11

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

SEGURIDAD EN LOS SISTEMAS ELECTRONICOS DE PAGO EN EL COMERCIO ELECTRONICO

TESIS PROFESIONAL QUE PARA OBTENER EL TITULO DE :
LICENCIADO EN INFORMATICA

PRESENTA:
PERLA CELENE MORALES MENDEZ

ASESOR:
Dr. RICARDO RIVERA SOLER

MEXICO, D.F. 2001

Agradecimientos y Dedicatorias

AGRADECIMIENTOS

A Dios:

Por permitirme la oportunidad de vivir.
Por permitirme concluir esta etapa de mi vida.

A mis padres Luis y Hortencia:

Por darme la vida.
Por el apoyo y comprensión que siempre me han brindado, gracias a que ellos siempre me han inyectado los ánimos de superación que me han orillado siempre a ser alguien mejor día con día.

A la UNAM:

Porque en ella he recibido mi formación profesional, humana, crítica y analítica de las cosas.
Por haberme dado la oportunidad de llegar a ser profesionista.

A mis amigos de carrera:

Porque ellos me enseñaron el significado de lo que es el trabajo en equipo y apoyo incondicional.

A mis profesores:

Si no fuera a todos los profesores que han participado en mi formación académica y profesional no hubiera podido realizar esta investigación, ya que gracias a ellos he obtenido las herramientas necesarias aplicadas en el mismo. Debo hacer un reconocimiento especial para mi asesor de tesis, profesor y amigo, el Dr. Ricardo Rivera Soler que me proporciono bases teóricas y metodológicas para la realización de este trabajo.

DEDICATORIAS

A mis hermanos Luis y Fabiola:

Dedico este trabajo, para demostrarles que con esfuerzo y dedicación se logran alcanzar los sueños.

A mis padres Luis y Hortencia:

Dedico este trabajo, como símbolo del fruto que han cosechado.

A mi abuelita Dolores:

Dedico este trabajo, porque gracias a ella sé que es el valor de la unidad y del trabajo.

A mi familia:

Dedico este esfuerzo a todas las personas que integran mi familia, gracias a que siempre me han apoyado y han confiado en mi , para la realización de mis metas.

Indice

INDÍCE

Introducción

INTRODUCCION

Los cambios constantes en la tecnología y por ende el rápido crecimiento de Internet, ha dado lugar a que las empresas tengan una mayor cobertura de mercados nacionales e internacionales en un menor tiempo posible y se puedan realizar transacciones comerciales y de negocios por Internet, en las cuales no solo se intercambian bienes y servicios, también se da la posibilidad al intercambio de información, este tipo de intercambio comercial en Internet es denominado comercio electrónico (e-comerce) Por lo mismo, que el e-commerce va dirigido a grandes mercados, existen una serie de aspectos que se deben cuidar con respecto a la seguridad de realizar una compra por Internet. Uno de ellos, es como lograr pagos de manera eficaz y confiable.

El presente trabajo de investigación surge como una inquietud por tratar de probar el funcionamiento y la seguridad de los sistemas de pago electrónico, los posibles riesgos, los problemas que se derivan de éstos y ver como estos problemas influyen para el uso moderado del comercio electrónico, así como, introducir en el tema principalmente a las personas que se dedican al e-commerce o a los interesados en la seguridad de los sistemas de pago electrónico.

Hago un pequeño compendio de algunos tópicos introductorios del tema aquí tratado, éstos son: como se realiza una compra en Internet, las inseguridades que se derivan del comercio electrónico, conceptos fundamentales de criptografía, el funcionamiento, seguridad, entre otros de los primeros sistemas electrónicos de pago, que se usaron. El contenido de cada uno de los capítulos incluidos en la investigación, es.

Capítulo1. Marco Problemático. En este capítulo se definió el problema de la investigación, se da una hipótesis preliminar y se demarca el alcance del fenómeno a estudiar, así como, se presentan los cuestionarios elaborados y los resultados obtenidos de su aplicación a personas conocedoras principalmente de e-commerce y seguridad. Estos resultados ayudaron a reforzar la definición del problema y la hipótesis.

Capítulo 2. Marco Teórico. Se presentan las referencias bibliográficas, hemerográficas, URL's, etc., de todos los documentos consultados durante la investigación, y se da un breve resumen del contenido de cada uno de ellos.

Capítulo 3. Marco Conceptual. Contiene información referente a conceptos fundamentales de e-commerce, criptografía, sistemas de pago tradicionales, pero principalmente está enfocado a cada uno de los sistemas de pago electrónicos pioneros en el comercio electrónico, en su funcionamiento, seguridad y otros aspectos.

Capítulo 4. Marco Metodológico. Muestra la investigación de campo realizada por medio de aplicación de cuestionarios a personas expertas en el tema, los resultados obtenidos sirven para reforzar la comprobación de la hipótesis junto con la información obtenida a lo largo de la investigación

Capítulo 5. Marco Instrumental. En este capítulo se proponen algunas actividades que realizaré para continuar la difusión del tema del trabajo de investigación

Conclusiones. Aquí se encuentran las conclusiones obtenidas del trabajo de investigación en general

Anexo 1. Smart Cards (Tarjetas Inteligentes). Se presenta información básica sobre las tarjetas inteligentes, ventajas y desventajas, en que aplicaciones se utilizan, algunos aspectos de seguridad y amenazas, y un concepto del futuro que les depara ha este tipo de dispositivo en el mundo de las transacciones electrónicas

Marco Problemático

SEGURIDAD EN LOS SISTEMAS ELECTRÓNICOS DE PAGO EN EL COMERCIO ELECTRÓNICO

I. MARCO PROBLEMÁTICO

1. ANTECEDENTES

Internet se ha expandido desde un acceso limitado a redes académicas y de investigación, con multipropósitos en el medio electrónico. En suma a los usos educacionales y de investigación, este ha llegado a ser un medio popular para elegir comunicaciones, publicidad y, con la ayuda del World Wide Web, para hacer negocios.

Por tal motivo, en estos tiempos cada vez es más la gente que tiene posibilidades de entrar a Internet, por lo que se está convirtiendo en un medio de difusión masiva de entretenimiento y conocimientos. Debido a su gran aceptación, los servicios que ofrece Internet también crecen poco a poco, uno de ellos se enfoca al mundo de las transacciones llamado comercio electrónico o e-commerce

Internet permite a este tipo de comercio el traspasar fronteras a nivel mundial, realizar transacciones de un país a otro, de día y de noche, en pocas palabras, se dirige a distintos mercados y economías a la vez, sin un límite de horario, cosa que ningún tipo de comercio había podido alcanzar, esto hace que se le denomine el comercio sin barreras.

En la actualidad muchas empresas tienen cada vez más el conocimiento del comercio electrónico, por lo cual, es mayor la demanda, debido a las razones antes mencionadas, se requiere que los sistemas de pago para cubrir las transacciones realizadas por este medio, sean seguras. Tales sistemas requieren de operaciones criptográficas bastante robustas y entendibles, que permitan de una manera sencilla ser manipulados por distintos tipos de usuarios, y que provean niveles de confianza que demuestren que la transacción fue procesada correctamente.

Por éstas razones, la seguridad en los sistemas de pago digital en el e-commerce es de gran importancia para que el mercado de compradores en Internet crezca cada vez más.

Hago la aclaración que en esta investigación utilizaré vocabulario en inglés, si algún término no es comprendido puede verificarlo en la parte de glosario, al igual que acrónimos y siglas utilizadas a lo largo de este trabajo

Esta tesis va dirigida a personas interesadas en el tema de la seguridad y del e-commerce, enfocándome a la seguridad en los sistemas de pago electrónico en las transacciones de e-commerce

2. IDENTIFICACIÓN DEL PROBLEMA

Los usuarios de e-commerce no confían en la seguridad de las transacciones comerciales realizadas en Internet, ni en los sistemas de pago electrónico. Aún existe el desconocimiento de estos sistemas y de la seguridad de información que proporcionan, por lo que muchas tiendas siguen manejando esquemas de pago que no tienen que ver con ninguna transacción electrónica, usan los métodos tradicionales, lo cual no permite que los sistemas de pago electrónico tengan una amplia difusión, y por lo tanto, se muestre que las transacciones realizadas en el e-commerce pueden ser seguras, y esto genere una mayor confianza en las personas

3. DEMARCACIÓN DEL FENÓMENO

Debido a la difusión mundial del e-commerce, no me es posible abarcar los aspectos mundiales del mismo, por lo que me enfocare a la seguridad en los sistemas de pago electrónico de uso más frecuente en la Ciudad de México, enfocándome sólo a la demostración de los sistemas de pago más comunes en Internet tomando en cuenta su seguridad, como realizan el proceso de la transacción y el porqué algunos de ellos pueden ser violados También doy a conocer aspectos fundamentales que se ven involucrados en las transacciones de e-commerce.

4. CONOCIMIENTO EMPÍRICO EN EL MEDIO

4.1Definición del Cuestionario

	PREGUNTA	RAZÓN DE SER	RESPUESTA
1.	¿Confía en las transacciones que se realizan por Internet?	Averiguar cuanta es la confiabilidad de la gente en las transacciones realizadas por Internet.	No
2.	¿Qué sistemas electrónicos de pago sabe que se usan en el comercio electrónico?	Confirmar si alguna de las personas entrevistadas, conocen alguno de los sistemas de pago.	➢ No, conozco ninguno ➢ Sólo sé que los pagos se realizan con el número de la tarjeta de crédito
3.	¿De estos sistemas de pago electrónico, a su criterio cuál es el más confiable?	Si conocen alguno de los sistemas de pago, saber cuanto es el grado de confianza en ellos.	No se.
4.	¿Conoce el funcionamiento de alguno de estos sistemas de pago electrónico?	Obtener información para saber cuantas de las personas entrevistadas, saben como se realizan este tipo de transacciones y así poder confirmar que muchas de ellas no tienen el conocimiento de que su transacción puede viajar segura	No
5	¿Sabe en qué basan su seguridad los sistemas de pago electrónico?	Conocer el grado de participación o información con que cuenta la persona entrevistada sobre la seguridad del comercio electrónico en Internet.	➢ No ➢ Si se basan en métodos criptográficos

