoras que proporcionan tanto a vendedores como a bancos de vendedores y compradores, servicios de emisión y distribución de certificados de llave pública a través del web.

El CMS se implementa como una jerarquía de servidores, cada uno con su propio soporte criptográfico. Algunos hechos importantes de los certificados en este contexto son:

1. El certificado de un comprador relaciona su llave pública a un número de tarjeta específico, asegurándole de esta manera al vendedor que está recibiendo un número de tarjeta legítimo en una transacción particular. Con el fin de proteger la confidencialidad del comprador, el valor hash del número de tarjeta de éste es incluido en el certificado de su llave pública; de esta manera, cuando el comprador envía a B su número de tarjeta y un núnico que lo protege, B posee los suficientes elementos como para verificar el valor hash del número de tarjeta que contiene el certificado del comprador.

2. El certificado del vendedor le garantiza al comprador que es un comerciante legítimo registrado ante MasterCard, gracias a que también está relacionado con el número de cuenta del vendedor administrada por MasterCard.

3. La llave pública contenida dentro del certificado del banco del vendedor es utilizada por el comprador para cifrar las instrucciones de pago, en las que se incluye el número de tarjeta [7] (pp.95-96).

La parte pública de los pares de llaves que posee cada entidad que participa en SEEP está certificada por el CMS. El número y uso de estos pares de llaves es descrito a continuación.

4.2.3.3 Llaves utilizadas en SEPP

Llaves del comprador

El comprador necesita un par de llaves para generar firmas digitales durante el pago de la transacción. La llave privada es almacenada en el disco de alguna máquina local, idealmente desconectada de cualquier otra máquina. Dicha llave debe estar cifrada por un password que debe ser conocido únicamente por el comprador. Este par de llaves es generado localmente por un dispositivo o software criptográfico.

Llaves del vendedor

El vendedor puede poseer uno o dos pares de llaves. Uno de ellos se utiliza para generar firmas digitales, el otro es opcional y se usa para cifrar información relacionada al pago enviada por el banco del vendedor a este ultimo.

Llaves del banco del vendedor

Para esta entidad se requieren tres pares de llaves. El primer par se usa para firmar digitalmente recibos proporcionados al comprador y vendedor. El segundo se usa para cifrar y descifrar datos del pago del comprador. Finalmente el tercer par se utiliza para firmar solicitudes de renovación de certificados enviados al CMS [7] (pp. 96)

4.2.3.4 Protocolo SEPP

El protocolo para SEPP es, en esencia, el mismo que 3KP, razón por la cual debe tomarse como referencia el protocolo mostrado en la figura 4-2 de la sección 4.2.2. Sin embargo por cuestiones de sencillez y claridad en este protocolo no se contempla al CMS, que como se ha mencionado es el elemento adicional que presenta SEPP con respecto a 3KP. A pesar de lo anterior no se debe olvidar que dentro de SEPP se contempla la posible existencia del CMS, lo que implica una serie de relaciones y de flujos de información no contemplados en la figura mencionada.

4.2.4 SET ("Secure Electrónic Transaction")

El lanzamiento de SEPP por parte de una asociación entre MasterCard, Netscape[4], IBM[5] y otras entidades más, en octubre de 1995, difirió en sólo unos cuantos días del lanzamiento de STT ("Secure Transaction Technology"), otro esquema distinto de CE

[4] Compañía desarrolladora de software orientado al web cuyo producto más famoso es el navegador para múltiples plataformas del mismo nombre

[5] IBM ("International Bussines Machine") es una compañía desarrolladora de hardware y software fundada en 1911. Actualmente es una de las empresas más robustas y de mayor renombre a nivel mundial.

basado en tarjetas de crédito, por parte de VISA[6] y Microsoft[7]. Esta coincidencia condujo a una desafortunada situación en la que las dos asociaciones principales de tarjetas de crédito a nivel mundial respaldaban diferentes soluciones para CE.

Por algunos meses ambos esfuerzos se realizaron en paralelo, cada uno desarrollando de manera separada referencias de implementación; de hecho se realizaron esfuerzos para desarrollar esquemas que permitieran trabajar con ambas propuestas. Afortunadamente el sentido común prevaleció, y en enero de 1996 tanto VISA como MasterCard anunciaron que trabajarían de manera conjunta para desarrollar un sistema unificado que sería llamado SET.

SET pretende preparar el camino para realizar transacciones sobre Internet de forma segura, rápida y sencilla. Concentra sus esfuerzos en lograr el intercambio seguro de números de tarjeta entre el comprador y un sistema de gestión de pagos. Por sus características técnicas y de origen, se espera que se convierta en el método estándar para efectuar pagos electrónicos en Internet [7] (pp. 101-102).

4.2.4.1 Características principales de SET

Entre las características principales de SET se incluye el hecho de que está basado en una infraestructura de certificado de llave pública, siendo importante señalar que no es de propósito general, ya que fue diseñado específicamente para utilizar tarjetas de crédito como medio de pago. En cuanto a los participantes, en SET se incluyen: un comprador, un vendedor, un banco del comprador, un banco del vendedor y un sistema de gestión de pagos (frecuentemente manejado por el banco del vendedor); y aunque son las cuatro entidades iniciales las que participan de forma directa también se considera la posible participación de una autoridad certificadora y una red financiera. Además SET utiliza RSA para firmas digitales e intercambio de llaves, diversos algoritmos de llave secreta tales como: el modo CBC de DES y CDMF para cifrado de información; además de SHA como función hash. Adicionalmente SET introduce el concepto de firma dual (técnica descrita en el capítulo 1 de esta tesis en la sección 1.5.3), por medio de la cual el comprador puede relacionar la información de la orden de compra enviada al vendedor con las instrucciones de pago enviadas al sistema de gestión de pagos, sin que ni el vendedor, ni el sistema de gestión de pagos tengan acceso a la información del otro. Con relación a las firmas duales, estas permiten que se firme un sólo mensaje en lugar de dos (como en SEPP), lo que le confiere a SET un rango de eficiencia considerablemente mayor [7] (pp.101-106).

4.2.4.2 Protocolo SET

A continuación se describe de manera detallada el protocolo de SET.

[6] VISA es una institución de banca múltiples cuyas tarjetas de crédito son actualmente aceptadas en 300 países, lo que la convierte en la institución líder de tarjetas de crédito.

[7] Microsoft es una corporación dedicada principalmente al desarrollo de software para computadoras personales. Fue fundada en 1975 y actualmente es la compañía más exitosa de su ramo.

1 $C \longrightarrow V$: $B\ ,\ LST_{cert}\ ,\ N_{c_1}\ ,\ N_{c_2}$

1a $V \longrightarrow C$: $S_{k_v}^{f}(N_{c_1}, N_{v_1}, F, N_{c_2}, N_{v_2})\ ,\ CERT,\ CERT_b$

2 $C \longrightarrow V$: $N_{c_1}\ ,\ N_{v_1}\ ,\ B\ ,\ F\ ,\ N_{c_2}\ ,\ N_{v_2}\ ,\ N_{c_3}\ ,\ S_{k_c}^{f}(h(DIO)\oplus h(DIP), h(h(DIO), h(DIP)))\ ,\ CERT_C$
$E_{k_b}^{p_b}(N_{c_1}, N_{v_1}, \$, h(DESC, \$, N_{c_3}), E_{k_c}^{p_c}(\$, F, N_{c_4}, N_{c_5}), S_{k_c}^{f}(h(DIO)\oplus h(DIP), h(h(DIO), h(DIP))))$

3 $V \longrightarrow B$: $S_{k_v}^{f}(E_{k_b}^{p_b}(N_{c_1}, N_{v_1}, \$, h(DESC, \$, N_{c_3}), h(DIO), LST_{cert}, InfAdic,$
$E_{k_b}^{p_b}(N_{c_1}, N_{v_1}, \$, h(DESC, \$, N_{c_3}), E_{k_c}^{p_c}(\$, F, N_{c_4}, N_{c_5}), S_{k_c}^{f}(h(DIO)\oplus h(DIP), h(h(DIO), h(DIP)))))$

3a $B \longrightarrow V$: $E_{k_v}^{p_v}(S_{k_b}^{f}(N_{c_1}, N_{v_1}, F, \$, S/N, S_{k_b}^{f}(E_{k_b}^{p_b}(\$, D_{cap}, N_{b_1}))))$

4 $V \longrightarrow B$: $S_{k_v}^{f}(E_{k_b}^{p_b}(N_{c_1}, N_{v_1}, F, \$, N_{c_4}), S_{k_b}^{f}(E_{k_b}^{p_b}(\$, D_{cap}, N_{b_1})))$

4a $B \longrightarrow V$: $S_{k_b}^{f}(E_{k_v}^{p_v}(N_{c_1}, N_{v_1}, \$, N_{c_4}, S/N))$

5 $C \longrightarrow V$: $S_{k_c}^{f}(N_{c_1}, N_{v_1}, N_{c_5})$

5a $V \longrightarrow C$: $S_{k_v}^{f}(N_{c_1}, N_{v_1}, N_{c_5}, estatus, A/C)$

Fig. 4-3 Pasos del protocolo SET

4.2.4.2.1 Explicación y análisis de SET

El protocolo de SET consiste en pares de mensajes solicitud/respuesta o *Req/Res*. Para permitir la interoperabilidad, dichos mensajes están definidos en un formato independiente de la máquina, lo que permite que la aplicación del comprador pueda trabajar con la del servidor a pesar de que cada una haya sido desarrollada por compañías de

software diferentes. En esta sección se presentan los pares de mensajes requeridos para efectuar una transacción por medio de SET

1. *Mensaje Inicial (PInitReq)*

C envía el mensaje inicial a V indicándole que está listo para la gestión del pago de la transacción. Este mensaje contiene los siguientes elementos:

a) La identificación del banco emisor de la tarjeta con la que se pretende pagar los bienes, pudiendo ser: BANAMEX, BANCOMER, VISA, etc. [B]

b) Un primer núnico que funciona como un identificador local de la transacción [N_{C1}]

c) Un segundo núnico que será utilizado por V en su respuesta a este mensaje inicial para garantizar la frescura de la comunicación [N_{C2}]

d) De manera opcional también puede incluirse una lista de "sellos" de certificados conocidos por el software de C [LST_{cert}] [7] (pp.107-108).

1a. Respuesta al mensaje inicial (PinitRes)

Una vez recibidos los elementos anteriores, V genera un primer núnico: N_{V1} que funcionará como identificador global de la transacción y que combinado con el identificador local, enviado por C, funcionará en adelante como el identificador formal de la transacción, identificando por lo tanto a la misma de manera única con respecto a otras transacciones. Como respuesta V envía:

a) El identificador global de la transacción [N_{C1}, N_{V1}]
b) La fecha en la que se efectúa la transacción [F]
c) Un segundo núnico generado por V [N_{V2}]
d) El segundo de los núnicos enviados por C para asegurar la frescura de la comunicación [N_{C2}]; todo lo anterior firmado con la llave privada de V
e) Además V envía el certificado de B y el suyo propio [$CERT_b$ y $CERT_V$] de tal manera que cuando C recibe estos elementos de manera correcta puede confiar en que V es un comerciante legítimo [7] (pp.107-108).

2. Orden de Compra (PReq/Pres)

En este mensaje, que es el más complejo dentro de SET, C envía a V los siguientes tres elementos:

a) La Información de la Orden o IO
b) Las Instrucciones de Pago o IP
c) y el certificado de C para que V pueda verificar la firma dual.

Debido a la complejidad de la estructura tanto de la IO como de las IP y para efectos de claridad, a continuación se describe de forma independiente la conformación de ambas.

La IO consiste de datos relacionados a la descripción de la misma, de tal manera que V pueda identificarla, estos elementos son una firma dual y los Datos de la Información de la Orden o DIO. Estos últimos se conforman como sigue:

a) El identificador de la transacción [N_{C1}, N_{V1}]
b) El identificador del banco de C o banco emisor [B]
c) La fecha enviada en el intercambio inicial [F]
f) El segundo núnico enviado por C a V en el paso 1 [N_{C2}]
g) El segundo núnico enviado por V, demostrando la frescura del mensaje [N_{V2}]
h) Un tercer núnico (por parte de C) [N_{C3}], que será utilizado más adelante en el momento de calcular el valor hash de la descripción de la orden con el fin de evitar ataques por diccionario a dicha descripción

En cuanto a la firma dual, cuando C cuenta con los DIO genera dicha firma dual (ver la sección 1.5.3 para el concepto de firma dual) usando los valores hash de los DIO: h(DIO) y los DIP: h(DIP). La conformación de los DIP será descrita más adelante. Esta firma relaciona a los DIO con los DIP, asociando de esta manera el pedido de C con las instrucciones de pago, demostrando que fueron firmadas al mismo tiempo. En este sentido cualquier entidad que posea ya sea los DIO o a los DIP y la firma dual mencionada, puede verificar dicha firma sin tener que conocer los DIO o los DIP según sea el caso. Además la firma dual ofrece un aspecto de optimización ya que se realiza una sola firma para los DIO y los DIP, en lugar de dos: una especifica para la IO y una para las IP. De esta manera la firma dual junto con los DIO conforman la IO.

Por su parte las IP son conformadas de la siguiente manera:

Inicialmente se forman los Datos de las Instrucciones de Pago o DIP que incluyen:
a) El identificador de la transacción [N_{C1}, N_{V1}]
b) El monto de la transacción [$]
c) El valor hash de la descripción de la orden, el monto de la transacción y de un núnico (el tercero generado por C) utilizado para proteger dicha descripción contra ataques por diccionario y que también está incluido en los DIO [$h(_{DESC},\$,N_{C3})$]
d) El cifrado con la llave pública de B, del número de la tarjeta con la que C pretende liquidar la transacción [#], la fecha de vencimiento de dicha tarjeta: [F_2], y de dos núnicos (el cuarto y quinto generados por C): [N_{C4} y N_{C5}] para proteger el número de tarjeta de C contra ataques por diccionario y reflexión. Este cifrado RSA brinda una protección extrafuerte en comparación con la protección brindada por algoritmos de cifrado de llave secreta.

Una vez conformados los DIP, se agrega la misma firma dual creada para la IO completándose así la construcción de las IP, las cuales son cifradas con la llave pública de B para evitar que V conozca su contenido y son enviadas a éste último. Tanto la IO como las IP representan las bases de SET y una vez que C las envía a V,

está demostrando su deseo de pagar la transacción, por lo que a partir de ese momento resultaría complicado si C deseara revertir el pago. Es importante remarcar que V no puede obtener acceso al contenido de las IP, por lo que éste simplemente las recibe y las envía a B.

Cuando V recibe la orden de compra, obtiene la IO por medio de verificar la firma de C, descifrándola con la llave pública de éste último, llave obtenida de su certificado. Después de esto V es capaz de verificar la firma dual de la IO utilizando de nuevo el certificado de C para tal fin.

Antes de enviar una respuesta a C, V normalmente solicita el pago de la transacción por medio de B, sin embargo es posible que V envíe en esta etapa una respuesta a C sin haber solicitado previamente el pago; indicando en estos casos a C que debe consultar posteriormente el estado de la transacción. En el caso en que en esta etapa V envíe una respuesta a C, ésta contendrá:

a) El identificador de la transacción [N_{C1}, N_{V1}]
b) El estado de la transacción [estatus]
c) Cualquier código de resultado existente. Estos códigos indican si las etapas de transferencia de fondos y autorización, descritos más adelante, se han completado [A/C]
d) Además, V debe incluir un resultado de la transacción, el cual contiene la autorización o los códigos de transferencia de fondos en el caso en que estas etapas ya se hayan desempeñado [S/N]. Estos códigos, son generados en el contexto financiero para autorizar y efectuar la transferencia de fondos, cuyos efectos serán dados a conocer a C en su estado de cuenta. Este paso es presentado como el número 5ª en la figura 4-3. De este modo cuando C recibe esta respuesta tiene conocimiento de si el pago se ha efectuado o de si la transacción está en espera para ser procesada dentro de la infraestructura de las redes financieras [7] (pp.108-112).

3. Autorización (Authreq)

Este par de mensajes permite a V verificar que C cuenta con crédito para liquidar la compra o contratación, y obtener de este modo la autorización para que B abone los fondos correspondientes a su cuenta.

En la solicitud de autorización, V envía datos firmados y cifrados acerca de la compra; además en esta etapa V envía a B las IP enviadas por C. Esta solicitud incluye:

a) El identificador de la transacción [N_{C1}, N_{V1}]
b) La fecha de la transacción [F]
c) La cantidad que se solicita sea autorizada [$]
d) El valor hash de los detalles de la orden, protegido por el núnico correspondiente. Este valor hash será comparado por B contra el valor hash enviado por C a través de V. Si coinciden podrá estar seguro de que C y V han acordado la orden de compra y el monto de la misma [$h(_{DESC},\$, N_{C3})$]
e) El valor hash de los DIO. el cual muestra el conocimiento de V sobre los DIO que es firmado dualmente, mostrando el acuerdo en la orden sin revelarla a B [h(DIO)]

f) Una serie de sellos de algunos certificados relevantes que V posee para evitar que B los envíe en la respuesta [LST_{cert}]
g) Algunos otros datos como el domicilio de C (obtenido fuera de SET) [InfAdic]
h) Y otros detalles de V tales como su tipo de empresa [InfAdic].
i) Finalmente las IP enviadas por C; todo lo anterior firmado por V y cifrado con la llave pública de B.

Tanto la gestión de la autorización como de la transferencia de fondos pueden efectuarse como un solo mensaje, conocido como una transacción de venta o "*sales transactions*", en cuyo caso V debe indicarle a B que desea utilizar este esquema [7] (pp.113-114).

3a Respuesta de autorización de pago (AuthRes)

Una vez que B recibe lo anterior, descifra las partes del mensaje, verifica las firmas y compara el valor hash de los detalles del pedido enviados por V y el obtenido de las IP. Checa además el monto enviado por V contra el obtenido de las IP, si son diferentes, B debe validar que la diferencia caiga en el rango permitido por sus políticas. Después de esto B debe gestionar el pago de la transacción por medio de las redes financieras. Una vez que B ha recibido una autorización positiva del banco de C, envía a V una respuesta que incluye:

a) El identificador de la transacción [N_{CI}, N_{VI}]
b) La fecha de la transacción [F]
c) La cantidad autorizada, la cual debe corresponder con el monto de la transacción [$]
d) Un código de autorización del banco de C [S/N]
e) Además incluye datos de la transferencia que serán utilizados más adelante para que V solicite la transferencia de fondos, estos datos están firmados y cifrados con la llave pública de B y son conocidos como *bloque de pago*. Este bloque incluye:

   a) La cantidad autorizada [$]
   b) Algunos datos de la transferencia (uso exclusivo de B) [D_{cap}]
   c) Un núnico que identifica al bloque de pago de forma única [N_{bl}]

Si la transferencia se realizó junto con la autorización (sales transactions), entonces un código de transferencia es enviado en lugar del bloque de pago. En esta circunstancia, si B recibe una autorización positiva, puede enviar a C los bienes contratados. Una autorización positiva indica que el banco de C ha verificado los detalles de la tarjeta y el límite de crédito o los fondos disponibles en la cuenta de B, dando así luz verde para el pago de la transacción [7] (pp.113-114).

4.Transferencia de fondos (CapReq)

Después de procesar una orden, V requiere solicitar que el pago previamente autorizado le sea transferido a su cuenta. El pago total por varias autorizaciones puede ser solicitado

en un único mensaje; en estos casos V debe acumular varios bloques de pago durante el día y al final del mismo solicitar el pago de todos ellos.

El contenido de este mensaje incluye:

a) El identificador de la transacción [N_{C1}, N_{V1}]
b) La fecha de la transacción [F]
c) El monto de la transacción autorizado [$]
d) Un núnico (el cuarto generado por V) [N_{V4}] que sirve como identificador de la transferencia. Todo lo anterior cifrado con la llave pública de B.
e) Además V envía los bloques de pago que recibió precisamente de B. Todo lo anterior firmado por V.

Como ya se mencionó V puede incluir varios bloques de pago de diferentes transacciones en una misma solicitud de pago para fines de eficiencia. Para cada bloque de pago debe incluirse la cantidad autorizada y el identificador de la misma. Estos datos deben coincidir con los que están cifrados y firmados dentro de los bloques de pago enviados por B [7] (pp.114-116).

4ª *Respuesta a la solicitud de pago (CapRes)*

Una vez que B recibe esta solicitud, debe verificar la firma de V, y todos los datos de la solicitud, para posteriormente abonar la cantidad especificada en la cuenta de V, restando a dicha cantidad los cargos por transacción que cobra B. Hecho esto B envía la respuesta a la solicitud de captura que incluye:

a) El identificador de la transacción [N_{C1},N_{V1}]
b) El monto transferido [$]
c) El identificador de la transferencia [N_{C4}]
d) y una indicación de éxito o fracaso enviado por el banco de C [S/N]

Después de una transferencia exitosa, V ha recibido el pago correspondiente a la compra de C. En el caso en que V no haya enviado aún la respuesta de compra a C, debe hacerlo ahora [7] (pp.114-116).

5. Consulta del cliente (InqReq)

Este par de mensajes permite que C verifique el estado de la transacción. Esta consulta puede ser enviada en cualquier momento después de la solicitud de compra, pudiendo consultar únicamente el estado correspondiente a sus propias compras. Esta consulta puede efectuarse múltiples veces durante una misma transacción. El mensaje de la consulta contiene:

a) El identificador de la transacción [N_{C1}, N_{V1}]

b) Un nuevo núnico (el quinto generado por C) [N_{C5}], el cual debe ser único para cada consulta, debido a que se pueden realizar consultas en múltiples ocasiones. Además las consultas deben ir firmadas por C para probar que vienen del comprador correcto [7] (pp.116).

5ª *Respuesta de estado de la transacción (InqRes)*

Finalmente la respuesta a la consulta contiene:

a) El identificador de la transacción [N_{C1}, N_{V1}]
b) El núnico asociado a cada consulta en particular [N_{C5}],
c) El estado de la transacción [estatus]
d) y cualquier código de resultado (autorización o transferencia) [A/C]

Una vez que C ha recibido este mensaje puede estar seguro de que una compra en particular está siendo procesada, restándole solamente esperar a que les sean entregados los productos adquiridos [7] (pp.116).