	PREGUNTA	RAZÓN DE SER	RESPUESTA
6.	¿Alguna vez ha sabido o ha experimentado un fraude en una compra realizada por Internet?	Saber si la persona entrevistada se ha formado una opinión mala sobre la seguridad en los sistemas de pago a través de las experiencias de la demás gente, o por su propia experiencia	➢ Si he escuchado mucho sobre los fraudes en Internet, y por eso mismo no quisiera intentar realizar una compra. ➢ No nunca ➢ Si alguna vez sufrí de un fraude por Internet. ¿Cómo fue?
7	¿Cuáles son los problemas que considera no permiten la expansión del comercio electrónico?	Tener la opinión de las personas entrevistadas, de los diferentes problemas que no han permitido el crecimiento acelerado del comercio electrónico.	➢ Por el temor que infunden los fraudes. ➢ El desconocimiento de este tipo de negocio
8.	¿Cuáles son los problemas que considera que existen en la seguridad de los sistemas de pago en el comercio electrónico?	Analizar el grado de conocimiento que se tiene sobre la seguridad de los sistemas de pago	➢ El pensar que existe gente que puede violar la seguridad de un sistema de computo. ➢ La mala aplicación de métodos criptográficos ➢ No tener un algoritmo seguro. ➢ La seguridad de los canales de información no es la adecuada. ➢ No tener el equipo necesario para cubrir los aspectos de seguridad relacionados con el comercio electrónico ➢ Poner una tienda virtual y aplicar un sistema de pago sin tener la certeza de su funcionamiento.
9	¿En qué basaría la seguridad de un sistema de pago electrónico?	Saber si tiene conocimiento de como se maneja la seguridad en Internet	No sé
10	¿Sabe en que consiste la criptografía?	Verificar cuanto es el conocimiento que tienen sobre la implantación de seguridad en los sistemas de pago	No
11	¿De los métodos criptográficos existentes, cuáles son los mas robustos?	Si la persona entrevistada sabe que es la criptografía, tendrá conocimientos relacionados con el tema	➢ Sé de algunos métodos criptográficos como DES, RSA, IDEA ➢ No sé de ninguno

PREGUNTA	RAZÓN DE SER	RESPUESTA
12. ¿Conoce algunas empresas que manejen actualmente el comercio electrónico en México?	Saber si la persona entrevistada sabe de algunas empresas mexicanas que actualmente apliquen el comercio electrónico, para poder tener referencia de algunas y basarme en los esquemas de seguridad que manejan esas empresas.	➢ Si. (Se realiza otra pregunta ¿Cuáles?) ➢ No
13. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico en México y fue buena su experiencia?	Ver cuanto confío la gente en la transacción realizada a una compañía mexicana.	➢ Si he realizado y no fue muy buena mi experiencia. Otra pregunta ¿Por qué? ➢ No he realizado. Otra pregunta ¿Por qué?
14. ¿En qué estriba la inseguridad del comercio electrónico, en los procedimientos de la compraventa del producto o en la estructura del sistema de pago?	Averiguar a que atribuyen más el problema de la inseguridad en el comercio electrónico	No es muy confiable la estructura del sistema de pago
15. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico y fue buena su experiencia?	Ver cuanto confío la gente en la transacción realizada a una compañía de comercio electrónico	➢ Si he realizado y no fue muy buena mi experiencia. Otra pregunta ¿Por qué? ➢ No he realizado. Otra pregunta ¿Por qué?

4.2 Formato del Cuestionario

Seguridad en los Sistemas de Pago Electrónico en el E-commerce

Nombre _____ Empresa _____

Puesto _____ Teléfono _____

1. ¿Confía en las transacciones que se realizan por Internet?

   SI NO

   ¿Por qué?

2. ¿Qué sistemas electrónicos de pago sabe que se usan en el comercio electrónico?

3. ¿De estos sistemas de pago electrónico, a su criterio cuál es el más confiable?

4. ¿Conoce el funcionamiento de alguno de estos sistemas de pago electrónico?

   SI NO

   ¿Cuál?

5. ¿Sabe en qué basan su seguridad los sistemas de pago electrónico?

   SI NO

   ¿En qué?

6. ¿Alguna vez ha sabido o ha experimentado un fraude en una compra realizada por Internet?

   SI NO

En caso de que sí coméntelo.

7. ¿Cuáles son los problemas que considera no permiten la expansión del comercio electrónico?

No llega la mercancía a su destino. ( )
Se cometen fraudes. ( )
Desconfianza en las personas. ( )
Miedo al no saber de la existencia de los sistemas de pago ( )

Otros: _____

8. ¿Cuáles son los problemas que considera que existen en la seguridad de los sistemas de pago en el comercio electrónico?

Falta de conocimientos en los diversos sistemas de pago y en su implementación. ( )
Mal diseño de la tienda virtual. ( )
Mala implantación de la seguridad en el equipo en el cual se encuentra la tienda. ( )
Mal establecimiento de los procedimientos de entrega del producto. ( )

Otros: _____

9. ¿En qué basaría la seguridad de un sistema de pago electrónico?

Conocimiento de la tienda virtual. ( )
La implantación del sistema de pago. ( )
Buena elección del sistema de pago ( )
Implantación de la seguridad del hardware y del SO ( )
Uso de técnicas criptográficas. ( )
Buen establecimiento del procedimiento de compraventa. ( )
Arquitectura HW/ SW ( )

Otros: _____

10. ¿Sabe en qué consiste la criptografía?

SI **NO**

Mencione qué es

11. ¿De los métodos criptográficos existentes, cuáles son los más robustos?

12. ¿Conoce algunas empresas que manejen actualmente el comercio electrónico en México?

13. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico en México y fue buena su experiencia?

14. ¿En qué estriba la inseguridad del comercio electrónico, en los procedimientos de la compraventa del producto o en la estructura del sistema de pago?

15. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico y fue buena su experiencia?

4.3 Definición de las Personas a Entrevistar

Las personas a entrevistar tienen el conocimiento empínco sobre las compras en Internet, todas ellas tienen las bases de seguridad y conocimientos de algunos de los sistemas de pago electrónicos y protocolos usados comúnmente en Internet

1 Genny Marisol León Leal
Dirección General de Servicios de Cómputo Académico (DGSCA)

2 Jorge Ángel González Canchola
Unisys de México S.A de C V

3 Marcelo Rodríguez Elizalde
Dirección General de Servicios de Cómputo Académico (DGSCA)

4.4 Aplicación del Cuestionario y Recopilación

Aquí mostrare un compendio de los resultados obtenidos en cada pregunta. Las respuestas se clasifican en respuesta **Sí**, que es afirmativa; **No**, que da un resultado de negación; **No Sé**, que no se sabe a que se refiere y **No Ne.**, la persona no considera necesaria esa respuesta.

Personas entrevistadas	**Genny León Leal**				**Jorge González Canchola**				**Jose Marcelo Rodríquez**			
	Sí	**No**	**No Sé**	**No Ne.**	**Sí**	**No**	**No Sé**	**No Ne.**	**Sí**	**No**	**No Se**	**No Ne.**
1. ¿Confía en las transacciones que se realizan por Internet?		x				x				x		
¿Por qué?												
Existen huecos de seguridad	x				x							
Robo del número de tarjeta de crédito									x			
2. ¿Qué sistemas electrónicos de pago sabe que se usan en el comercio electrónico?												
Tarjeta de Crédito	x				x				x			
Deposito a cuentas del vendedor	x											
Tarjeta Inteligente	x											
Otros:												
3. ¿De estos sistemas de pago electrónico, a su criterio cuál es el más confiable?							x					
Depósito a cuenta bancaria	x								x			
Otros:												
4. ¿Conoce el funcionamiento de alguno de estos sistemas de pago electrónico?	x					x			x			
5. ¿Sabe en qué basan su seguridad los sistemas de pago electrónico?	x					x			x			
6. ¿Alguna vez ha sabido o ha experimentado un fraude en una compra realizada por Internet?		x			x					x		

Personas entrevistadas	Genny León Leal				Jorge González Canchola				Jose Marcelo Rodríquez			
	Si	No	No Se	No Ne.	Si	No	No Se	No Ne.	Si	No	No Se	No Ne.
7. ¿Cuáles son los problemas que considera no permiten la expansión del comercio electrónico?												
No llega la mercancia a su destino.		x			x				x			
Se cometen fraudes.	x				x				x			
Desconfianza en las personas	x				x				x			
Miedo al no saber de la existencia de los sistemas de pago	x				x					x		
8. ¿Cuáles son los problemas que considera que existen en la seguridad de los sistemas de pago en el comercio electrónico?												
Falta de conocimientos en los diversos sistemas de pago y en su implementación	x				x				x			
Mal diseño de la tienda virtual.	x				x				x			
Mala implantación de la seguridad en el equipo en el cual se encuentra la tienda.	x				x				x			
Mal establecimiento de los procedimientos de entrega del producto.		x			x				x			
9. ¿En qué basaría la seguridad de un sistema de pago electrónico?												
Conocimiento de la tienda virtual		x			x					x		
La implantación del sistema de pago.	x				x				x			
Buena elección del sistema de pago.	x				x				x			
Implantación de la seguridad del hardware y del SO	x				x				x			
Uso de técnicas criptográficas	x					x			x			
Buen establecimiento del procedimiento de compraventa		x			x				x			
Arquitectura HW/ SW	x					x				x		
10. ¿Sabe en qué consiste la criptografía?	x				x				x			
11. ¿De los métodos criptográficos existentes, cuáles son los más robustos?												
RSA									x			
IDEA							x		x			
DES		x					x					
TEA		x					x					

Personas entrevistadas	Genny León Leal				Jorge González Canchola				Jose Marcelo Rodriquez			
	Si	No	No Se	No Ne.	Si	No	No Se	No Ne.	Si	No	No Se	No Ne.
12. ¿Conoce algunas empresas que manejen actualmente el comercio electrónico en México?	x				x				x			
13. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico en México y fue buena su experiencia?		x				x				x		
14. ¿En qué estriba la inseguridad del comercio electrónico, en los procedimientos de la compraventa del producto o en la estructura del sistema de pago?												
Procedimiento de Compraventa		x				x				x		
Estructura del Sistema de Pago	x				x				x			
15. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico y fue buena su experiencia?		x				x				x		

4.5 Conclusión de cada Pregunta

1. ¿Confía en las transacciones que se realizan por Internet?

Ninguna de las personas entrevistadas confía en las transacciones que se realizan por Internet. Esto permite ver, que todavía se sigue dando la desconfianza de las personas en este tipo de transacciones. Unas de las razones que dieron son:

- Por la existencia de huecos de seguridad.
- Robos de números de tarjeta de crédito.

2. ¿Qué sistemas electrónicos de pago sabe que se usan en el comercio electrónico?

Al no mencionar ninguno de los sistemas de pago electrónico, observe que las personas tienen el conocimiento de que se realizan las transacciones en Internet por medio de tarjeta de crédito, cosa que es cierta, sin embargo, mencionan otros métodos como el depósito físico a una cuenta bancaria, y dicen que puede ser más fiable, y alguien hace referencia al uso de las tarjetas inteligentes Esto me da a notar que las personas saben los instrumentos por los cuales se realiza el pago, más no tienen un conocimiento real de que sistemas de pago electrónico existen.

3. ¿De estos sistemas de pago electrónico, a su criterio cuál es el más confiable?

La mayoría apunto que el sistema de pago, tomando en cuenta la pregunta anterior, en el que más se confía es el depósito físico a cuenta bancaria, y se hizo referencia que algunos no confiaban en el uso de las tarjetas de crédito en el e-commerce.

4. ¿Conoce el funcionamiento de alguno de estos sistemas de pago electrónico?

Se ve que las personas entrevistadas obviamente conocen el funcionamiento de un depósito físico, sin embargo no conocen el funcionamiento de un sistema de pago electrónico.

5. ¿Sabe en qué basan su seguridad los sistemas de pago electrónico?