4.3 Comentario acerca de estos esquemas

Con base en la anterior descripción de SSL, 3KP, SEPP y SET, se puede puntualizar lo siguiente:

SSL es el único de los esquemas descritos que de origen tiene un diseño de propósito general, pero gracias a sus características es ampliamente utilizado en muchos países de todo el mundo, incluido México, sobre todo para transacciones que involucran montos moderados (entre uno y 100 dólares) e información confidencialidad. En la situación contraria se encuentran 3KP, SEPP y SET cuyo diseño y desarrollo fue enfocado desde un inicio para permitir el pago utilizando tarjetas de crédito, aunque en el caso específico de SEPP éste puede adecuarse para la gestión de cobro de cheques electrónicos. Esta situación provoca que estos tres últimos esquemas proporcionen niveles de seguridad muy por encima de SSL puesto que en su diseño se tomaron en cuenta escenarios y variables específicas para la adecuada protección de los datos involucrados en las tracciones como por ejemplo el número de tarjeta del comprador.
El hecho de que SSL sea el único de los esquemas descritos de propósito general establece una clara diferencia con respecto de 3KP, SEPP y SET; esta diferencia se refleja en muchos y muy variados aspectos, los cuales serán mencionados con mayor detalle en el análisis comparativo del capítulo siguiente. Sin embargo, adelantando un poco se puede establecer sin entrar todavía a un análisis profundo, que todos los esquemas descritos en este capítulo, exceptuando a SSL cubren exclusivamente el pago de la transacción por medio de tarjetas de crédito, razón por la cual una serie de esquemas adicionales que soporten la selección de productos y servicios, la negociación del precio, la selección del tipo de pago y la entrega de información deben ser incorporados, de tal manera que se cuente con una aplicación

completa de CE. De igual forma se deben de proporcionar interfaces gráficas de fácil configuración, de tal manera que las fases de la transacción sean transparentes para el usuario.

Ahora bien, si se confronta a 3KP contra SEPP, sin olvidar que el segundo se basa en el primero, se puede observar que las diferencia principal radica en la definición del CMS por parte de SEPP, agregando de este modo una entidad más, pero ganando en la formalización de una jerarquía de confianza tan necesaria en el contexto de transacciones de CE. Finalmente en lo concerniente a SET, este se muestra con un número elevado de mensajes, y entidades involucradas; además del uso de diversas técnicas como las firmas duales con las que va un paso adelante en cuanto a robustez y seguridad. La utilización de este tipo de técnicas distingue claramente a SET de los otros tres esquemas descritos, sin olvidar que SEPP fue tomado como una de las bases de su desarrollo.

Por último, en el apartado de los servicios de seguridad que cada esquema proporciona, SSL es el que se muestra en mayor medida limitado a este respecto al proporcionar solamente confidencialidad de las comunicaciones entre el comprador y el comerciante, autenticación de las entidades involucradas e integridad de los mensajes de la transacción. En este sentido y como ya se mencionó 3KP, SEPP y SET muestran un mayor nivel de seguridad proporcionando además de los servicios ofrecidos por SSL, la autenticación y no-repudio de los mensajes así como anonimato en el caso particular de 3KP y SEPP.

En este capítulo se han revisado a detalle los esquemas de CE: SSL, 3KP, SEPP y SET, describiendo a detalle sus protocolos respectivos; en el siguiente capítulo estos esquemas se analizan comparativamente.

Capítulo 5

ANÁLISIS COMPARATIVO

En este capítulo se hace un análisis comparativo entre los esquemas de CE: SSL, 3KP, SEPP y SET, descritos en el capítulo anterior. Los elementos de comparación van desde los más generales como el número de entidades involucradas, hasta los específicos como el tamaño de llave del algoritmo de cifrado utilizado o el número de operaciones de cifrado efectuadas. Tales elementos intentan brindar un panorama general de la seguridad que ofrece cada esquema, así como de los requerimientos necesarios para brindar dicha seguridad, con respecto a los demás esquemas analizados. Para tal fin se ha dividido el análisis en niveles, los cuales a su vez agrupan una serie de parámetros de comparación relacionados entre sí. Muchos de estos parámetros fueron seleccionados debido a que proporcionan información acerca de los costos técnicos y recursos de cómputos utilizados que se asocian a los cálculos efectuados; por ejemplo, generación de llaves, firmas digitales, valores hash, núnicos, etc., así como a los costos que cada esquema involucra en términos financieros, ya sea por la compra, administración, mantenimiento de equipo y software o por la infraestructura de telecomunicaciones requerida, entre otras razones. Además se considera para el análisis el rango de montos que involucra una transacción en particular. A este respecto frecuentemente se considera que una transacción involucra montos reducidos o moderados cuando se trate desde uno hasta 100 dólares, de montos intermedios cuando se trata de más de 100 y hasta 1000 dólares, y finalmente de montos altos para las transacciones que involucren más de 1000 dólares.

Los niveles de análisis que comprende éste trabajo son los siguientes:

5.1 Parámetros del nivel de comparación 1

Este nivel de análisis agrupa parámetros que proporcionan información con respecto a la seguridad de cada esquema, siendo estos los siguientes.

5.1.1 Entidades participantes

El número y la forma en que participa cada una de las entidades involucradas, es un factor determinante en el desempeño de los esquemas de CE. Mientras mayor sea el número de entidades participantes mayor será la complejidad que implique, debido

entre otras cosas a la administración de llaves, los mensajes, los recursos, etc.; además, los costos que implica el funcionamiento del esquema también serán mayores.

A pesar de lo anterior el número elevado de entidades también puede representar un aspecto de seguridad ya que dentro de estas pueden encontrarse entidades como autoridades certificadoras o sistemas de gestión de pagos que robustecen el nivel de seguridad brindados.

Con relación a los costos que implique la operación de cada uno de los esquemas, estos pueden verse incrementados con un número elevado de entidades debido a los recursos que estas necesitan para funcionar.

Finalmente en cuanto al desempeño, un número elevado de entidades puede, en ocasiones, conferir desempeños menos eficientes con relación de aquellos esquemas donde participan un número reducido de ellas; pero proporcionando por otro lado un mayor nivel de seguridad en la mayoría de los casos.

5.1.2 Entidades que se autentican durante el protocolo

En el contexto de los esquemas de CE, la posibilidad de que cada entidad participante pueda tener la certeza de que está tratando con quien realmente desea tratar, a pesar de que no exista un trato "cara a cara", es uno de los fundamentos de la seguridad durante una transacción, razón por la cual mientras mayor sea el número de entidades participantes que se autentiquen mayor será el nivel de seguridad que proporcione cada esquema.

5.1.3 Algoritmos de cifrado que utiliza o soporta cada esquema

Los diferentes algoritmos de cifrados ofrecen diversos niveles de seguridad. Sin embargo, como se explicó en el capítulo 1, la mayoría de las veces la seguridad de un algoritmo de cifrado radica en la longitud de la llave que utiliza. A pesar de esta característica, la seguridad de un esquema de CE dependerá parcialmente del diseño del algoritmo o de los algoritmos de cifrado utilizados puesto que, además, influye la capacidad de cómputo con que cuente un atacante para tratar de romper un cifrado, entre otros aspectos.

Con respecto a lo anterior, organismos reguladores tales como: la Oficina Nacional de Estándares, el NIST y el CCITT después de serios análisis y evaluaciones han establecido como estándares a ciertos esquemas de cifrado tales como: el DES, el RSA, el SHA, entre otros; debido a sus características y niveles de seguridad. Algunos de los esquemas analizados hacen uso de varios de estos estándares.

5.1.4 Tamaños de llaves utilizadas

Como se ha mencionado, la longitud de una llave define en gran medida la seguridad de un algoritmo de cifrado. Dentro del contexto de CE en el que participan autoridades

certificadoras, la longitud que utilizan estas llaves debe ser considerablemente mayor a las que utilicen las demás entidades participantes, ya que su función así lo requiere.

Sin embargo, no se debe perder de vista que el hecho de generar llaves, sobre todo para cifrado de llave pública, lleva asociados costos de procesamiento por los múltiples cálculos matemáticos que estos implican.

Otro aspecto a considerar con respecto al tamaño de las llaves es que por políticas de ciertos países, esencialmente EUA, está prohibida la exportación de aplicaciones que efectúen cifrado y que utilicen llaves de longitud generalmente mayor a 40 bytes, razón por la cual el acceso a las aplicaciones que hacen uso de llaves por arriba de dicha longitud está limitada en gran medida.

Por todo esto, el tamaño de las llaves es uno de los puntos clave dentro de un esquema de CE, aspecto que debe de tenerse muy en cuenta cuando se piensa en la seguridad que brinda y el desempeño que muestra un esquema en particular.

5.1.5 Número total de llaves requeridas

La generación de las llaves utilizadas representa costos de procesamiento, y por lo tanto de recursos de cómputo. En promedio la generación de llaves para cifrado de llave secreta es 100 veces menos costoso que la generación para cifrado de llave pública [2](pp. 162). Sin embargo, éste último tipo de cifrado proporciona servicios que el cifrado de llave secreta no otorga, tales como firmas digitales y distribución de llaves.

A este respecto deben contemplarse además los costos adicionales asociados a la emisión de certificados para las llaves públicas que así lo requieran, a causa de la intervención de las autoridades certificadoras.

Es por lo anterior, entre otras razones, que cuando se analiza un esquema en particular debe de tenerse en consideración el número total de llaves que se utilizan durante el mismo.

5.2 Parámetros del nivel de comparación 2

Este nivel de análisis agrupa parámetros que proporcionan información acerca de los costos asociados a las operaciones que se realizan en cada uno de los esquemas, operaciones tales como cifrados, firmas digitales, generación de núnicos, entre otros. Estos parámetros son los siguientes:

5.2.1 Número de operaciones de cifrado de llave pública

Las operaciones de cifrado involucran costos de procesamiento que deben contemplarse para determinar el desempeño de los esquemas de CE. A pesar de lo versátil que resulta el cifrado de llave pública, llegando incluso a resolver algunas desventajas del cifrado de llave secreta tales como la necesidad de usar una llave distinta para cada entidad con la que quiera comunicarse y el hecho de que se requieren acordar, dichas llaves por medios seguros, su uso debe combinarse junto con el cifrado de llave secreta, como en el caso de los sobres digitales.

Como consecuencia de que frecuentemente el cifrado de llave pública está relacionado a la firma digital, con todas las ventajas que ello implica en este contexto, se requiere el uso de certificados, situación que eleva y extiende el origen de los costos de estos procesos a terceras partes como las AC.

5.2.2 Número de firmas digitales

Como se ha mencionado las firmas digitales trabajan bajo un esquema de cifrado de llave pública, cifrado que involucra cálculos que implican costos técnicos considerables. Esta técnica involucra además la existencia de una jerarquía de confianza para el respaldo de los certificados necesarios para su funcionamiento.

A pesar de lo anterior, en el contexto del CE, las firmas digitales son un elemento básico y de gran importancia para poder contar con autenticación de mensajes y por ende con el no-repudio de los mismos; hecho que permite el mismo nivel de compromiso, sino es que mayor, que se logra con el comercio convencional.

Es por lo anterior que las firmas digitales deben de contemplarse en el análisis de los esquemas de CE desde la perspectiva de los costos que implican las operaciones asociadas a las mismas, pero también desde el punto de vista de los comprobantes y los compromisos que generan y respaldan respectivamente, ya que a pesar de que mientras un mayor número de firmas significa un mayor número de operaciones, también significa mayor formalidad y respaldo de los mensajes intercambiados por parte de las entidades involucradas en la transacción.

5.2.3 Número de núnicos generados

Uno de los papeles principales de los núnicos en este contexto es el de proteger la información y la transacción misma contra ataques por diccionario y de reflexión, entre otros. Aunque en promedio la generación de números aleatorios no es costosa, muchos generadores de estos números se basan en cifrado; hecho que puede costar una o más operaciones de cifrado. A este respecto un punto importante a considerar al momento de analizar un esquema de CE en particular es el número de núnicos generados con relación a los supuestos costos del esquema [10] (pp.369-428).

5.2.4 Número total de mensajes intercambiados durante el protocolo

Una de las principales medidas de eficiencia de un protocolo lo constituyen el número de mensajes que involucra; además del número y complejidad de los elementos que conforman cada mensaje. En el contexto de CE, tanto el contenido como el número de dichos mensajes es de vital importancia sobre todo en aquellos que se intercambian los datos confidenciales del comprador.

En la mayoría de los esquemas se busca que el número de mensajes intercambiados sea el menor posible, sin embargo en este contexto, debido a la cantidad de entidades involucradas así como a la necesidad de mensajes específicos para cada una de las fases que integran la transacción, el número máximo de mensajes debe disponer de una tolerancia adecuada, donde frecuentemente se busca más que la velocidad, la seguridad.

5.3 Parámetros del nivel de comparación 3

Este nivel de análisis agrupa parámetros que proporcionan información general acerca de los esquemas analizados en la comparación, tomando en cuenta las ventajas y desventajas principales de cada esquema. Estos parámetros son:

5.3.1 Servicios de seguridad que proporciona cada esquema

Los servicios de seguridad que cada esquema analizado satisface es una de los aspectos vitales a considerar. Mientras mayor sea el número de estos requerimientos que cumpla un esquema mayor será el nivel de seguridad y de robustez del mismo.

Idealmente un esquema de CE debe cubrir el mayor número de requerimientos posibles, sin embargo esto dependerá del nivel de seguridad requerido. A este respecto mientras mayor sea el número de requerimientos proporcionados, mayores serán también los costos asociados. Cuando se habla de transacciones que involucren montos elevados de dinero, se debe de considerar como una necesidad el hecho de que el esquema a utilizar proporcione un nivel suficiente de seguridad aunque los costos asociados sean más que moderados; por el contrario si la cantidad de dinero involucrada es baja, los niveles de seguridad requeridos, y por ende los requerimientos satisfechos y los costos asociados suelen ser limitados.

5.3.2 Ataques que evita

Aunque como se explicó en el apartado 1.2.2 del capítulo 1 de este trabajo los posibles ataques a la seguridad de la información son muy variados, la naturaleza de este tipo de esquemas los convierte en víctimas potencialmente vulnerables a los ataques por diccionario o por reflexión. Los esquemas más robustos y seguros proporcionan

mecanismos para evitar este tipo de ataques; mecanismos que sin embargo requieren de un mantenimiento que involucra ciertos costos que deben de ser contemplados. Frecuentemente dichos costos, resultan menores con relación a aquellos que se originan al momento de sufrir y afrontar un ataque que pudiera llegar a causar serios daños. [11] (pp. 648-656).

5.3.3 Principales ventajas

Las principales ventajas que presenta cada uno de los esquemas, proporcionan un panorama general de los aspectos positivos que aporta un esquema en particular con respecto a los demás analizados. Estas ventajas pueden consistir tanto de elementos que brindan cierto aspecto de optimización, protección extra para los datos confidenciales, versatilidad del esquema para adaptarse a variaciones, así como en sencillez; entre otros aspectos más. Muchas de estas ventajas pueden ser decisivas al momento de elegir un esquema de CE en particular.

5.3.4 Principales desventajas

Las desventajas que presente cada uno de los esquemas pueden originarse ya sea por el diseño mismo del esquema e incluso de ciertas ventajas; así existen esquemas que presentan la sencillez como una de sus virtudes, pero sin embargo también ofrecen niveles bajos de seguridad y robustez. A este respecto estas ventajas deben de considerarse seriamente para poder evitar el uso de un esquema de CE que no cumpla con las necesidades requeridas.

5.4 Estudio comparativo

En los siguientes apartados se desarrolla el análisis comparativo entre los esquemas de CE: SSL, 3KP, SEPP y SET, tomando como referencia para esta comparación los parámetros anteriormente citados. Al inicio de cada apartado se proporciona una breve explicación de la razón o razones por las que dichos parámetros fueron seleccionados para ser incluido en el análisis, para continuar después con el análisis como tal. Finalmente, para mostrar un compendio de los resultados obtenidos de éste análisis se ha seleccionado el uso de tablas comparativas, al ser considerado uno de los métodos más eficaces para mostrar de una forma resumida, sencilla de interpretar y práctica, los resultados de éste tipo de análisis. Cada una de estas tablas muestra de manera condensada los resultados obtenidos en cada uno de los niveles de análisis, de tal forma que la tabla número 1 muestra los resultados del nivel 1 y así sucesivamente.

5.4.1 Nivel de comparación 1

5.4.1.1 Entidades participantes

En este apartado, se destaca que SSL contempla la participación formal de únicamente dos entidades: el comprador y el comerciante. De manera adicional también intervienen las autoridades certificadoras que hayan emitido el certificado del comprador y el vendedor, en el caso de que dichos certificados existan. A este respecto puede darse el caso de que los certificados de ambas entidades hayan sido emitidos por una misma autoridad certificadora, o de que cada uno haya sido emitido por una autoridad diferente, situación que aplica para cada uno de lo esquemas analizados.

En el caso de 3KP, SEPP y SET, el número de entidades participantes se incrementa debido principalmente al hecho de que en su diseño se contempló la participación de una institución financiera que administra la cuenta bancaria, propiedad del vendedor, en la que se depositarán los fondos recibidos por el cobro del monto de las transacciones.

Además las tres entidades participantes cuya presencia es común tanto en 3KP, SEPP y SET, en el caso específico de SEPP se contempla la participación opcional de una cuarta entidad que consiste en el sistema de administración de certificados o CMS, cuya función se explicó en la sección *4.2.3.2.* de este mismo capítulo.

Finalmente en el caso específico de SET, se puede observar que debido a lo robusto de su diseño involucra por un lado a un sistema de gestión de pagos (participación que también es válida para SEPP), que como se mencionó en su oportunidad, actúa como un enlace entre el vendedor y la infraestructura financiera involucrada en el pago de la transacción y por el otro a una jerarquía de autoridades certificadoras cuya estructura dependerá del vendedor y comprador específicos en cada transacción en particular.

Aunque los alcances de estos esquemas no contemplan la participación formal de la institución financiera del comprador, se debe recordar que está debe existir para que sea posible realizar cualquier transacción de CE que base el pago de la misma en el uso de tarjetas de crédito, por la simple razón de que esta institución financiera es precisamente la que debió haber emitido la tarjeta con la que el comprador pretende pagar la transacción, administrando adicionalmente la cuenta asociada a dicha tarjeta, aunque como se ha establecido, opere a través de las redes privadas de carácter financiero.

5.4.1.2 Entidades que se autentican durante el protocolo

A este respecto, se tiene que los cuatro esquemas descritos permiten que se autentiquen las entidades participantes; sin embargo, también se destaca el hecho de que SSL frecuentemente permite que sea únicamente el comerciante el que se autentique.

Por su parte 3KP y SEPP contemplan la autenticación del comprador, el comerciante y la institución financiera del comerciante, aunque dicha autenticación se contemple formalmente sólo por SEPP al incluir la definición del sistema de administración de certificados, no contemplado por 3KP.

Sin embargo, son características de SET tales como: trabajar dentro de una jerarquía de confianza, utilizar un par de llaves por cada entidad participante, hacer uso de pares de llaves exclusivos para firmas digitales, así como del hecho de que define el uso de una llave de 2048 bits de longitud para la raíz de la jerarquía de confianza sobre las que basa su funcionamiento, las que proporcionan los elementos claves para ofrecer mecanismos de autenticación altamente eficientes.

5.4.1.3 Algoritmos de cifrado que utiliza o soporta cada esquema tanto de llave secreta como de llave pública

5.4.1.4 El tamaño de las llaves que utiliza cada uno de los algoritmos de cifrado

Tanto el apartado 5.4.1.3 como el 5.4.1.4 son especialmente importantes a considerar con respecto a los esquemas descritos pues como se ha descrito están íntimamente ligados al nivel de seguridad ofrecido por cada esquema, además de estar muy relacionados entre sí, razón por la cual ambos serán analizados a continuación.

En este sentido se destaca que SSL soporta varios algoritmos de cifrado de llave secreta entre los que se pueden mencionar, sin restringirse a ellos el RC4, RC2 IDEA, y el triple DES, considerando a los tres últimos en su modo CBC. Tanto RC4 como RC2 utilizan un tamaño de llave de 128 y 40 (en sus versiones exportables), mientras que IDEA y triple DES usan una llave de 64 y 192 bits de longitud respectivamente.

Refiriéndose a 3KP y SEPP, se tiene que soportan una variedad tan amplia como SSL, pero sin embargo a diferencia de éste que no establece un algoritmo para cifrado de llave pública en particular. Estos dos esquemas usan RSA de manera formal con un tamaño de llave de 1024 bits para todas las entidades participantes.

Finalmente SET establece específicamente el uso de DES con tamaño de llave de 50 bits y CMDF con una llave de 40 bits de longitud, como algoritmos para cifrado de llave secreta y a RSA para cifrado de llave pública, utilizando una llave de 1024 bits para todas las entidades participantes, exceptuando a la autoridad certificadora central para la que define el uso de una llave de 2048 bits de longitud, estableciendo de este

modo el uso de los actuales estándares tanto de cifrado de llave secreta como de llave pública.

5.4.1.5 El número total de llaves requeridas tanto para cifrado de llave secreta como para cifrado de llave pública

Continuando con el rubro de las llaves, se tiene que SSL emplea únicamente una llave secreta y un par de llaves pública y privada tanto del comprador como del vendedor que se utilizan para autenticación y cifrado de los datos intercambiados en los pasos iniciales de SSL, en los que como ya se describió se establecen los parámetros para proteger la información de la transacción.
La llave secreta, por su parte, se utiliza para a cifrar la información de la transacción como por ejemplo el número de tarjeta del comprador. A este respecto resulta importante recordar que esta llave secreta se genera utilizando tanto elementos intercambiados entre el comprador y el vendedor protegidos por un esquema de cifrado de llave pública, como con datos generados aleatoriamente.

Pasando a 3KP se tiene que involucra el uso de un número variable de llaves secretas y tres pares de llaves públicas y privadas. De hecho la especificación de 3KP no define formalmente el uso de llaves secretas, por lo que el número y uso de este tipo de llaves dependerá, en todo caso, de cada una de las implementaciones que se efectúen. En cuanto a los tres pares de llaves públicas y privadas, utilizadas en este esquema, número que da el nombre específico para este integrante de la familia *i*KP, se debe recordar que cada uno de ellos es utilizado por las entidades involucradas, a saber: comprador, vendedor y e institución financiera del vendedor, estableciéndose así una clara diferencia de 3KP con relación a los otros dos miembros de la familia iKP: 1KP y 2KP en los que se utilizan uno y dos pares de llaves públicas y privadas respectivamente. Estos tres pares de llaves, permiten que durante una transacción de CE que se base en 3KP, se cuente con no-repudio para cada mensaje firmado por cualquiera de las entidades participantes. Además, en 3KP estas llaves se utilizan tanto para proporcionar confidencialidad a través de cifrar información, como autenticación y no-repudio por medio de firmas digitales.

Todo lo anteriormente expuesto para 3KP es aplicable a SEPP, con la importante diferencia de que la especificación de este considera la opcional participación de un sistema de administración de certificados o CMS, situación que incrementa el número de pares de llaves de 3 a 5. Estos dos pares adicionales son utilizados por el Sistema de Gestión de Pagos, tanto para generar firmas digitales como para cifrar información dirigida tanto para el comprador como para el CMS.