No saben en que basa su seguridad un sistema de pago electrónico, de acuerdo a las respuestas anteriores, mencionan que el sistema de pago de depósito a una cuenta bancaria es seguro ya que se realiza la transacción de manera personal.

6. ¿Alguna vez ha sabido o ha experimentado un fraude en una compra realizada por Internet?

Supuestamente la mayoría no sabe si alguien ha experimentado un fraude en una compra realizada por Internet, solamente pocos se han enterado de fraudes y mencionan que la mercancía adquirida no llega al destino, o simplemente llega con fallas o en mal estado, y por lo tanto hacen que la gente se entere de los malos servicios que ofrecen las tiendas virtuales

7. ¿Cuáles son los problemas que considera no permiten la expansión del comercio electrónico?

En base a los puntos mostrados en el cuestionario se dan los siguientes resultados

- La mayoría de ellos piensan que la mercancía no llega al destino
- Todos coinciden en que se cometen fraudes
- Todos mantienen su desconfianza en este tipo de transacciones
- Observe que hay gente que tiene incertidumbre al desconocimiento de los sistemas de pago

También se hizo referencia, a que la gente piensa que el e-commerce es similar a las compras por televisión, en las cuales no se entregan los productos o simplemente se entrega algo que no pidió el cliente.

8. ¿Cuáles son los problemas que considera que existen en la seguridad de los sistemas de pago en el comercio electrónico?

Los problemas de seguridad que se mostraron en el cuestionario son los principalmente considerados que existen en el e-commerce:

- Todos coinciden en que si existen tiendas virtuales en las cuales no se tenían los conocimientos suficientes en los sistemas de pago y en su implementación, lo que ocasiona que gente externa pueda interceptar información importante.
- Dan la razón a que un mal diseño de la tienda virtual ocasiona problemas de seguridad.
- Si no se implantan buenos mecanismos de seguridad obviamente se coincidirá, en que una mala implementación de estos mecanismos ocasiona inseguridad.
- La mayoría coinciden que en el establecimiento del procedimiento, puede radicar la inseguridad.
- Algunas personas creen que obviamente como usuarios, no nos interesa tener conocimiento en los diversos sistemas de pago y en su implementación, pero otros creen que puede ser considerado como un problema si lo vemos desde el punto de vista de la persona que está poniendo la tienda.

9. ¿En qué basaría la seguridad de un sistema de pago electrónico?

Estas son algunos de los posibles aspectos a evaluar al momento de hablar de seguridad en el e-commerce

- Unos dicen que la seguridad del sistema de pago no se basa en el conocimiento de la tienda virtual, en ello tienen razón. Pero si es mala su implantación o simplemente su método de seguridad no es el adecuado, pueden darme la razón, es importante considerar este aspecto, porque entre más se tenga conocimiento de la tienda virtual, si es popular o simplemente si la persona ha escuchado buenos comentarios de ella, nos podemos dar cuenta que es un buen establecimiento y no podremos pensar en algún fraude, por el contrario si la hallamos al azar, puede ser que simplemente sea un muestra fantasma de una tienda en la cual habrá una persona obteniendo información de nosotros y puede realizar transacciones con esta información
- Coinciden en que exista una buena implantación del sistema de pago
- Coinciden en que el sistema de pago que se elija debe ser uno de los mejores para proteger la seguridad.
- Dicen que no importa como se encuentre la arquitectura para la seguridad del sistema de pago, sin embargo, es importante mencionar que si no es buena la arquitectura aunque exista una buena implantación habrá huecos de seguridad.

10. ¿Sabe en qué consiste la criptografía?

Todos tienen el conocimiento de que es la criptografía, más sin embargo ninguno la ha considerado para ingresarla como medio de seguridad en un sistema de pago electrónico Mencionan que es la ciencia o arte de ocultar información

11. ¿De los métodos criptográficos existentes, cuáles son los más robustos?

Se hacen referencia a algunos métodos criptográficos como IDEA, RSA, DES, TEA, de los cuales los más robustos de ellos son RSA e IDEA Se ve que no se tiene un conocimiento más amplio de que sistemas criptográficos son los comúnmente aplicados en los sistemas de pago

12. ¿Conoce algunas empresas que manejen actualmente el comercio electrónico en México?

Si conocen empresas que actualmente tienen su tienda virtual como Submarino, Samborns, Amazon, DeCompras, TheOne, PlazaClick, Porrua, Todito, Esmas, DeRemate, Electra, Ghandi, y dan algunos bancos como Banamex y Bancomer Se ve que si existe el conocimiento de las tiendas virtuales, y la mayoría de ellas

el método de pago que utilizan es el de tarjeta de crédito, y otras a parte de éste se basan en lo que son puntos (sistemas de lealtad), los sistemas de lealtad consisten en ir acumulando puntos y después de haber juntado cierta cantidad, son canjeados por artículos o valen cierta cantidad de dinero.

13. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico en México y fue buena su experiencia?

Ninguna de las personas entrevistadas ha realizado una compra en un establecimiento de e-commerce en México. Porque no confían en las compras con tarjeta de crédito.

14. ¿En qué estriba la inseguridad del comercio electrónico, en los procedimientos de la compraventa del producto o en la estructura del sistema de pago?

Ninguno cree que la inseguridad del comercio electrónico pueda darse en el procedimiento de compraventa, más sin embargo, si no se tiene bien establecido, lo que puede pasar es que no llegue al destino la mercancía solicitada y se les haya hecho el cargo o pierdan la información de la orden, pero todos coinciden en que estriba en la estructura del sistema de pago.

15. ¿Ha realizado alguna vez una compra con una empresa de comercio electrónico y fue buena su experiencia?

Ninguno realizo compras.

4.6 Conclusión General

En base a los resultados obtenidos en el cuestionario, podemos ver que la mayoría de las personas entrevistadas no confían aún en el e-commerce, y en su mayoría en las transacciones realizadas con tarjeta de crédito, que es el único sistema que conocen que exista en Internet. Por lo cual, existe el desconocimiento de todos los sistemas de pago porque mencionan en general el uso de la tarjeta, pero no mencionan un sistema de pago electrónico en concreto, nunca se menciona el uso del dinero y cheques electrónicos, ni tampoco los micropagos, por lo tal sí existe desconocimiento del tema. Se sabe que es la criptografía, pero ninguna de las personas entrevistadas la considera como un medio de seguridad. También pude observar, que nadie considera que un mal establecimiento del procedimiento a seguir en la transacción pueda producir inseguridad, más que nada en la entrega del producto, señalando que es más importante la estructura de un sistema de pago que el procedimiento. En México ya existen varias tiendas de e-commerce pero ninguna, ha sido utilizada para adquirir un producto

Por lo que pude ver casi nadie realiza compras en tiendas virtuales con tarjeta de crédito, ya que desconfían de su seguridad. Prefieren los depósitos físicos a una cuenta del vendedor de bienes o servicios

5. HIPÓTESIS

Causa: Mal establecimiento del procedimiento de compraventa
Efecto: Pérdida de la mercancía
Produce desconfianza al cliente en el sistema de pago
Fraudes en el comercio electrónico
No permite el crecimiento del comercio electrónico

Causa. Malos sistemas de seguridad en los sistemas de pago digital
Efecto. Fraudes en el comercio electrónico
Produce desconfianza a los usuarios.
No permite el crecimiento del comercio electrónico

Causa: Fraudes en el comercio electrónico
Efecto: Produce desconfianza a los usuarios.
No permite el crecimiento del comercio electrónico

Causa. Incertidumbre al no saber cómo funcionan los sistemas de pago y el comercio electrónico en general
Efecto. No permite el crecimiento del comercio electrónico

Causa: Falta de confianza, de que la información de pago esté viajando por un canal seguro
Efecto: No permite el crecimiento del comercio electrónico

De las diversas relaciones hipotéticas que anteceden he hecho una selección conceptual que dan origen a la que enseguida se presenta, y es la que determino como mi hipótesis definitiva

"Es frecuente que haya desconfianza e incertidumbre de las personas a realizar una compra en Internet, principalmente en la seguridad del medio por el cual se realiza el pago, en que la mercancía solicitada no llegue a su destino final y que se produzcan fraudes, dando lugar a que no se pueda dar crecimiento en el e-commerce".

6. MARCO JUSTIFICATORIO

6.1 Objetivos Personales

- Uno de los aspectos por los que llevaré a cabo este trabajo es con el fin de realizar una Tesis que es una de las opciones para poder obtener el grado de Licenciatura en Informática basada en el:

  Reglamento General de Exámenes.
  Capítulo IV – Exámenes Profesionales y de Grado.
  Artículos 18, 19, 20 y 21

- El tema de la segundad lo considero muy interesante al igual que el de comercio electrónico, por lo que el objetivo al mezclarlos, es el de poder desarrollarme en un futuro en algo relacionado en la seguridad en el comercio electrónico en mi país.

6.1 Objetivos Particulares - Generales

- Demostrar cuáles son los sistemas electrónicos de pago más confiables, para que este documento sirva como referencia, para mostrar cuál de estos es el más robusto, el más seguro, en pocas palabras, cual de estos sistemas es el que proporciona mayores ventajas dependiendo los resultados que se quieran obtener con cada uno de ellos
- Demostrar el porqué muchas veces se llegan a realizar fraudes con alguno de estos sistemas de pago, mostrando sus vulnerabilidades y si me es posible proponer algunos métodos de protección contra las vulnerabilidades de los mismos

- Probar una hipótesis útil para personas que quieren poner una tienda de e-commerce

Marco Teórico

II. MARCO TEÓRICO

Este capítulo se enfoca a realizar un breve resumen de los diferentes medios, que ocupe, para llevar a cabo la recopilación de información escrita, que me ayudo a la realización de mi investigación. El proceso de recopilación de información consistió en el acopio en libros, revistas, periódicos, Internet y eventos, de información referente al comercio electrónico en Internet, sistemas de pago actual y electrónicos, métodos criptográficos, información básica de Internet, y cierta información de lo implementado en sistemas de pago electrónicos en los sitios de comercio electrónico

1. LIBROS

1.1 Electronic Payment Systems

Título:	**Electronic Payment Systems**
Autor:	O'Mahony, Donal; Peirce, Michael; Tewari, Gitesh
Editorial:	Artech House
Edición:	Primera Edición en Inglés, Norwood, MA, 1997
ISBN:	0-89006-925-5 Libro adquirido en Amazon.com

1.1.1 Prefacio

Las técnicas para realizar pagos a través de la red, ha requerido de mucha investigación criptográfica, desde que más gente se conecta a Internet. Desde hace 3 años la investigación se enfoca al e-commerce (comercio electrónico), por lo que se han estado desarrollando diferentes sistemas de pago electrónico.

1.1.2 Capítulo 1. Motivación para el Pago Electrónico

Nos muestra como ha sido el desarrollo de Internet en los últimos 30 años y su influencia en el desarrollo de nuevas tecnologías, entre las cuales se encuentra el desarrollo del comercio electrónico, que permite el intercambio internacional de bienes y/o servicios, adquiridos por medio de sistemas de pago seguros que se realizan de manera electrónica a través de Internet.

1.1.3 Capítulo 2. Características de los Sistemas de Pago Actuales

Se mencionan algunos de los diferentes sistemas de pago que han existido en el mundo, y son

- Trueque Intercambio directo de bienes y/o servicios, por otros bienes y/o servicios
- Dinero o mercancía de intercambio (maíz, sal, oro) Artículos que tenían valor para efectuar los pagos.
- Notas de pago o lo que se llamaba mercancía estándar, que estaban respaldadas por depósitos de oro y plata sustentados por el emisor de la nota
- Pago en efectivo Tipo de pago simple y efectivo Es fácil transferirlo de un individuo a otro En forma de papel, es bastante portable y una gran cantidad puede ser cargada en un monedero o cartera. No hay transacciones que tengan un cargo cuando un pago es hecho, el cual hace que sea muy apropiado para transacciones con un bajo valor Éste es un método de pago favorito para las actividades criminales
- Pagos a través de bancos Las partes tiene su efectivo con un banco para ahorrarlo, esto llega a ser innecesario para una de las partes que retira notas en orden para hacer de un pago a otro. En vez, de que ellos puedan escribir un cheque, que es una orden a su banco para pagar la cantidad especificada a

nombre del tenedor. El tenedor puede colectar los fondos en el banco del pagador y cobrar el cheque. Alternativamente, el tenedor puede tener el cheque, así que los fondos son transferidos de la cuenta del pagador a la cuenta del tenedor.

- Pago con cheque. Si las partes tienen cuentas con bancos separados, el proceso es más complicado. El ciclo empieza cuando A presenta un cheque en pago a B. B aloja el cheque con su banco (banco colector), quien colecta los fondos en su nombre. En la mayoría de los casos, un crédito es hecho a la cuenta de B tan pronto como el cheque es alojado, pero inmediatamente los fondos son disponibles aunque no en todos los caso. Todos los cheques alojados con el banco B sobre el curso del día serán enviados al departamento de aclaración, donde ellos son ordenados por los bancos en los cuales fueron cobrados. El siguiente día, son llevados a la casa de aclaraciones, donde un grupo de bancos se juntan para intercambiar cheques. El cheque en cuestión será dado al banco A, y (usualmente) un día más tarde el banco A verificara que los fondos son disponibles para cubrir el cheque y una cuenta de débito de A por la suma indicada. Si los fondos no están disponibles, la firma en el cheque no es igual con la muestra, o algún otro problema ocurre, entonces el cheque debe ser regresado al banco colector junto con algunas indicaciones que no pudieron ser procesadas. El Banco A debe atender esto inmediatamente, para que no cometan algún tipo de fraude. Si los fondos están disponibles para cubrir el cheque, entonces el siguiente día los bancos que son parte del arreglo de aclaraciones calcularán cuanto deben a los demás bancos. Esta cantidad es saldada haciendo un crédito o débito de una cuenta especial usualmente mantenida por el banco central.
- Pago por giro o transferencia de crédito. Un giro es una instrucción del banco del pagador para transferir fondos al banco del tenedor. El procesamiento de un giro es similar al cheque, con la diferencia principal que la transacción no es iniciada si A no tiene fondos disponibles. Esto elimina alguna incertidumbre y costos extras, impuestos, por la necesidad del proceso de regresar las partidas. Es un proceso más fácil como conducto electrónico, desde que la corrección del proceso de pago no requiere ser enviado con la firma del documento a través del sistema de aclaraciones.
- Pagos Automáticos de la casa de aclaraciones (ACH - Automated Clearing House). Operan similar al papel de aclaración, excepto que las instrucciones de pago son en forma electrónica. Los bancos preparan cintas magnéticas de esas transacciones para que sean transportadas al ACH, ordenadas por el banco destino, y distribuido en muchos de los mismos caminos como el cheque y el giro.
- Servicios de transferencia alámbrica o telegráfica. El método ACH de efectuar pagos es ideal para transacciones de valores medio y bajos. Donde el valor de los pagos es considerablemente más alto, el nivel de riesgo se incrementa y la diferencia de procedimientos involucra más escrutinios que son requeridos. Esos pagos de valores más altos se refieren como transferencias alámbricas.
- Tarjetas de crédito. Diseñadas para realizar pagos en situaciones de renta. Esto significa que el pago puede sólo ser hecho por un tarjetahabiente a un vendedor, quien será registrado para aceptar los pagos usando la tarjeta. Las compañías de tarjetas no tratan con tarjetahabientes o vendedores. Un banco que emite tarjetas a los clientes es llamado banco emisor de tarjetas. Ellos registran a los tarjetahabientes, producen una tarjeta incorporada a la asociación de tarjetas, y operan una tarjeta de cuenta en la cual los pagos pueden ser cargados. Los vendedores quienes desean aceptar los pagos deben registrarse también con un banco. Es este caso, al banco se le refiere como el banco adquirente o simplemente el adquisitor. En un crédito basado en tarjetas de crédito, un vendedor prepara un voucher (comprobante) de venta, que contiene el número de la tarjeta del pagador, la cantidad del pago, la fecha y la descripción de los bienes. Dependiendo de una política, la transacción quizá necesita ser autorizada. Este involucra contactos y la operación de un centro de autorización por o en nombre del banco adquirente para ver si el pago puede seguir. Esto quizá simplemente involucra verificación, de que la tarjeta no aparezca en la lista negra de tarjetas, o quizá involucre una referencia al banco emisor de tarjetas para asegurar que los fondos son disponibles para cubrir el pago. Al final del día, el vendedor traerá los vouchers de vuelta al banco adquirente, el cual los aclara usando un sistema de aclaración, como los usados para los cheques y giros pero operado por o en nombre de la asociación de tarjetas. La cuenta del vendedor es acreditada, el tarjetahabiente es deudor y los detalles de la transacción aparecerán en el siguiente estado del mes.

1.1.4 Capítulo 3. Técnicas Criptográficas

Este capítulo nos habla de criptografía, que es el proceso de ocultar un mensaje (texto plano) se le llama encripción o cifrado y su resultado es el texto cifrado. El proceso en reversa (descifrado o decripción) toma el texto cifrado como entrada y regresa el texto plano original. Un algoritmo criptográfico, también llamado cifrador, es una función matemática usada para cifrar y descifrar. Todos los algoritmos modernos de cifrado usan una llave, denotada por K. El valor de esta llave afecta a las funciones de cifrado y descifrado.

Existen dos tipos de cifrados el simétrico y el asimétrico o de llave pública. El cifrado simétrico, implica que ambas partes, para que tengan una comunicación deben poseer una copia de una sola llave secreta conocida. Los que aquí se mencionan son DES, 3-DES, RC2, RC4, RC5 y Kerberos. El cifrado asimétrico o de llave pública. En la criptografía de llave pública, cada persona obtiene un par de llaves, llamadas llave pública y llave secreta. La llave pública es publicada y ampliamente distribuida mientras la llave privada nunca es revelada. La necesidad por el intercambio de la llave privada es eliminada, por lo que todas las comunicaciones sólo involucran a la llave pública. Nos menciona las funciones Hash o Message Digest (Resumen del Mensaje): Uno de sus objetivos es que el contenido del mensaje sea guardado confidencialmente de los intrusos, quienes no pueden descifrar el mensaje encriptado, y que, la integridad del mensaje es asegurada. Esta puede ser garantizada desde que el mensaje no puede ser alterado sino se tiene la llave.

1.1.5 Capítulo 4. Sistemas basados en Tarjeta de Crédito

Se enuncian métodos de pago en red utilizando tarjetas de crédito para lograr transferencias financieras por la adquisición de bienes en Internet. Los métodos más baratos y más simples son FV y CARI, que no utilizan la criptografía, el protocolo SSL utiliza métodos criptográficos sofisticados para asegurar la comunicación entre el vendedor y el cliente. Existen otros 3 métodos que también utilizan la criptografía y son CyberCash, iKP y SEPP, que contribuyeron al desarrollo del protocolo SET.

1.1.6 Capítulo 5. Cheques Electrónicos

Describe tres sistemas en los cuales las organizaciones bancarias pueden introducir sistemas de pago basados en cheques. Los sistemas NetBill y NetCheque difieren muy poco en su diseño y están enfocados a las aplicaciones de comercio electrónico, donde una parte actúa como un vendedor que ofrece bienes, mientras que el cheque electrónico FSTC es un sistema con propósitos más generales. El uso de hardware seguro dentro de la solución FSTC limita su usabilidad para compras en línea, hasta que el hardware lector de tarjetas llegue a ser más común en las estaciones de trabajo.

Una ventaja es que tiene aceptación con los consumidores. Ya que operan bajo nombres de grandes organizaciones bancarias o industrias bancarias, las cuales fomentan la confiabilidad entre los consumidores.

1.1.7 Capítulo 6. Sistemas de Pago de Dinero Electrónico

En el comercio convencional el pago en efectivo es el más demandado, por lo que el pago electrónico en efectivo será un sistema demandado, y es el medio electrónico más atractivo debido al anonimato que provee. Ecash y CAFÉ son sistemas que usan innovadoras técnicas de criptografía. NetCash nos muestra los requerimientos de anonimato.

A pesar de que Ecash se usa en un gran número de áreas a través del mundo, la banca tiene ya afiliados a un gran número de industrias. Se da su éxito porque proveen un anonimato total del medio de pago. El sistema CyberCoin no intenta proporcionar anonimato, sólo se concentra en proporcionar un sistema que sea lo

suficientemente ligero para poder ser usado en pequeñas transacciones Mondex, inicialmente provee anonimato, subsecuentemente promueve el mantenimiento de un rastro de auditoria limitada de las transacciones que toman lugar. Los detalles técnicos de EMV, que se basan en el trabajo de monederos electrónicos no están disponibles para el dominio público, utilizan tarjetas Visa cash así que esto implica que se proporciona anonimato.

1.1.8 Capítulo 7. Sistemas de Micropago

Estos sistemas se utilizan para cubrir cantidades de pagos menores a 5 dólares. PayWord minimiza los costos de comunicación para una transacción de pago. A diferencia de los sistemas Millicent, un corredor no tiene que ser contactado para un nuevo pago al vendedor, no hay alguna necesidad de intercambiar scrip o regresar uno sin pasar de un vendedor específico al corredor. Sin embargo, el esquema PayWord provee más oportunidades para usarse fraudulentamente que Millicent, especialmente si una llave secreta del usuario está comprometida.

Los Micropagos surgen en 1995. Millicent, ha sido diseñado específicamente para suministrar la nueva forma de pago, mientras otros tales como μ-iKP, ha sido diseñado como un agregado para un existente esquema de macropago. Hace el uso de alguna técnica criptográfica nueva, incluyendo el uso de los primero algoritmos hash para autenticar un mensaje y el uso de economías de escala en la emisión de monedas.