Finalmente en el caso de SET, su especificación establece que durante una transacción de CE se utilizan dos llaves secretas para poder generar *sobres digitales*, los cuales consisten en el hecho de cifrar información de la transacción con una llave secreta para posteriormente cifrar esta llave con la llave pública del destinatario, de tal forma que cuanto éste último reciba ambos cifrados proceda a descifrar la llave secreta con su

llave privada, y una vez obtenida esta, se encuentre en condiciones para descrifrar la información de la transacción utilizando la llave secreta recién recuperada del "sobre". Está técnica permite cifrar información de manera eficiente pues brinda la posibilidad de cifrar una gran cantidad de información con un algoritmo de llave secreta, evitando que se utilice al cifrado de llave pública que, como se mencionó en su oportunidad, es más lento en proporción de uno a cien aproximadamente, que el cifrado de llave secreta; razón por la cual es frecuente que se haga uso de algoritmos de cifrado de llave pública únicamente para proteger a una llave secreta que se utilizará a su vez para proteger a la información de la transacción; obteniéndose de esta manera una eficiente combinación de ambos tipos de cifrado.

Finalmente en cuanto al número de pares de llaves privadas y públicas que considera una transacción con SET, se tiene que son 6 de ellos. Este número de pares de deriva de que SET establece que cada entidad participante debe contar con dos pares de llaves, un par para cifrar información y obtener confidencialidad, y el otro par para firmar logrando así no-repudio y autenticación.

5.4.2 Nivel de comparación 2

5.4.2.1 Número de operaciones de cifrado de llave pública

Se destacan en este rubro que SSL involucra únicamente una operación de cifrado de llave pública; dicha operación tiene el fin de cifrar el presecreto, generado por el comprador, para asegurar la confidencialidad de este elemento, garantizando de esta manera que solamente el comerciante pueda conocerlo.

En el caso de 3KP y SEPP el número de operaciones de cifrado de llave pública se mantiene, como en SSL, en uno; y en este caso dicha operación corresponde al cifrado de información confidencial como el monto y el valor hash de la descripción o el número de tarjeta del comprador, siendo estos datos los de mayor confidencialidad de entre todos los involucrados durante la ejecución del esquema.

Para el caso de SET el número de operaciones de cifrado se incrementa a 8 para el caso de SET, aumento considerable originado tanto a una protección extra fuerte (se debe recordar que debido al mayor tamaño de las llaves utilizadas en los algoritmos de llave pública con respecto a los de cifrado de llave secreta, se considera que en general dicho tamaño proporciona mayor seguridad) de la información confidencial, principalmente el número de tarjeta del comprador; así como a la utilización de firmas duales, siendo ambos casos, dos de los puntos fuertes de SET con respecto a sus niveles de seguridad.

Nota : En el análisis comparativo no se incluye el número de operaciones de cifrado de llave secreta debido por un lado, a que en la mayoría de los esquemas este dato

no es constante y por lo mismo es dificilmente mensurable, y por el otro al ya mencionado costo 100 veces mayor del cifrado de llave pública con relación al cifrado de llave secreta, siendo éste último menos representativo para los fines de éste análisis.

5.4.2.2 El número de firmas digitales

En este rubro se destaca que SSL no presenta ninguna firma digital, dejando así cerrada la posibilidad de obtener autenticación y por lo mismo no-repudio de los mensajes.

En cuanto a 3KP y SEPP, estos presentan 5 procesos de firmas digitales cada uno, firmas efectuadas sobre mensajes de autorización de pago, mensajes de instrucciones pago, mensajes de solicitudes de pago y mensajes de confirmaciones de compra.

En el caso específico de SEPP debe considerarse fuera de este total de 5, la posibilidad de firmas sobre mensajes de solicitud de renovación de certificados dirigidas al CMS, caso en el que este número se incrementaría.

SET, por su parte se posiciona de nuevo con un número mayor de procesos de firma digitales al involucrar 7 de estos procesos. En este caso los procesos de firma se efectúan sobre mensajes de instrucciones de pago, orden de compra o pedido, solicitud de pago, transferencia de fondos, consulta de estado de la transacción, entre otros más. Un punto importante a resaltar en SET es que una de estas siete firmas corresponde a una firma dual, la cual relaciona las instrucciones de pago con la orden de compra o pedido.

5.4.2.3 El número de núnicos generados

En cuanto a este número de núnicos generados, SSL involucra la generación de tres de ellos, dos de los cuales son utilizados como material para la generación de la llave secreta o de sesión, y el tercero como un identificador de la transacción misma.

Por su parte 3KP y SEPP involucran la generación de cinco núnicos, uno de los cuales se asocia a la fecha en la que se efectúa la transacción para identificarla de manera única, otro de ellos al ser firmado por el comerciante es utilizado para efectos de que el comprador cuente con un comprobante de que el vendedor ha aceptado el pago por la transacción, otro de estos núnicos se utiliza para demostrar la frescura de los mensajes y los dos restantes se utilizan para proteger contra ataques tipo diccionario el valor hash calculado sobre algún dato confidencial como el número de tarjeta del comprador.

Finalmente en cuanto a SET, éste involucra 6 núnicos en total durante una transacción, siendo utilizados de manera similar que en 3KP y SEPP como parte del identificador de la transacción, para proteger los valores hash de información confidencial contra

ataques por diccionario y para asegurar la frescura de los mensajes y evitar así los ataques por reflexión, principalmente.

5.4.2.4 El número total de mensajes intercambiados durante el protocolo

Aunque como ya se mencionó en su oportunidad, con un menor número de mensajes se obtiene sencillez del esquema, SET demuestra que el definir mensajes específicos para por ejemplo la consulta del estado de la transacción por parte del comprador, añade seguridad y robustez a la realización de la misma. Bajo estas premisas se observa que SSL involucra de manera formal 5 mensajes, de los cuales los cuatro primeros se usan para establecer parámetros e identificadores de la transacción, provocando que el intercambio de datos relacionados a la transacción misma se efectúe a partir del quinto intercambio.

Por su parte 3KP y SET, involucran 6 mensajes o intercambios, entre los que se contemplan: un envió inicial, un procesamiento inicial y composición de factura, un procesamiento de factura, un procesamiento de instrucciones pago y generación de la solicitud de autorización de pago, un procesamiento de la solicitud del pago y por último una respuesta de factibilidad de pago.

Finalmente SET incluye durante una transacción un total de 10 mensajes o intercambios. Este número considerable de mensajes se deriva del uso de pares de mensajes por parte de SET, donde cada par consiste de una Solicitud/Respuesta tales como: SolicitudInical/RespuestaInicial, Pedido/RespuestaPedido, SolicitudPago/RespuestaPa go, entre otros. Dentro de este conjunto de pares específicos para cada paso, SET define uno que destina para que cualquier comprador pueda conocer el estado de sus transacciones en cualquier momento de la transacción que sea posterior al pedido u orden de compra conocido como SolicitudConsulta/RespuestaConsulta.

5.4.3 Nivel de comparación 3

5.4.3.1 Los servicios de seguridad que satisface cada esquema

A este respecto a este rubro e iniciando nuevamente con SSL, se puede destacar que proporciona confidencialidad en las comunicaciones entre el comprador y el comerciante, autenticación de ambos, así como integridad de los mensajes que se intercambian durante la transacción. Aunque estos servicios son los básicos requeridos para una comunicación segura, para el caso específico de una transacción de CE que utilice una tarjeta de crédito como medio de pago es recomendable disponer de otros más. Por esta razón 3KP, SEPP y SET proporcionan además de los ya mencionados para SSL, la autenticación de los mensajes de autorización de la transacción por parte

del comprador, el comerciante y de la institución financiera del vendedor; adicionalmente tanto 3KP como SEPP ofrecen la posibilidad de brindar anonimato para el comprador.

Esta serie adicional de servicios de seguridad, permite entre otras cosas que la información confidencial que el comprador envía al comerciante, como por ejemplo su número de tarjeta, no pierda dicha confidencialidad al llegar al vendedor, situación que si ocurre con SSL debido a que éste sólo asegura la información durante su transmisión dejándola sin protección adecuada al llegar al comerciante. De hecho SET se muestra altamente efectivo en este sentido con el uso de las firmas duales, las cuales permiten que el comprador demuestre haber firmado al mismo tiempo tanto las instrucciones de pago como la información de la orden, sin revelar las primeras al comerciante ni la segunda a la institución financiera del vendedor.

5.4.3.2 Las principales ventajas

En este sentido se tiene que SSL presenta la mayor sencillez de entre los cuatro esquemas confrontados, sencillez originada por el reducido número de mensajes, de elementos intercambiados en dichos mensajes, entre otros más. Además de esto SSL está incluido en la mayoría de los navegadores actuales lo que le brinda la mayor disponibilidad de los esquemas confrontados. Otra de las ventajas principales de SSL radica en el hecho de que es de propósito general.

Finalmente SSL es el esquema que involucra al menor número de entidades de manera directa durante una transacción de CE que base el pago de la misma en el uso de tarjetas de crédito al contemplar la participación del comprador y el comerciante únicamente.

En cuanto a 3KP y SEPP, comparten dos ventajas principales; por un lado la de poder adecuarse para el cobro de cheques electrónicos, característica que le confiere una atractiva flexibilidad, y por el otro lado el permitir que tanto la información bancaria como los datos confidenciales del comprador conserven su confidencialidad después de haber llegado al comerciante, situación que como se estableció en su oportunidad SSL no contempla.
Como característica adicional de SEPP se tiene la definición del sistema de administración de certificados o CMS, con el que da un paso adelante de 3KP en la formalización de una jerarquía de confianza.

Por último con respecto a SET, se cuentan entre sus principales ventajas la introducción de las firmas duales, la protección extra fuerte de los datos confidenciales del comprador, el uso de una llave de 2048 bits de longitud para la autoridad certificadora central, y el hecho de estar disponible como una extensión de los navegadores.

5.4.3.3 Las principales desventajas

Para finalizar con éste análisis comparativo y contemplando las principales desventajas mostradas por cada uno los esquemas, se puede destacar que SSL protege a la información confidencial del comprador únicamente durante su transmisión dejándola sin protección al llegar al comerciante, asociada a esta desventaja se tiene que SSL tampoco protege de manera especial al número de tarjeta del comprador, dejándolo en cierta medida vulnerable a ataques por diccionario.

Finalmente otro aspecto negativo de SSL lo representa el hecho de que se limita al uso de los certificados conocidos por el navegador, perdiendo así puntos de flexibilidad para el rango de certificados aceptados.

En cuanto a 3KP comparte con SEPP como una de sus ventajas principales el hecho de que no ofrece una forma en la que el comprador pueda relacionar de forma directa las instrucciones de pago con la información de la orden o pedido, hecho que SET resuelve de forma elegante con las firmas duales. Además 3KP no define alguna manera en la que un comprador pueda conocer el estado en el que se encuentra alguna de sus transacciones antes que reciba a través del comerciante el mensaje de autorización de la transacción por parte de la institución financiera de este último.

Refiriéndose específicamente a SEPP, una de sus principales ventajas radica en el hecho de que su desarrollo y mejoras han sido paulatinamente abandonadas a causa del desarrollo y aparición de SET.

Por último en el caso de SET, se tiene por una parte que su implementación resulta compleja y relativamente costosa a causa de los requerimientos que involucra tanto de equipo como de infraestructura, al número elevado de entidades que involucra, a la necesidad de contar con un certificado SET para cada tarjeta de crédito del comprador y a que puede trabajar únicamente con tarjetas de crédito.

Como se comentó al inicio del capítulo, el compendio de los resultados del anterior análisis capítulo se muestra en tablas comparativas. Cabe recordar que cada una de las tablas corresponde a uno de los tres niveles de análisis definidos para este trabajo en particular. Estas tablas se muestran a continuación.