Los micropagos minimizan las comunicaciones necesarias durante una transacción, y reducen el número de cálculos intensivos en las operaciones de llave pública. Millicent no usa criptografía de llave pública, y es optimó para repetidos micropagos al mismo vendedor. Es de acceso distribuido para permitir que un pago sea validado, y se previene el doble gasto, sin tener que contactar a una tercera parte centralizada en línea durante una compra. Pagos tan bajos como de un centavo son factibles, parece ser uno de los mejores candidatos para los micropagos, su única desventaja es que para múltiples vendedores, debe impedir el tener contacto con un corredor para cada nueva parte o vendedor encontrados.

SubScrip también es optimizado para repetidos micropagos con el mismo vendedor Sin embargo usa un sistema de macropago para colocar una cuenta temporal en un vendedor forzando al usuario a gastar una cantidad adecuada en el vendedor para justificar este gasto Es más conveniente remplazar servicios de subscripción de corto tiempo o hacer micropagos para un vendedor visitado regularmente

El PayWord improvisa un Millicent y SubScrip, para remover la necesidad de contactar a una tercera parte cuando hacemos un pago a un nuevo vendedor. La necesidad de regresar alguna forma de cambio, como con Millicent y SubScrip, es también eliminada. Aquí una cuenta de usuario no es deducida hasta después del tiempo de compra. Esto provee mayor oportunidad para un fraude, desde que grandes cantidades de compras pueden ser hechas contra una cuenta con fondos insuficientes. El uso de certificados de usuario con operaciones de llave pública, también agrega algún costo computacional.

Los micropagos iKP son los únicos que ofrecen dos soluciones diferentes. una para pagos con el mismo vendedor y la otra para pagos únicos a diferentes vendedores Sin embargo, los requerimientos de una completa certificación jerárquica y el flujo de varios mensajes para una transacción, hacen que éste sea menos eficiente que otros sistemas.

MicroMint usa una nueva forma de identificación de dinero electrónico, para proveer un sistema optimizado de micropagos a diferentes vendedores. Mientras éste es el esquema más eficiente para hacer esos pagos inconexos, una pequeña escala de fraudes son posibles El doble gasto no está prevenido, aunque estos sean detectados después del hecho Combinado con altos requerimientos computacionales necesitara un corredor que emita las monedas, en un futuro cercano

1.1.9 Capítulo 8. Sistemas de Pago – Prospectos para el Futuro

Haciendo referencia al capítulo 2, la mayoría de los métodos de pago mencionados, tienen su contraparte en las técnicas de pago electrónico, y éstas han sido agrupadas en 4 grupos: tarjetas, cheques, dinero electrónico y micropagos

Se espera que como sucede en el comercio convencional, los usuarios requerirán un rango de métodos de pago con al menos un (y probablemente más) sistema que sea ampliamente soportado, en las transacciones de e-commerce

En el área de tarjetas (crédito, débito y cargo), la industria ha convergido en SET (Secure Electronic Transactions / Transacciones Electrónicas Seguras), como el método más eficiente para este tipo de pago Sistemas que no usan criptografía como First Virtual, quizá puedan seguir operando donde la infraestructura necesitada para SET no este disponible, si es que no desaparece.

En los cheques electrónicos, no se ha dado mucho desarrollo, la industria solamente se basa en esquemas simples, que envuelven pequeñas extensiones de sistemas de procesamiento de cheques basados en papel, por lo que es lento su crecimiento.

En el dinero electrónico se requieren de técnicas criptográficas que produzcan monedas electrónicas que puedan ser gastadas con anonimato. Ecash se usa poco, el foco de esto han sido los sistemas de monedero electrónico como Mondex y tarjetas EMV Cash. Que dependen del uso de tarjetas de chip, y sólo son usadas donde la tarjeta puede ser insertada en un lector de tarjetas del vendedor, o donde los pagadores tienen algún hardware que permita la lectura de la tarjeta dentro de su estación de trabajo, aunque su uso es muy poco.

Los micropagos tienen una ventaja, que son nuevos sistemas de pago que en el comercio de hoy no existen.

Si los métodos electrónicos suplieran el 1% de los pagos convencionales, representaría una industria mundial. Pero se cree que en poco tiempo esta cifra será rápidamente superada.

1.2 E-commerce Security

Título:	**E-commerce Security**
Autor:	O'Mahony, Donal; Peirce, Michael, Tewari, Gitesh
Editorial:	Artech House
Edición:	Primera Edición en Inglés, Norwood, MA, 1997
ISBN:	0-89006-925-5. Libro adquirido en Amazon.com

1.2.1 Prefacio

El comercio electrónico es un nuevo camino de atractivas actividades - interacción, trueque, y negociar con gente y negocios A pesar de sus orígenes DARPA fundó un proyecto de investigación, en las comunidades académicas, Internet ha demostrado ser un vehículo esencial de comercio El hecho es que el negocio se realiza on line sobre un medio bastante inseguro para incitar la actividad delictiva en Internet

Este libro contiene varias soluciones tecnológicas, para asegurar a los usuarios finales y negocios, la privacidad y confidencialidad en transacciones on line Examina que la seguridad más crítica, involucra a los usuarios y negocios que comprometen de todas formas el e-commerce En cualquier actividad on line, hay un número de componentes, desde el software cliente de un usuario al software servidor de la otra parte que ejecutará el manejo de las transacciones on line (correo, transferencia de archivo, login remoto, navegar en WEB, o tratados comerciales) Se ha mostrado que una falla en cualquiera de estos componentes, puede comprometer la integridad de la transacción entera Este libro empieza con la premisa de una liga débil en la cadena de

componentes, que manejan sesiones on line, puede comprometer la seguridad de la transacción y finalmente no puede determinar la confidencialidad de consumidores y negocios en el e-commerce En pocas palabras, trata de eliminar el miedo sobre las preocupaciones de seguridad en el e-commerce reemplazándolo con una discusión basada en los riesgos relevantes de las tecnologías actuales.

1.2.2 Capítulo 1. Daños en un Paradigma cambiante de Negocios

Da muchos casos de la vida real de fallas en uno o más de los componentes, que últimamente comprometen la seguridad. Esos ejemplos enfatizan el punto de los problemas de seguridad en el comercio electrónico que no son teóricos, y que actualmente ocurren en práctica. Menciona diferentes casos de compañías, las cuales incurrieron en estos problemas.

1.2.3 Capítulo 2. Contenido Mortal: Las Vulnerabilidades del Lado del Cliente

Discute los riesgos inherentes al software que utiliza el cliente, incluso en los browsers (navegadores), plug-ins, y el contenido de aplicaciones activas tales como applets de Java y controles ActiveX. Informa sobre los peligros del contenido activo en Internet, la importancia del contenido activo es que supera las limitaciones de HTML en el Web para hacer del Web un medio viable para todos los rangos de aplicaciones de negocio y entretenimiento. El contenido activo está incluido en todas partes de las páginas Web, a menudo sin el conocimiento de su presencia por los usuarios finales. Lo que hace al contenido activo peligroso, es que alguien que lo pone en una página Web tiene la habilidad de ejecutar programas en su máquina. Esto significa que alguien más puede acceder a sus archivos personales, alterar sus archivos, enviar datos sobre las conexiones de red, o depositar caballos de Troya, todos sin su conocimiento Discute otros problemas con clientes Web como se evidencia en algunas de las versiones liberadas de Netscape Navigator/Communicator y el Explorador de Internet de Microsoft. Además, discute las ramificaciones de seguridad (con ejemplos reales) de integración del desktop del browser del Web y el sistema operativo, así como la seguridad inherente al emisor en la tecnología.

Aunque la tecnología promete entregar el contenido en nuevos e innovadores logros, también reconoce el abuso potencial de la seguridad y la privacidad del usuario final. La tecnología está cambiando la manera en que recibimos nuestra información del Web. En lugar de solicitar datos desde el Web, tenemos la capacidad de hacerlo desde nuestras máquinas. La tecnología puede ser una manera sumamente eficaz de recibir actualizaciones de sitios Web o canales, personalizados a través de filtros personalizados. El uso de tecnología para entregar el contenido activo y las actualizaciones de software (esencialmente los ejecutables del programa), hacen que la transmisión de programas malévolos sea transparente

1.2.4 Capítulo 3. Asegurando la Transacción de Datos

Describe varios protocolos usados para asegurar la transacción de datos en aplicaciones de e-commerce. Actualmente, los usuarios finales y vendedores tienen una variedad de opciones para ser usadas en la aseguración de los datos del cliente al servidor Una apreciación global de varios protocolos de transacciones seguras, es que son ampliamente usados en computadoras personales y smart cards (tarjetas inteligentes), junto con una evaluación de sus fortalezas y debilidades. Es importante recordar, que la seguridad de transacción de datos protege a la información que es observada en tránsito por terceras partes desautorizadas Es decir, los datos no pueden leerse y no pueden ser interpretados por alguien que no tiene ningún privilegio comercial de los datos enviados por Internet. Es importante proporcionar privacidad en las transacciones. Pero, los protocolos de transacciones seguras, no mantendrán la seguridad para los sistemas al final del protocolo de transacción La seguridad proporcionada por estos protocolos puede ser completamente engañada si el final de la transacción es insegura

1.2.5 Capítulo 4. Asegurando el Servidor de Comercio

Se enfoca a debilidades en el software del servidor Web, usado para la administración de las transacciones de e-commerce. Este capitulo echa un vistazo a un aspecto pasado por alto de e-commerce: la seguridad del lado del servidor. Las fallas en cualquiera de los tres componentes básicos del servidor de comercio: el servidor Web, el software de la interfaz, y la base de datos pueden ser suficientes para permitir un acceso del intruso a la compañía y a datos sensitivos del cliente. Presenta vulnerabilidades en cada uno de estos componentes y métodos por asegurar. Resalta los problemas simples en configuración de servidores Web, que tienen un impacto grande en la seguridad del servidor. Además, la importancia para incluir la seguridad dentro del diseño del software y la necesidad para analizar la seguridad del software.

1.2.6 Capítulo 5. Cracks en la Fundación

Se enfoca a la seguridad de la máquina del servidor Web. El servidor Web, es normalmente un servidor de red que ofrece un host de servicios de red para Internet entre otros. Las vulnerabilidades en los servicios de red, incluyendo y más allá del propio servidor de Web, pueden ser puertos de entrada para los usuarios malvados de Internet. Pueden usarse las vulnerabilidades en este software, para desviar los mecanismos seguros (como el control de acceso a los servicios de la red) y configuraciones seguras de software del servidor Web, para violar la seguridad del servidor de comercio. En la mayoría de los sitios que ofrecen transacciones comerciales en el Web, los datos valiosos se guardan en bases de datos que residen detrás de los firewalls y del servidor de red. Los ataques de manejo de datos pueden aprovecharse de las debilidades en el software del servidor de red, para acceder al servidor de base de datos. Clasifica las vulnerabilidades del servidor de red en siete categorías que se han demostrado en la práctica. El capitulo muestra cómo las dos plataformas de servidores de red más populares encontraron soluciones a sus vulnerabilidades, Unix y Windows NT, según las siete categorías.

1.2.7 Capítulo 6. Asegurando el Futuro del e-commerce

Finalmente, este capítulo proporciona una visión en el futuro de la seguridad del e-commerce. El software usado en aplicaciones de e-commerce, seguirá el paradigma del software basado en componentes activamente promovido y desarrollado por compañías de software. El futuro de aplicaciones de e-commerce, se asegurara más rápidamente cuando la seguridad sea considerada durante el desarrollo y antes de la liberación. Discute técnicas para fortalecer y analizar los componentes de software que están debajo de las transacciones de e-commerce contra los ataques. El uso de certificados de seguridad para los componentes de software, se discuten como un acercamiento práctico para asegurar la confianza en la seguridad del e-commerce.

1.3 Inicie su Negocio en Web

Título:	**Inicie su Negocio en Web**
Autor:	Cook, David; Sellers, Debora
Editorial:	Prentice Hall
Edición:	Primera Edición, México, 1997
ISBN:	

1.3.1 Capítulo 7. Inicie su negocio en Web

En este capitulo se mencionan los por menores de colocar un negocio en el Web Como encontrar al mejor proveedor para el sitio Web de comercio electrónico y formas de trabajar con el mismo para beneficio de ambos

Muestra como manejar los beneficios y desventajas de usar ayuda externa, y lo que sus empleados necesitan conocer, así como las técnicas que se pueden usar para entrenar a los empleados con las computadoras e Internet.

1.3.2 Capítulo 18. Seguridad en Internet

En este capítulo se ven los distintos delitos que se cometen e Internet, así como se da la clasificación de las personas que cometen delitos en los sistemas de cómputo en Internet. Se mencionan los fraudes y robos, y se dan algunas de las recomendaciones de cómo se pueden evitar estos.

1.4 Internet en Acción

Título:	**Internet en Acción**
Autor:	Boizard Piwonka, Alicia; Pérez Arata, Miguel
Editorial:	McGraw Hill
Edición:	Primera Edición, Santiago, Chile, 1996
ISBN:	

1.4.1 Capítulo. Seguridad en Internet

Nos habla de varios aspectos de seguridad que debemos cuidar, muestra las diferencias entre los sistemas de pago tradicionales, y hace una relación con los sistemas de pago electrónicos que se utilizan en el comercio electrónico, estos son: First Virtual, CyberCash y Digicash. Habla de sus fortalezas, debilidades y su funcionamiento

1.5 Tarjetas de Crédito

Título:	**Tarjetas de Crédito**
Autor:	Simon, Julio A.
Editorial:	Abeledo-Pedot
Edición:	Primera Edición, Buenos Aires, Argentina, 1990
ISBN:	

1.5.1 Capítulo 1. Historia del Dinero

Este capítulo nos muestra como se fueron dando las primeras formas de intercambio de cosas (trueque), y como poco a poco los pueblos que se establecieron antes de Cristo fueron haciendo uso de lo que conocemos hoy en día como la moneda, desde como fueron realizadas, a como son hoy actualmente Como la moneda fue evolucionando a lo que fue la letra de cambio, el crédito, y por último a la tarjeta de crédito

1.5.2 Capítulo 2. Historia de la Tarjeta de Crédito

Aquí se menciona como inicio la tarjeta de crédito, primero surgió como tarjeta en la cual sólo se podía tener crédito o algunas preferencias en establecimientos, como hoteles, restaurantes, etc De ahí los bancos fueron los que decidieron sacar esta tarjeta de crédito para una localidad o región, y ésta puede ser válida en varios establecimientos afiliados al banco La tarjeta de crédito surge como sustituto de la moneda.

1.5.3 Capítulo 3. Ventajas E Inconvenientes de la Tarjeta de Crédito

Habla de las ventajas que tienen los titulares de las tarjetas de crédito, como el poder de adquirir algunas cosas sin necesidad de tener efectivo, y poco a poco se van pagando, las desventajas que esto puede acarrear es el gasto de dinero que difícilmente se podrá juntar. Las ventajas de los vendedores y los emisores de las tarjetas, radican en que pueden atraer más clientela y por lo tanto hacer que sientan los clientes fidelidad por la misma. Otras ventajas que acarrea son reducción de gastos en comisiones para vendedores, y para los emisores reducción de cargos de manejos de las cuentas de tarjetas de crédito y en las investigaciones, que se realizan para comprobar si el candidato a adquirir la tarjeta de crédito es digno de ella.

1.5.4 Capítulo 4. Clases de Tarjetas de Crédito

Se mencionan la clasificación de las tarjetas desde el punto de vista del autor, éstas se clasifican en tarjetas de crédito por: el crédito que conceden, el tipo de entidad emisora, el ámbito objetivo, ámbito territorial de validez y por el ámbito temporal.

1.6 Kit de Recursos de Intranet

Título:	**Kit de Recursos de Intranet**
Autor:	Ambegaonkar, Prakash
Editorial:	McGraw Hill
Edición:	Primera Edición, España, Madrid, 1997
ISBN:	

1.6.1 Capítulo. Seguridad en la Intranet

Este capítulo nos habla de cómo conseguir seguridad en Internet, primeramente dice que hay que entender los riesgos del entorno e identificar las vulnerabilidades de la red. Esta información se puede usar para crear políticas de seguridad, que deben incluir

- Derechos y responsabilidades de los usuarios
- Uso aceptable de la intranet y sus recursos
- Procedimientos para la seguridad y uso de las aplicaciones.
- Procedimientos para identificar e informar de los problemas y brechas de seguridad

1.7 Using SET for Secure Electronic Commerce

Título:	**Using SET for Secure Electronic Commerce**
Autor:	Drew, Grady N
Editorial:	Prentice Hall PTR
Edición:	Primera Edición, NJ
ISBN:	0-13-099715-3

1.7.1 Capítulo 1. Introducción a SET

Este capítulo nos da una breve introducción de la historia de SET y su funcionamiento básico, de las compras con SET y la transacción

1.7.2 Capítulo 2. Componentes de Software

Nos menciona los componentes de software que participan en SET la cartera, el servidor del vendedor, la autoridad certificadora (AC) y el gateway de pago, como funcionan y como llegan a completar juntos una transacción SET

1.7.3 Capítulo 4. Certificados y Certificación

Da una introducción a los certificados mencionando que su fortaleza es la autenticación, da la jerarquía de un certificado, da los tipos de certificado y sus formatos, como se revoca y se cancela un certificado, y el procedimiento de emisión de un certificado SET.

1.7.4 Capítulo 5. Mensajes de Pago SET

Da una explicación de los escenarios más comunes que se encuentran en los negocios como autorización hoy y captura después, autorización después y captura hoy, autorización hoy y captura después con la parte inversa para una nueva cantidad, división del embarque, pagos recurrentes y de instalación. Da una detallada descripción de todos los mensajes ocupados en una compra SET.

1.7.5 Capítulo 6. Adiciones y Extensiones del Protocolo SET

Se da un pequeño vistazo a la arquitectura básica de débito SET, la solución de smart cards con SET, algoritmos propuestos, un resumen de las opciones de pago Japonesas, y los elementos adicionales de SET en la versión 2.0.

2. TESIS

2.1 Mejoramiento de Transacciones y obtención de Servicios haciendo uso de Tarjetas Inteligentes

Titulo:	**Mejoramiento de Transacciones y obtención de Servicios haciendo uso de Tarjetas Inteligentes**
Autor:	Ayala Martínez, Adriana
Fecha:	
Carrera:	Lic. en Informática
Universidad:	UNAM- Facultad de contaduría y Administración (FCA)

El veloz desarrollo de la tecnología de cómputo y redes de computadoras está cambiando la forma en que se realizaban muchas transacciones, incluyendo aquellas de naturaleza comercial o financiera, permitiendo que éstas se puedan efectuar de forma electrónica. Estas nuevas posibilidades no han sido ignoradas por aquellas instituciones financieras, comerciales y de servicios que a través de la experiencia propia o de la competencia, están conscientes que incorporar nuevas tecnologías en sus procesos operativos puede representar una ventaja competitiva dentro de los esquemas de libre comercio, que tienen presencia a nivel mundial. He ahí la causa y la necesidad de generar nuevos esquemas, que permitan ofrecer a sus clientes o usuarios de la mejor forma posible, lo siguiente

a) Reduce el tiempo de las transacciones o procedimientos.
b) Garantizar al cliente, que los datos involucrados en una transacción o servicio, están protegidos contra la lectura, alteración, destrucción o falsificación por parte de personas o entidades ajenas o no autorizadas Entre estos datos se contemplan: importes monetarios o información financiera, números de identificación personal, datos del individuo, etc.
c) Asegurar al usuario que está efectuando la transacción o servicio con las entidades participantes de forma directa.

Estas observaciones, entre otras más, resultan de gran interés y rentabilidad, por lo que un gran número de instituciones y gobiernos del mundo entero apoyan de alguna forma al desarrollo de los esquemas que las proporcionen Debido a mejores técnicas, mejoras científicas y mejores equipos, hemos llegado a estar conscientes de varios contrastes severos, más y mejor información, mejores formas de procesarla claramente muestran nuestro entendimiento de la naturaleza y distribución de los recursos –físicos y humanos- de la Tierra La combinación general de dispositivos electrónicos, incluyendo microcomputadoras y una vasta red de comunicaciones, ahora es llamada Tecnología de Información. Esto es universalmente entendido para representar un tremendo –y aún cambiante impacto en la entera condición humana.

En este sentido, este trabajo pretende servir como punto de inicio en la creación de aplicaciones de tarjetas inteligentes, dando a conocer su concepto, sus antecedentes, los avances tecnológicos que adquiere al paso del tiempo, su plataforma de trabajo y la cobertura de servicios que se pueden manejar De ésta forma, se busca proporcionar al lector un acercamiento sencillo que sirva como base a la creación de aplicaciones con tarjetas inteligentes, a las organizaciones que les interese incursionar en el mercado de tarjetas chip.

2.2 Metodología y Herramientas para mantener y crear una Tienda Virtual en el Web

Título:	**Metodología y Herramientas para mantener y crear una Tienda Virtual en el Web**
Autor:	Macías Pérez, Patricia Elizabeth
Fecha:	2000
Carrera:	Lic. en Informática
Universidad:	UNAM- Facultad de contaduría y Administración (FCA)

El tema que se trata en la tesis es una manera de hacer negocios que simula a la vida real Es la versión electrónica o virtual del comercio como se lleva a cabo en la realidad. El comercio electrónico tiene varias modalidades el Intercambio Electrónico de Datos (EDI) entre grandes empresas, banca electrónica, telemarketing, comercio en el Web, y es precisamente el tópico más interesante por ser la simulación de una tienda o un centro comercial en Internet. La tecnología Web brinda la oportunidad de intercambiar información y acercar a las personas, por lo que es posible llevar a cabo transacciones electrónicas Una tienda virtual en el Web posee características especiales que las hacen atractivas Se pueden visualizar todo tipo de productos de una tienda de cualquier parte del mundo y a cualquier hora. La mayoría cuenta con tecnología para incluir, por ejemplo, un "vendedor de mostrador virtual", que aconseja sobre diferentes opciones de compra, se pueden simular muchas o la mayoría de las características y elementos que poseen las tiendas y centros comerciales reales, y he ahí su utilidad y atractivo. Se ven en las páginas de las tiendas virtuales en el Web, los "carritos de compra", los catálogos o mostradores virtuales de productos, los formularios y ordenes de compra, los libros de visita, información sobre el negocio, recomendaciones, retroalimentación de información, asistencia, etcétera. Por todo esto, la investigación se centro en lo qué es una tienda virtual, sus características, su tecnología, la metodología para crearla y las herramientas de software y hardware que se requieren para su creación y mantenimiento

3. REVISTAS

3.1 Comercio Electrónico en Latinoamérica

Nombre:	**Comercio Electrónico en Latinoamérica. Más allá de la Página Web**
Dir. Revista:	Presidente Sánchez-Jaimes, Jonathan
Domicilio:	Exchange Place Boston, MA 02109 Estados Unidos de América
Periodo Revisado:	Octubre 2000

Es un análisis realizado por The Boston Consulting Group y Visa International, donde documenta el éxito de numerosos segmentos del mercado de ventas por Internet en América Latina, y los dolores que resultan del crecimiento de la industria. Los sitios que venden al consumidor se expanden con rapidez, aunque las realidades del mercado obligan a muchas de ellas a modificar sus modelos de negocios.