Esquema	Entidades que Participan	Entidades Autenticadas	Tipo de Algoritmo de Cifrado	Algoritmos de Cifrado que Utiliza (o soporta)	Tamaño de Llave en bits	Número de	total llaves
SSL	C, V	V, C (Opcional)	PÚBLICA SECRETA	Variable RC4 RC4 RC2 CBC RC2 CBC IDEA CBC DES CBC Triple DES CBC	128 40 (exportable) 128 40 (exportable) 128 64 192	SECRETA PÚBLICA	1 Variable
3KP	C, V, B	C, V, B	PÚBLICA SECRETA	RSA RC4 RC4 RC2 CBC RC2 CBC IDEA CBC DES CBC Triple DES CBC	1024 128 40 (exportable) 128 40 (exportable) 128 64 192	SECRETA PÚBLICA	Variable Variable
SEPP	C, V, B	C, V, B	PÚBLICA SECRETA	RSA RC4 RC4 RC2 CBC RC2 CBC IDEA CBC DES CBC Triple DES CBC	1024 128 40 (exportable) 128 40 (exportable) 128 64 192	SECRETA PÚBLICA	1 5
SET	C, V, B, SGP,AC	C, V, SGP	PÚBLICA SECRETA	RSA DES CDMF	2,048 (para root de AC) 1,024 56 40	SECRETA PÚBLICA	2 6

Tabla 1. Elementos del nivel de comparación 1

Esquema	Número de Cifrados de Llave Pública	Número de Firmas Digitales	Número de Núnicos Generados	Número de Mensajes
SSL	1	0	3	5
3KP	1	5	5	6
SEPP	1	5	5	6
SET	8	7	6	10

Tabla 2. Elementos del nivel de comparación 2

Esquema	Servicios de seguridad que proporciona	Principales Ventajas	Principales Desventajas
SSL	a) Confidencialidad en las comunicaciones entre C y V b) Autenticación de V c) Integridad de los mensajes intercambiados entre C y V	1. Sencillez de Protocolo 2. Incluido en la mayoría de los navegadores 3. De propósito General 4. Número reducido de entidades participantes	1. No protege especialmente el número de cuenta de C 2. Cuando la información llega a M pierde confidencialidad 3. Certificados limitados a los conocidos por el navegador
3KP	a) No-repudio de autorización de la transacción por C b) No –repudio de autorización por V c) No –repudio de autorización por B d) Certificación y autorización de V e) Recibo de V f) Confidencialidad de la transacción g) Anonimato h) Evita pagos no autorizados	1. Puede adecuarse para la gestión de cobros de cheques electrónicos 2. La información bancaria y los datos de C conservan su confidencialidad	1. El protocolo no define forma alguna de que C conozca el estatus de la transacción antes de que reciba el mensaje de autorización de transacción 2. No ofrece una forma en que C pueda relacionar directamente la orden de compra con las instrucciones de pago
SEPP	a) No-repudio de autorización de la transacción por C b) No –repudio de autorización por V c) No –repudio de autorización por B d) Certificación y autorización de V e) Recibo de V f) Confidencialidad de la transacción g) Anonimato h) Evita pagos no autorizados	1. Puede adecuarse para la gestión de cobros de cheques electrónicos 2. Define un sistema de administración de certificados 3. La información bancaria y los datos de C conservan su confidencialidad	1. Su desarrollo fue abandonando para desarrollar SET 2. No ofrece una forma en que C pueda relacionar directamente la orden de compra con las instrucciones de pago
SET	a) No-repudio de autorización de la transacción por C b) No –repudio de autorización por V c) No –repudio de autorización por B d) Certificación y autorización de V e) Confidencialidad de la transacción f) Evita pagos no autorizados	1. Introducción de Firmas Duales 2. Uso de llave pública con tamaño de 2048 bits para la raiz de la jerarquía de confianza 3. Disponible como extensión a los navegadores	1. Implementación compleja 2. Varias entidades participantes 3. Requiere un certificado SET para cada tarjeta 4. Sólo transacciones de Tarjetas de Crédito

Tabla 3. Elementos del nivel de compración 3

Como se explicó en su oportunidad la tabla 1 contiene el resumen del análisis hecho sobre los cuatro esquemas mencionados, considerando 5 columnas, donde cada una de ellas se corresponde con uno de los parámetros de comparación del primer nivel de comparación de los tres en los que se dividió el análisis efectuado en este capitulo, siendo estas columnas las siguientes: la primer columna menciona las entidades que participan en cada uno de loas cuatro esquemas analizados, la columna 2 menciona las entidades participantes que se autentican durante una transacción, la columna 3 resume el tipo de algoritmo de cifrado que cada uno utiliza, la columna cuatro resume el o los algoritmo de cifrado que son utilizados o soportados, finalmente la columna 5 muestra el numero total de llaves que son utilizadas durante una transacción.

Por su parte la tabla 2, contiene el resumen del análisis hecho sobre los cuatro esquemas de CE comparados en este capítulo, considera 4 columnas, cada una de ellas se corresponde con uno de los parámetros de comparación del nivel de comparación 2 del análisis realizado. La primer columna muestra el número de cifrados de llave pública, la columna 2 muestra el número de firmas digitales efectuadas, la columna 3 resume el número de núnicos generados durante una transacción, finalmente la columna 4 indica el número mensajes totales.

Finalmente la tabla 3, contiene el resumen del análisis hecho sobre los cuatro esquemas de CE comparados en este capítulo, considera 3 columnas, y cada una de ellas se corresponde con uno de los parámetros de comparación del nivel de comparación 3 del análisis realizado. Cada una de estas columnas son las siguientes: la primer columna se refiere a los servicios de seguridad que son proporcionados, la columna 2 enumera las principales ventajas mostradas y finalmente la columna tres enumera las principales desventajas de cada esquema.

Nota: Las tres tablas poseen una columna adicional de las establecidas anteriormente que es la primera en cada una de ellas e indica el esquema de CE de que se trata, razón por la cual se considera como la columna cero.

Capítulo 6

RESULTADOS, CONCLUSIONES Y TRABAJO FUTURO

En este capítulo se presentan tanto los resultados arrojados por el análisis comparativo presentado en el anterior capítulo, como las conclusiones obtenidas de la elaboración de este trabajo. También se mencionan algunas de las actividades pendientes de realizar a corto plazo, tomando como punto de partida este trabajo.

6.1 Resultados

En este trabajo se ha presentado un estudio sobre cuatro esquemas de CE que se basan en tarjetas de crédito. Este estudio muestra los principales ataques a este tipo de esquemas, las fortalezas y debilidades de cada uno de ellos. Adicionalmente se han establecido las características principales de cada uno de estos esquemas.

Es estudio y descripción de cada uno de los esquemas, se ha realizado partiendo de la definición precisa de la manera en la que operan las tarjetas de crédito y de las razones que las han convertido en uno de los métodos más utilizados para realizar compras por internet. Aunque el estudio se realizo sobre las características generales de cada uno de los esquemas, se ha enfatizado el aspecto de la seguridad. Dicho énfasis responde principalmente a la preocupación por parte de compradores, empresas, instituciones financieras y en general de los involucrados en las transacciones de este tipo, sobre el hecho de enviar sus datos confidenciales, tal como su número de tarjeta a través de la red, con el conocimiento de los múltiples peligros a lo que éste número se expondrá durante tu transmisión hacia su destino.

Para realizar lo anterior, se ha mantenido comunicación directa con investigadores de tiempo completo en criptografía y seguridad en cómputo, con equipos de desarrollo de portales comerciales de gran envergadura, con desarrolladores de soluciones de seguridad de una de las pocas empresas que de manera especializada se dedican a esta área en nuestro

país y se ha participado ampliamente en el desarrollo de varios de los módulos, aunque específicamente en el de seguridad, de un sistema de comercio electrónico para el sector gobierno, que representa una de las primeras y más completas soluciones en nuestro país en esta área.

Como contribución fundamental de este trabajo en el área de comercio electrónico, se hizo un análisis comparativo de los esquemas presentados en el capítulo 4. Este análisis se presenta en el capítulo 5 de este trabajo y se resume en las tablas 1, 2 y 3 del mismo capitulo. Dicho análisis fue realizado en función de las entidades participantes, de las características de cada uno de los esquemas, algoritmos de cifrado utilizados, número de operaciones de cifrado, tamaños de llaves usadas, ventajas y desventajas principales. Hasta el momento la existencia de tesis que aborden cuestiones de comercio electrónico desde el punto de vista de la seguridad son muy escasos, y aún más aquellos trabajos que presenten bases criptográficas formales.

El análisis mencionado puede resultar de gran valía sobre todo por el gran auge que junto con internet está teniendo el comercio electrónico en todo el mundo, incluido nuestro país. Sin embargo, a pesar del gran interés que ha despertado esta nueva modalidad del comercio las empresas, compradores, gobiernos, e instituciones bancarias han adoptado una actitud muy pasiva, lo que ha ocasionado que el desarrollo de legislaciones, implementaciones de esquemas como los estudiados en este trabajo, políticas, etc., se muestre rezagado en comparación con los EUA, Europa y alguno países e Mercosur tales como Brasil y Colombia. Es por lo anterior que el análisis mencionado pretende responder a la creciente necesidad de información con respecto a los diferentes esquemas de comercio electrónico que pueden ser eventualmente utilizados por las empresas de nuestro país, siempre desde un punto de vista de seguridad y acudiendo a las bases criptográficas que utilizan la mayoría de este tipo de esquemas como una de las mejores formas para obtener servicios de seguridad indispensables en este tipo de transacciones.

Otra contribución de este trabajo consiste en el tratamiento formal que se da a ciertos aspectos relacionados al comercio electrónico, y que en los sitios de internet y en mucha de la documentación existente hoy en día es abordado con un estilo más mercadológico que técnico, careciendo de las bases formales presentes en el presente trabajo. Entre estos aspectos se pueden incluir: el tratamiento de protocolo de una transacción de comercio electrónico, el estudio de los diversos medios de pago para las transacciones de comercio electrónico, la descripción formal de cuatro esquemas de comercio electrónico que se basan en tarjetas de crédito y el análisis comparativo ya mencionado.

6.2 Conclusiones

De acuerdo al estudio y análisis realizado en el presente trabajo, a continuación se establecen una serie de conclusiones con respecto al mismo.

Conforme el número de usuarios en Internet aumenta, aumenta también el número y variedad de transacciones de tipo comercial que se efectúan de forma electrónica. De hecho el CE es una de las tecnologías que han alcanzado gran relevancia y cautivado la atención de muchos individuos y organizaciones que hacen uso de internet. Varias son las ventajas que presenta con respecto al comercio tradicional y que lo posicionan como una interesante y novedosa opción para efectuar una de las actividades de mayor relevancia en la sociedad actual: la de comprar y vender productos y servicios. Y es precisamente esta importancia la que aporta un buen número de elementos que dan motivos para vislumbrar un futuro rico y basto para el CE. Sin embargo, a pesar de lo anterior se debe entender al CE como una nueva modalidad del comercio, no como su sustituto o como una práctica radicalmente distinta o ventajosa.

Entre las ventajas más sobresalientes del CE, se incluyen la presencia global de bienes y servicios, al permitir que las empresas u organizaciones presenten y promocionen sus productos y servicios por medio de catálogos electrónicos a través de internet, la disminución de costos asociados por ejemplo a niveles de inventarios muy bajos o al evitar la participación de intermediarios o gastos de distribución, en el caso específico de los bienes de naturaleza digital, así como la seguridad obtenida por medio de técnicas criptográficas tales como las firmas digitales y el cifrado de información.