La primera parte del informe, "Tamaño y Crecimiento del Mercado", ofrece una visión objetiva de las dimensiones y la forma del mercado. La segunda sección, "Más allá de la página Web", y la tercera, "Las empresas tradicionales hacen clic", analizan temas que pueden acelerar o bloquear esta industria de rápido desarrollo.

3.2 RED

Nombre:	**RED**
Dir. Revista:	Aldaco, Yolanda
Domicilio:	Boulevard Adolfo López Mateos 202, 3er. Piso Col. San Pedro de los Pinos. C P 01180 México, D F.
Periodo Revisado:	Agosto 1999, Diciembre 1999

Título:	**Monedero Electrónico: ¿El Dinero del Futuro?**
Autor:	Luna, David
Fecha:	Agosto 1999, Núm. 107

Habla de la incorporación de chips a las tarjetas plásticas convencionales como la telefónica, permite guardar valor monetario en ella, por lo que en un futuro no muy lejano, se tendrá la posibilidad de comprar una aspirina o un abrigo sin necesidad de pagar con dinero en efectivo

El "dinero digital", permitirá a los comerciantes minimizar sus costos de operación, puesto que no manejarán dinero en efectivo, ni realizarán tareas rutinarias y engorrosas como cortes de caja Por su parte, el usuario evitará cargar en su cartera o en sus bolsillos dinero en efectivo, lo que le proporcionará seguridad y bienestar

Título:	**Comercio Electrónico. Con un Paso Adelante**
Autor:	Revista Red
Fecha:	Diciembre 1999, Núm. 111

Comercio electrónico es cualquier forma de transacción comercial, en la cual las partes interactúan electrónicamente en lugar de realizar un intercambio por medio del contacto físico directo.

Permite a las empresas ser más eficientes y flexibles en sus operaciones internas, trabajar más estrechamente con sus suministradores y dar mejor respuesta a las necesidades y expectativas de sus clientes. Permite además seleccionar los mejores proveedores, sin tener en cuenta su localización geográfica, y vender en un mercado global.

Título:	**Extender el uso de Internet y ofrecer Servicios Sencillos: Factores para el Éxito del Comercio Electrónico**
Autor:	Burgani, Carlos
Fecha:	Diciembre 1999, Núm. 111

Este artículo trata de la situación del comercio electrónico de hoy en día, los niveles del comercio electrónico, como es apoyado el e-commerce por parte del gobierno y las universidades, y se va frenado su desarrollo por el back office. Da una serie de gráficas analizando cifras que arroja Internet.

3.3 BYTE

Nombre:	**BYTE MEXICO**
Dir. Revista:	Espinoza Ortega, Cesar H.
Domicilio:	Balboa 813 Col. Portales. C P 03300 México, D F
Periodo Revisado:	Junio 1996

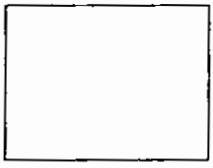
Título:	**Dinero Electrónico**
Autor:	Flohr, Udo
Fecha:	Junio 1999, Núm. 101

Habla del efectivo, cheques y cupones que se están volviendo digitales. Se dan los detalles de la moneda de curso legal del mañana. Se dan los puntos principales que deben cumplir alguno de los mecanismos de pago, antes descritos, en el mundo digital

4. SEMINARIOS

4.1 LatinCards 2000

Título: **LatinCards 2000**
Lugar: Sheraton María Isabel Hotel & Towers México, D.F.
Fecha: 28-30 de noviembre del 2000
Autor: Wagner, David, Schneier Bruce
Compañía: Terrapin
Material: Conferencias impresas. Grabaciones.



4.1.1 El Caso de Negocios de Tarjetas Inteligentes

Título: **El Caso de Negocios de Tarjetas Inteligentes**
Expositor: Cacho, Francisco
Compañía: Sub Director de Nuevas Tecnologías, Banco Bital, México Coordinador en la Migración a Estándar EMV, Asociación de Banqueros de México, México

Usar las tarjetas bancarias como vehículo para otras aplicaciones de tarjeta inteligente:

- Los grandes emisores de tarjetas inteligentes
- La migración bancaria de banda magnética a tarjeta inteligente
- Nuevas aplicaciones bancarias en tarjeta inteligente
- "Rentar" espacio en tarjetas bancarias para otro tipo de aplicaciones

4.1.2 El Mercado Global de Tarjetas Inteligentes: Estado del Mercado

Título: **El Mercado global de tarjetas inteligentes: Estado del mercado**
Expositor: Pagniez, Claire
Compañía: Research Business Manager, Smart Cards & E-Payment Technologies, Frost & Sullivan, Estados Unidos

- Un análisis del mercado global de tarjetas en términos de aplicaciones y porcentaje de mercado
- Un enfoque en la banca global, telecomunicaciones y transporte
- Un enfoque en América Latina por país y por aplicación
- Desafíos del mercado

4.1.3 Panel de Discusión: Abriendo la plataforma de tarjetas inteligentes para todos

Título: **Panel de Discusión: Abriendo la plataforma de tarjetas inteligentes para todos**
Panelistas: Cattaneo, Peter, Saunders, Keith, Ducshe, Mike
Compañía: Gerente de Desarrollo de Negocios para Java Cards, Sun Microsystems, Estados Unidos, Vicepresidente, Desarrollo de Negocios (Américas), MAOSCO, Microsoft

- Plataformas abiertas y aplicaciones múltiples
- La flexibilidad de operación entre tarjetas inteligentes
- Estándares de la industria. CEPS y EMV

4.1.4 Estrategias de la Migración a Tarjetas Inteligentes

Título:	**Estrategias de la Migración a Tarjetas Inteligentes**
Expositor:	Shuken, Randall
Compañía:	Vicepresidente, e-business y Tecnologías Emergentes para América Latina, Mastercard, Estados Unidos

Las principales motivaciones para la migración a tarjetas inteligentes en América Latina

- Prevención de fraude
- Reducción de costos
- Usando tarjetas inteligentes para diferenciar su empresa en el mercado y aumentar su base de clientes
- Creando la infraestructura para tarjetas inteligentes de multi-aplicaciones

4.1.5 La Transición de Banda Magnética a Chip

Título:	**La Transición de Banda Magnética a Chip**
Expositor:	Smith, John W
Compañía:	Director Regional, IFS International Inc., Estados Unidos

- Planificando su lanzamiento
- Ofreciendo aplicaciones múltiples al consumidor

4.1.6 Implementado Sistemas de Lealtad en Base de Tarjetas Inteligentes en América Latina El Mercado Masivo y "B to B"

Título:	**Implementado Sistemas de Lealtad en Base de Tarjetas Inteligentes en América Latina El Mercado Masivo y "B to B"**
Expositor:	Díaz, Víctor M.
Compañía:	Director General, Estrategias en Marketing electrónico SC, México

- Los requisitos para implementar una solución de lealtad - Equipo, software y tarjetas
- Analizando aplicaciones actuales y posibilidades para el futuro que unen el mundo "real" con el virtual

4.1.7 Caso Práctico. El Monedero Electrónico

Título:	**Banco Inbursa: La Implementación y Expansión del Mercado para un Monedero Electrónico**
Expositor:	Mesa Iturbide, Juan
Compañía:	Director de Tarjeta Inteligente, Banco Inbursa, México

- Estrategias implementadas para escoger una plataforma
- La importancia de una infraestructura moderna, segura y eficiente
- Cómo aprovechar de los beneficios de la tecnología

Título:	**El Uso de la Tarjeta de Compras en el Gobierno de Brasil**
Expositor:	Luiz de Almeida
Compañía:	Director Ejecutivo de Negocios, Visa do Brasil, Brasil

- Los beneficios de una tarjeta de compra
- Caracteristicas del producto Ideal para las compras pequeñas de empresas grandes y el gobierno
- Ejemplos de su éxito

4.1.8 Caso Práctico. Seguridad: El Camino Inteligente a Transacciones Seguras

Título:	**Biometría y Tarjetas Inteligentes**
Expositor:	Leiva, Jose
Compañía:	Director Desarrollo de Negocios, Keyware, Estados Unidos

- Los factores a favor y en contra de la descentralización de biometría en tarjetas inteligentes
- El uso de biometria y tarjetas inteligentes en las Américas
- Los obstáculos que enfrentan vendedores de tarjetas inteligentes al enfrentar información de biometria

Título:	**Aplicaciones Múltiples en el Contexto de Autenticación de Consumidores en Internet**
Expositor:	Dreifus, Henry
Compañía:	Presidente, Dreifus Associates Ltd, Estados Unidos

- Un análisis de Amex Blue
- DOD PKI tarjetas inteligentes
- PKI y la tarjeta Java

4.1.9 Caso Práctico. Tarjetas Inteligentes: Cambiando la Cara de Tarjetas de Lealtad

Título:	**Lealtad y Turismo: El Programa "Smiles Mileage" de Varig**
Expositor:	Cabral Ortiz, Amauri
Compañía:	Gerente General, Programa "Smiles", Varig Airlines, Brasil

- El lanzamiento del programa - Cómo suman las millas
- Metas de marketing Crecer y retener la base de clientes
- El valor de sumarse a otros programas de lealtad

Título:	**La Ventaja de Retener a los Clientes: Supermercados Egas y su Tarjeta de Lealtad**
Expositor:	Hidalgo, Carlos
Compañía:	Director Ejecutivo, Egas SA de CV, Chile

- Abrazando las ventajas de promoción y marketing
- Entendiendo y conociendo a sus clientes
- Premiando el comportamiento que quiere promover
- Cómo marketing de lealtad se relaciona con estrategias de marketing en comercio
- La reducción en costos que se produce al retener a los clientes

Título: **La Tarjeta de Lealtad de Amway Conavi**
Expositor: Avila, Esperanza
Compañía: Gerente, Amway, Colombia

- Un resumen del programa
- La administración de información sobre sus clientes en una tarjeta inteligente
- Un incremento en ventas: los resultados positivos de un sistema de premios basado en chip

4.1.10 Aplicaciones de Tarjetas Inteligentes

Título: **Pagos Electrónicos**
Expositor: Representante Senior de Giesecke & Devrient, México
Compañía: Senior de Giesecke & Devrient, México

- ¿Por qué Banca por Internet?
- Los fundamentos de Banca por Internet
- HBCI
- Resultados de las actividades de Banca por Internet

Título: **ePICNETZ: Entregando Valor Agregado a Servicios para el comerciante**
Expositor: González, Jairo
Compañía: Presidente de Tecnologías Emergentes, Hypercom Corporation, E U.