Las anteriores ventajas son sólo algunas de las mostradas por el CE. Sin embargo, como cualquier tecnología presenta importantes desventajas tales como las diferentes legislaciones y prácticas comerciales en países diferentes, la infraestructura y conocimientos requeridos para poder efectuar una transacción de CE, así como el aumento en el tiempo de entrega de los productos de naturaleza física en el caso de transacciones que involucren el traslado de los productos de un país a otro.

Si bien el concepto de CE no es estrictamente novedoso, su realización sí lo es, pues desde hace tiempo tanto investigadores como empresas y organizaciones se han dado a la tarea de preparar el camino para que esta realización sea cada vez más palpable.

Con respecto a la situación actual del CE en el ámbito mundial, éste se encuentra en una etapa de muchos cambios, desarrollos, experimentación, promoción y demás aspectos relacionados a una tecnología de gran interés y novedad. Entre estos aspectos uno de los fundamentales consiste en la legislación necesaria en el ámbito del CE; y aunque en algunos países de Europa, EUA y Sudamérica se ha iniciado de manera formal; en el caso particular de México dicha legislación no existe. Una de las razones para esta situación radica en el hecho de que los legisladores de nuestro país han tomado, en el mejor de los casos, una actitud pasiva; a tal grado que al momento de la realización de este trabajo, una

única iniciativa de ley para la regulación del CE se ha efectuado por parte de legisladores del Partido Acción Nacional y solamente una ley considera aspectos de transacciones electrónicas, siendo esta ley la Ley de Adquisiciones Publicas, emitida por la Secretaría de Contraloría y Desarrollo Administrativo. Esta falta de regulación se ha reflejado en una actitud desconfiada y cautelosa en extremo por parte de consumidores, comerciantes e instituciones financieras al momento de efectuar alguna transacción de CE. Esta desconfianza hasta cierto punto razonable no ha permitido la entrada tan rotunda y consistente que el CE ha mostrado en otros países, postergando, y en ocasiones perjudicando, el inicio de operaciones de CE por empresas e instituciones financieras mexicanas.

A pesar de esta actitud tan poco receptiva de los niveles avanzados del CE en nuestro país, muchas empresas han comenzado, al menos, a montar catálogos electrónicos de sus productos y servicios en Internet. Algunas de estas empresas han obtenido una respuesta adecuada a las expectativas. Sin embargo, se han comenzado a observar las primeras quiebras de tiendas virtuales o simplemente algunas empresas han dejado de vender por Internet como en el caso de una de las compañías más fuertes en la fabricación y venta de ropa casual y de mezclilla: Levi's Strauss

Todo este ambiente cambiante y de situaciones extremas es natural, sobre todo por el poco camino recorrido en todos los ámbitos relacionados al CE en nuestro país. Sin embargo a pesar de todos estos contrastes, se prevé un incremento paulatino en el número de transacciones de CE a todos niveles; dicho incremento se verá reflejado en la maduración de muchos procesos y actividades asociadas al CE.

Dentro de estos procesos, uno de los más importantes es el pago de forma electrónica, que se presenta en los niveles avanzados del CE. Estos pagos pueden realizarse por medio de dinero y cheques electrónicos, además de tarjetas de crédito.

A este respecto son muchos los esquemas que existen y que se han propuesto para soportar pagos electrónicos usando tarjetas de crédito. En la mayoría de los casos se espera que dichos esquemas proporcionen el nivel suficiente de seguridad como para que la información confidencial que este tipo de transacciones involucra, como por ejemplo el número de la tarjeta con el que el comprador pretende pagar la transacción, viaje de una entidad a otra de manera segura contra ataques de todo tipo perpetrados por atacantes que van desde los inexpertos hasta aquellos que han hecho de este tipo de actividad su modo de subsistencia. Para lograr esta protección, se ha recurrido al desarrollo de esquemas que implementan servicios de seguridad basados en la mayoría de los casos en métodos y herramientas de naturaleza criptográfica.

En este trabajo se analizaron con respecto a sus debilidades, fortalezas, características principales, ventajas y desventajas, cuatro de los principales esquemas de CE que basan el pago de la transacción en tarjetas de crédito: SET, SSL, iKP y SEPP, pudiéndose concluir de este análisis, lo siguiente:

Cada uno de los esquemas analizados puede trabajar de forma adecuada dependiendo de las necesidades y niveles de seguridad requeridos:

a) SSL se muestra adecuado para transacciones que no involucren una gran cantidad de dinero o información confidencial.

b) iKP proporciona una serie importante de servicios de seguridad, sobre todo con 3KP que junto con SEPP proporciona algunos servicios de seguridad que SSL no ofrece. Sin embargo, como uno de sus puntos negativos se puede mencionar que protege de igual manera a toda la información de una transacción, incluida la confidencial y como otro punto que carece en algunos aspectos de eficiencia, como en el caso de las firmas digitales, por lo que ambos esquemas pueden trabajar de forma aceptable en transacciones que involucren montos moderados, además de que pueden resultar opciones adecuadas para entidades que no cuenten con una gran cantidad de recursos como para implantar esquemas que requieren un mayor número de ellos como por ejemplo SET.

c) Finalmente SET se posiciona como el esquema más robusto y completo de los analizados, sin olvidar que es también el más complejo de implementar y el que más recursos requiere, por lo que se perfila como uno de los candidatos más fuertes para convertirse en estándar de esquemas de comercio electrónico que se basan en tarjetas de crédito, sobre todo para aquellas transacciones que involucren montos que vayan desde los moderados hasta los altos y que involucren datos confidenciales.

Es importante señalar que estos cuatro esquemas no son los únicos disponibles, de hecho existe una gran variedad de ellos, y su número va en aumento. A pesar de esta de esta variedad, SSL es uno de los esquemas de mayor uso sobre todo en el continente americano. Sin embargo, se espera que en un lapso relativamente corto comience a ser reemplazado por otros esquemas más seguros como SET.

Desafortunadamente la mayoría de las escasas instituciones financieras en nuestro país que actualmente ofrecen algún tipo de transacción de CE, utilizan también SSL; situación que encuentra su opuesto en Sudamérica y algunos países de Europa y Asia donde SET ha sido recibido de manera más entusiasta y ha demostrado sus ventajas sobre SSL.

Hablando en forma específica de México, se tiene que poco a poco la cantidad y variedad de empresas que de alguna u otra forma han comenzado a participar del comercio electrónico ha ido en aumento. Los resultados que cada una de estas empresas han obtenido son tan variadas como las propuestas de cada una de ellas. En la gran mayoría de los casos se ha iniciado en los niveles básicos de comercio electrónico, y a través de la experiencia se ha logrado llegar a participar en los niveles avanzados, ofreciendo en este último caso diversas formas de pago, incluyendo el electrónico, para llegar a muy diversos sectores del mercado.

Con relación a la actitud de las instituciones financieras de nuestro país ante el comercio electrónico, esta había sido hasta la fecha, muy pasiva a la espera de las adecuaciones a las legislaciones actuales o la formulación de nuevas leyes que considerarán los procesos que involucran los niveles avanzados del comercio electrónico. Sin embargo, recientemente han comenzado a tomar la iniciativa y las asociaciones de instituciones

bancarias se han dado a la tarea de definir sus propias reglas del juego con el fin de comenzar el desarrollo de propuestas que involucren el uso de esquemas tan robustos como SET. A pesar de lo anterior los resultados de estos esfuerzos iniciales, no se verán sino hasta un mediano plazo.

Finalmente considerando a los compradores, la actitud siempre ha sido abierta aunque con gran desconfianza sobre todo al momento de enviar por la red su número de tarjeta. Se espera, sin embargo que esta desconfianza disminuya conforme las empresas ofrezcan diversas formas de pago y se logre demostrar lo seguras que pueden resultar las transacciones de CE cuando éstas son sustentadas por esquemas que proporcionan niveles de seguridad suficientes y adecuados.

A este respecto el análisis hecho en este trabajo puede servir a varios fines. En primer lugar como un acercamiento general pero completo y formal del concepto de comercio electrónico, segundo como una forma sencilla y directa de conocer las características principales de cuatro de los esquemas de comercio electrónico basados en tarjetas de crédito de amplio uso en la actualidad, y tercero como una manera formal de comparar, desde un punto de vista de seguridad, a los cuatro esquemas analizados que se basan en técnicas criptográficas para proporcionar una serie de servicios de seguridad indispensables para esta modalidad del comercio.

Para finalizar cabe decir que se espera dentro de poco tiempo que el comercio electrónico alrededor de todo el mundo sea una forma rápida, barata, sencilla, cómoda, eficiente y cotidiana de adquirir bienes y contratar servicios; las personas comprarán por medio de internet a diario desde su despensa hasta automóviles. Sin embargo lo único de lo que se puede estar seguro es que tal vez después del comercio electrónico la realidad económica del mundo no será la misma.

6.3 Trabajo Futuro

El análisis presentado es un trabajo aún no acabado, puesto que se realizó en papel con enfoque teórico. Se requiere pues que se analicen otros esquemas de CE que usen tarjetas de crédito, que no fueron considerados dentro del alcance de este trabajo, tales como CyberCash. Se requiere además, realizar la parte práctica del trabajo por medio implementaciones de los esquemas presentados; tales implementaciones pueden realizarse tomando como punto de partida el presente trabajo, de tal manera que se consideren las características propias de cada esquema para que cumpla con las necesidades de seguridad y disponibilidad de recursos de los sistemas a los que se integre cada implementación en particular.

S

SEP (Sistema Electrónico de Pagos): Tipo de sistema que permite que el pago de alguna transacción se efectúe de forma electrónica

SGP (Sistema de Gestión de Pagos): Sistema de cómputo que durante una transacción electrónica de tipo comercial sirve de enlace entre el comerciante y la institución financiera de éste último.

SHA (Secure Hash Algorithm): Función hash basada en MD4 y desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) y publicado como un estándar federal para el procesamiento de información en 1993.

T

TEF: Transacción que consiste en mover dinero de una cuenta a otra de forma electrónica

TETC: Transacción Electrónica de Tipo Comercial

Texto cifrado: Conocido también como ciphertext se refiere a cualquier conjunto de datos que permanecen de forma legible.

Texto en claro: También llama plaintext, se refiere al mensaje original que se encuentra de forma legible, el cual es transformado, por medio de un proceso de cifrado o encripción, en un texto aparentemente aleatorio y sin sentido.

U

URL(Uniform Resource Locator): Es la dirección de algún recurso accesible en internet. El tipo de recurso depende del protocolo de aplicación en internet. De este modo si se utiliza el protocolo HTTP, los recursos pueden ser una página HTML, un archivo de imagen, etc.

X

X.509: Recomendación emitida por la CCITT como parte de la serie de recomendaciones X.500 que establece un formato y contenido particulares para los certificados digitales. X.509 está basada en el uso de criptografía de llave pública y firmas digitales. Este estándar no establece el uso de algún algoritmo pero recomienda a RSA.

REFERENCIAS

[1] W. Stallings, *Network And Interntwork Securiy Principles and Practice,* Prentice Hall,1995

[2] Charles F. Pfleeger, *Security in Computing* Prentice Hall,1997

[3] B. Schneier, *Applied Criptography,* John Willey & Sons Inc, 1994

[4] Roger Clarke, *Electronic Commerce Definitions,* Xamax Consultancy, http://www.anu.edu.au/people/Roger.Clarke/EC/ECDefns.html

[5] Ch. Kaufman, R. Perlman, M. Speciner, *Network Security Private Communication in a Public World,* Prentice Hall, 1995

[6] Frederic J. Cooper, *Implementing Internet Security,* Prentice Hall, 1995

[7] D. O' Mahony, M. Peirce, *Electronic Payment Systems,* Artech House,1997

[8] D. Tapscott, *La Economía Digital,* McGraw Hill, Mayo 1997

[9] N. Asokan, M. Steiner, M. Waidner, *The state of the Art in Electronic Payment Systems,* IEEE Computing Practices, Junio 1998

[10] B. Schneier, *Cryptography Second Edition: protocols, algorithms and source code in C,* John Willey And Sons, Inc., 1996

[11] L. Gong, T. Mark, A. Lomas, R. N. Needham y J.H. Saltzer, "Protecting Poorly chosen Secrets from Guessing Attacks", IEEE Journal on Selected Areas in Communications, Vol. 11, No.5, Junio, 1993

[12] Jamie Jaworski, *Java 1.2 Al descubierto,* Prentice Hall, Madrid 1999

[13] L. Hernández, "Protocolos Criptográficos de Autenticación e Intercambio de Llaves Basados en Passwords", Mayo 1999.

GLOSARIO

A

Autenticación: Proceso usado para verificar la integridad de datos transmitidos, especialmente un mensaje.

ACC (Autoridad Certificadora Central): Entidad que ocupa el nivel más elevado en la estructura jerárquica o de confianza sobre la que trabajan los certificados digitales en algunos esquemas de CE. Entidad también conocida como raíz de certificación.

CCITT (Consultative Committee on International Telephone and Telegraphy): Organismo que en la actualidad es conocido como el ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union), es el organismo principal en la promoción de estándares cooperativos para equipo de telecomunicaciones y sistemas. Su sede se encuentra en Geneva, Suiza.

C

CDMF: Versión modificada de DES con un tamaño de llave efectiva de 40 bits. Es exportable fuera de EUA

Certificado digital: Documento digital que identifica a la autoridad certificadora que lo ha emitido y a la entidad dueña de la llave pública certificada. Este documento contiene tanto la llave pública del dueño de la llave como la firma digital de la autoridad que emitió el certificado

Cifrado: Transformación de texto legible en texto ilegible y sin sentido aparente. Dicha transformación debe ser reversible y esta basada en tablas o algoritmos de transformación.

Cifrado de llave pública: Tipo de cifrado que se conoce también como cifrado de llave asimétrica y que utiliza dos llaves: una pública y otra privada. Se apoya en funciones matemáticas para relacionar cada una de las llaves. efectuando el cifrado con la llave pública y el descifrado con la privada si se desea obtener confidencialidad, y el orden inverso si se desea autenticación y no repudio.

bancarias se han dado a la tarea de definir sus propias reglas del juego con el fin de comenzar el desarrollo de propuestas que involucren el uso de esquemas tan robustos como SET. A pesar de lo anterior los resultados de estos esfuerzos iniciales, no se verán sino hasta un mediano plazo.

Finalmente considerando a los compradores, la actitud siempre ha sido abierta aunque con gran desconfianza sobre todo al momento de enviar por la red su número de tarjeta. Se espera, sin embargo que esta desconfianza disminuya conforme las empresas ofrezcan diversas formas de pago y se logre demostrar lo seguras que pueden resultar las transacciones de CE cuando éstas son sustentadas por esquemas que proporcionan niveles de seguridad suficientes y adecuados.

A este respecto el análisis hecho en este trabajo puede servir a varios fines. En primer lugar como un acercamiento general pero completo y formal del concepto de comercio electrónico, segundo como una forma sencilla y directa de conocer las caracteristicas principales de cuatro de los esquemas de comercio electrónico basados en tarjetas de crédito de amplio uso en la actualidad, y tercero como una manera formal de comparar, desde un punto de vista de seguridad, a los cuatro esquemas analizados que se basan en técnicas criptográficas para proporcionar una serie de servicios de seguridad indispensables para esta modalidad del comercio.

Para finalizar cabe decir que se espera dentro de poco tiempo que el comercio electrónico alrededor de todo el mundo sea una forma rápida, barata, sencilla, cómoda, eficiente y cotidiana de adquirir bienes y contratar servicios; las personas comprarán por medio de internet a diario desde su despensa hasta automóviles. Sin embargo lo único de lo que se puede estar seguro es que tal vez después del comercio electrónico la realidad económica del mundo no será la misma.

6.3 Trabajo Futuro

El análisis presentado es un trabajo aún no acabado, puesto que se realizó en papel con enfoque teórico. Se requiere pues que se analicen otros esquemas de CE que usen tarjetas de crédito, que no fueron considerados dentro del alcance de este trabajo, tales como CyberCash. Se requiere además, realizar la parte práctica del trabajo por medio implementaciones de los esquemas presentados; tales implementaciones pueden realizarse tomando como punto de partida el presente trabajo, de tal manera que se consideren las caracteristicas propias de cada esquema para que cumpla con las necesidades de seguridad y disponibilidad de recursos de los sistemas a los que se integre cada implementación en particular.

Cifrado de llave secreta: Esquema conocido también como cifrado de llave simétrica que permite el cifrado de información con el uso de una sola llave, donde dicha llave es utilizada tanto para cifrar como para descifrar los datos.

CMS (Certificate Managment System): Sistema administrador de certificados, definido en SEPP y operado por uno o más instituciones financieras que proporciona servicios de generación y distribución de certificados digitales.

Criptoanálisis: Rama de la criptología que se ocupa del rompimiento de cifrados para recuperar información, o forzar información cifrada que puede ser considerada como auténtica.
Criptología: Ciencia que se encarga del ocultamiento de la información para su protección. Se divide en criptografía y criptoanálisis

Criptografía: Rama de la criptología encargada del diseño de algoritmos para cifrado y descifrado con el fin de asegurar la privacidad y/o autenticación de mensajes

D

DES (Data Encription Standard): Algoritmo estándar de cifrado de llave asimétrica, fue adoptado por la Oficina Nacional de Estándares en 1977. DES cifra los datos en bloques de 64 bits utilizando una llave de 56 bits

F

Firma blindada: Técnica basada en las firmas digitales y puede equipararse a poner un mensaje en un sobre junto con una pieza de papel carbón situación en la que nadie puede leer el mensaje a través del sobre. Una firma digital es efectuada a través de firmar desde el exterior del sobre. La firma se hará a través del papel carbón hacia el mensaje. Cuando el mensaje es extraído del sobre, estará firmado y de esta manera la entidad que lo haya firmado, no habrá sido capaz de conocer el contenido de lo que firmó

Firma digital: Resultado de cifrar un mensaje utilizando un esquema de cifrado asimétrico, de manera que la persona que posea el mensaje inicial y la llave pública del firmante, pueda determinar de forma fiable si dicho cifrado se hizo utilizando la llave privada correspondiente.

Firma dual: Técnica que permite asociar la identidad de alguna entidad con un mensaje en específico sin que esto implique necesariamente que el receptor pueda conocer el contenido del mensaje. Como su nombre lo indica las firmas duales son utilizadas cuando dos mensajes relacionados deben ser enviados a dos entidades diferentes.

Función hash: Técnica criptográfica conocida como compendio de mensaje, funciones hash o transformaciones unidireccionales. Estas funciones reciben como entrada una cadena de longitud arbitraria y regresan como salida otra de longitud fija, frecuentemente de menor longitud que la original; a esta salida se le nombra valor hash

M

MD5: Función hash desarrollada por Ron Rivest en el Instituto Tecnológico de Massachusets (MIT) que recibe mensajes de longitud arbitraria y produce salidas de 128 bits

N

Navegador: Tipo de software conocido también como "browser", diseñado específicamente para visitar los documentos electrónicos que permiten que los datos, imágenes, etc. sean presentados en Internet.

Núnico: Cierta cantidad o número en cada mensaje que será usado únicamente para ese mensaje en particular

P

Prosumer: Figura del CE resultado de la mezcla de productor y consumidor, y del cual se pretende que sea capaz de diseñar en línea (mediante Internet) y de manera exacta el producto que desee, eligiendo su color, características técnicas, extras que requiera, etc.

R

RC2 y RC4: Algoritmos de cifrado de llave secreta desarrollados por RSA Security Inc. como alternativa a DES, y que en sus versiones exportables utilizan una llave de 40 bits.

RSA (Rivest Shamir Adleman): Algoritmo estándar de cifrado de llave pública desarrollado por Ron Rivest, Adi Shamir y Len Adleman en el MIT, y publicado por vez primera en 1978. RSA es el algoritmo de cifrado de llave pública más ampliamente aceptado e implementado hasta la fecha.

S

SEP (Sistema Electrónico de Pagos): Tipo de sistema que permite que el pago de alguna transacción se efectúe de forma electrónica

SGP (Sistema de Gestión de Pagos): Sistema de cómputo que durante una transacción electrónica de tipo comercial sirve de enlace entre el comerciante y la institución financiera de éste último.

SHA (Secure Hash Algorithm): Función hash basada en MD4 y desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) y publicado como un estándar federal para el procesamiento de información en 1993.

T

TEF: Transacción que consiste en mover dinero de una cuenta a otra de forma electrónica

TETC: Transacción Electrónica de Tipo Comercial

Texto cifrado: Conocido también como ciphertext se refiere a cualquier conjunto de datos que permanecen de forma legible.

Texto en claro: También llama plaintext, se refiere al mensaje original que se encuentra de forma legible, el cual es transformado, por medio de un proceso de cifrado o encripción, en un texto aparentemente aleatorio y sin sentido.

U

URL(Uniform Resource Locator): Es la dirección de algún recurso accesible en internet. El tipo de recurso depende del protocolo de aplicación en internet. De este modo si se utiliza el protocolo HTTP, los recursos pueden ser una página HTML, un archivo de imagen, etc.

X

X.509: Recomendación emitida por la CCITT como parte de la serie de recomendaciones X.500 que establece un formato y contenido particulares para los certificados digitales. X.509 está basada en el uso de criptografía de llave pública y firmas digitales. Este estándar no establece el uso de algún algoritmo pero recomienda a RSA.

REFERENCIAS

[1] W. Stallings, *Network And Interntwork Securiy Principles and Practice,* Prentice Hall,1995

[2] Charles F. Pfleeger, *Security in Computing* Prentice Hall,1997

[3] B. Schneier, *Applied Criptography,* John Willey & Sons Inc, 1994

[4] Roger Clarke, *Electronic Commerce Definitions,* Xamax Consultancy, http://www.anu.edu.au/people/Roger.Clarke/EC/ECDefns.html

[5] Ch. Kaufman, R. Perlman, M. Speciner, *Network Security Private Communication in a Public World,* Prentice Hall, 1995

[6] Frederic J. Cooper, *Implementing Internet Security,* Prentice Hall, 1995

[7] D. O' Mahony, M. Peirce, *Electronic Payment Systems,* Artech House,1997

[8] D. Tapscott, *La Economia Digital,* McGraw Hill, Mayo 1997

[9] N. Asokan, M. Steiner, M. Waidner, *The state of the Art in Electronic Payment Systems,* IEEE Computing Practices, Junio 1998

[10] B. Schneier, *Cryptography Second Edition: protocols, algorithms and source code in C,* John Willey And Sons, Inc., 1996

[11] L. Gong, T. Mark, A. Lomas, R. N. Needham y J.H. Saltzer, "Protecting Poorly chosen Secrets from Guessing Attacks", IEEE Journal on Selected Areas in Communications, Vol. 11, No.5, Junio, 1993

[12] Jamie Jaworski, *Java 1.2 Al descubierto,* Prentice Hall, Madrid 1999

[13] L. Hernández, "Protocolos Criptográficos de Autenticación e Intercambio de Llaves Basados en Passwords", Mayo 1999.