- Utilizando terminales de punto de ventas basados en Internet para entregar valor al cliente
- Ofreciendo aplicaciones múltiples para el comerciante
- Procesamiento seguro de pagos
- El lanzamiento de ePICNETZ

Título: **Caso Práctico: El uso de Tecnología de Tarjetas Inteligentes en Programas de Salud: La Experiencia de Unimed y la Solución Medicinet**
Expositor: Tadeu Mota, José, Mamede João
Compañía: Gerente General, Unimed de São Paulo, Brasil, Director, Medicinet, Brasil

- Un resumen de las ventajas de almacenar información médica en tarjetas inteligentes
- Fiscalizando la información y facturación automática
- ¿Cómo se implementó el programa? Factores para analizar antes de lanzar el programa
- Una introducción a la Farmacia Medicicard Farmacia - Compras farmacéuticos mediante la tarjeta inteligente

Título: **Caso Práctico: Programas de Lealtad Basadas en Tarjeta Inteligente**
Expositor: Representante Senior de Schlumberger, México
Compañía: Senior de Schlumberger, México

- Cómo conocer a sus clientes, uno por uno
- Campañas de promoción y Marketing 1 a 1
- Conociendo y prediciendo el comportamiento de sus clientes
- El valor de las tarjetas inteligentes en los programas de lealtad

Título:	**Tendencias e influencias económicas, demográficas y psicológicas: ¿Cómo afectan a la industria de tarjetas en América Latina?**
Expositor:	Almash, John
Compañía:	Presidente, Stratcom

- El impacto de mercados globales e indicadores económicos sobre el uso de tarjetas en América Latina
- Cómo el envejecimiento de la población, cambios demográficos cambiarán la industria de tarjetas y creará ventajas comparativas
- Aprenda sobre las necesidades de los consumidores y cómo satisfacerlas

4.1.11 Talleres Prácticos

Título:	**Módulo I. El diseño, desarrollo e implementación de tarjetas inteligentes con aplicaciones múltiples**
Expositor:	Dreifus, Henry
Compañía:	Presidente, Dreifus Associates Ltd, Estados Unidos

Este taller práctico ofreció una mirada analitica de esta labor al estudiar un caso real de éxito de una implementación de aplicaciones múltiples. Los asistentes pudieron sugerir casos hipotéticos que después fueron analizados y discutidos según los principios estándares de análisis presentados en el taller.

- Estándares y arquitectura de tarjetas inteligentes
- Sistemas de operación de tarjetas inteligentes
- Diseño y desarrollo de aplicaciones de tarjetas inteligentes
- Herramientas de desarrollo

Título:	**Módulo II. Tarjetas Inteligentes y un nuevo estilo de marketing: Entregando una nueva forma a una idea antigua**
Expositor:	Almash, John
Compañía:	Presidente, Stratcom

Este taller ofrecía un resumen de las tendencias económicas, demográficas y psicológicas y su influencia en la implementación de tarjetas inteligentes en América Latina. Un modelo de competencia y plan de negocios se desarrollaron. El taller parte de la base de un análisis del comportamiento del consumidor junto con fundamentos de negocios con un resumen de los efectos de marketing Puntos de énfasis incluirán precios, desarrollo de producto, promoción y gestión del canal de negocios. Un resumen detallado de publicidad y marketing analizará puntos como el establecimiento de la marca, correo directo, publicidad por televisión y medios escritos El taller le ayudará a integrar su publicidad en línea con su trabajo en medios tradicionales para optimizar la adquisición, uso, retención y activación de tarjetas Un resumen detallado de publicidad en línea tocará puntos como la banca electrónica, campañas de email marketing, publicidad de banners, meta-tagging, navegación, patrocinios y trabajo para aumentar el tráfico a su sitio de web.

5. URL (Páginas WEB)

5.1 First Virtual, the "Green Commerce" Model

Título:	**First Virtual, the "Green Commerce" Model**
Autor:	Standtke, Ronny
Compañía:	Faculty of Computer Science
URL:	http://www.niksula.cs.hut.fi/~ronnys/fv.html
Versión:	1.00, 28 noviembre,1996

En 1994 First Virtual introduce un sistema de pago en Internet, el cual permite vender la información de productos. Esto difiere en muchos aspectos de los otros enfoques del comercio electrónico en Internet. No confía en la encripción y tiene muy bajo costo de entrada. El sistema de pago First Virtual es construido en la cima de los protocolos preexistentes en Internet y basa su seguridad en contestaciones de e-mails.

5.2 RFC 1898. CyberCash Credit Card Protocol Version 0.8.

Título:	**RFC 1898. CyberCash Credit Card Protocol Version 0.8.**
Autor:	Eastkle, D.; Boesch, B ; Crocker, S ; Yesil, M
Compañía:	CyberCash
URL:	http://www.cis.ohio-state.edu/htbin/rfc/rfc1898.html
Versión:	0.8, febrero,1996

CyberCash está desarrollando un sistema de pagos general para uso en Internet La estructura y los protocolos de comunicación de la versión 0.8 son descritos en este documento. Esta versión sólo incluye pagos de tarjetas de crédito Se planean capacidades adicionales por las versiones futuras

Este documento cubre sólo el sistema actual de CyberCash que es uno de los pocos sistemas operacionales en el área que rápidamente han evolucionando a Pagos en Internet. CyberCash se compromete al desarrollo extenso de su sistema, y a la cooperación con las organizaciones del IETF y otros estándares.

5.3 The SSL Protocol

Título:	**The SSL Protocol (Internet Draft)**
Autor:	Hickman, Kipp E.B.
Compañía:	Netscape Communications Corp.
URL:	http://home.netscape.com/eng/security/SSL_2.html
Versión:	5.0, 9 Febrero, 1995

En este documento se especifico el protocolo Secure Sockets Layer (SSL) la manera de la que esta compuesto y su funcionamiento, es un protocolo que provee seguridad sobre Internet. Este protocolo permite que las aplicaciones cliente/servidor se comuniquen en un canal, el cual no pueda ser interceptado Siempre se requiere que los servidores sean autenticados y los clientes son opcionalmente autenticados

5.4 Introduction to SSL

Título:	**Introduction to SSL**
Autor:	
Compañía:	Netscape Communications Corp.
URL:	http //developer netscape.com/docs/manual/security/sslin/contents.htm
Versión:	

Introduce al protocolo Secure Sockets Layer. Protocolo desarrollado por Netscape, que ha sido aceptado en el World Wide Web para autenticar y encriptar las comunicaciones entre los clientes y servidores.

Intenta introducir a su funcionamiento a los administradores de servidores Netscape, pero la información que contiene es más usual para los desarrolladores de aplicaciones que soportan SSL.

5.5 The SSL Protocol

Título:	**The SSL Protocol (Internet Draft)**
Autor:	Freier, Alan O.; Karlton, Philip; Kocher, Paul C.
Compañía:	Netscape Communications Corp., Independent Colsultant
URL:	http://home.netscape.com/eng/ssl3/draft302.txt
Versión:	3.0, 18 noviembre, 1996

Se trata el protocolo SSL versión 3.0, protocolo de seguridad que provee la privacidad e las comunicaciones sobre Internet. Y cuida las comunicaciones entre las aplicaciones cliente/servidor en canales diseñados para prevenir intercepciones, alteraciones, o falsificación de mensajes

5.6 How SSL Works

Título:	**How SSL Works**
Autor:	
Compañía:	Netscape Communications Corp
URL:	http://developer.netscape.com/tech/security/ssl3/howitworks.html
Versión:	

Nos narra en forma breve cual es el funcionamiento de SSL, y como funciona la autenticación utilizando criptografía de llave pública.

5.7 The Secure HyperText Transfer Protocol

Título:	**The Secure HyperText Transfer Protocol (Internet Draft)**
Autor:	E. Rescorla, A. Schiffman,
Compañía:	Terisa Systems, Inc
URL:	http //www.terisa.com/shttp/current.txt
Versión:	1.2. Mayo 1996

Este documento describe la sintaxis y el funcionamiento de los mensajes de seguridad usados en el Protocolo de Transferencia de Hypertexto (HTTP – Hypertext Transfer Protocol) y S-HTTP, el cual forma parte de las bases para el World Wide Web El HTTP Seguro (S-HTTP – Secure Hypertext Transfer Protocol) provee

independientemente servicios de segundad aplicables para la confidencialidad, autenticidad, integridad y origen de no repudiabilidad de las transacciones

Este protocolo enfatiza una flexibilidad máxima en la elección de mecanismos de manejo de llaves, políticas de seguridad y algoritmos criptográficos que soportan la opción de negociación entre las partes para cada transacción.

5.8 Microsoft Corporation's PCT Protocol

Título:	**Microsoft Corporation's PCT Protocol (Internet Draft)**
Autor:	Benaloh, Josh; Lampson, Butler; Simon, Daniel; Spies, Terence; Yee, Bennet;
Compañía:	Microsoft Corp.
URL:	http://activex.adsp.or.jp/Japanese/Specs/pct.htm
Versión:	1.00, Octubre 1995

Este documento contiene la primera versión del protocolo de Tecnología de Comunicación Privada (PCT-Private Communication Technology), este protocolo de seguridad provee privacidad sobre las comunicaciones en Internet. Como SSL, protocolo que intenta prevenir los ataques en las comunicaciones de aplicaciones cliente/servidor, con la autenticación de los servidores y los clientes que son autenticados dependiendo si se habilite la opción en el servidor Este protocolo intenta corregir y mejorar partes contenidas en el protocolo SSL

5.9 Certificados Digitales

Título:	**Certificados Digitales**
Autor:	
Compañía:	
URL:	http://www.dat.etsit.upm.es/~mmonjas/cripto/08.html
Versión:	24 Octubre 1998

Este artículo habla de un certificado que es un documento al cual le da validez una autoridad certificadora por medio de la utilización de criptografía de llave pública. Da el ciclo de vida de las claves que consiste en la generación, distribución, emisión, expiración, retirada y terminación. Habla de la Infraestructura de Llave Pública.

5.10 Firmas Digitales

Título:	**Firmas Digitales**
Autor:	Puig de la Pena, Iván
Compañía:	Canal TI
URL:	http://www.timagazine.net/magazine/0497/firmas.cfm
Versión:	

El objetivo de este articulo es dar a conocer la firma digital y sus requerimientos También se explica que es una Función Hash En el Articulo Message Digest MD5 se puede observar el funcionamiento de una de las funciones Hash más utilizadas y famosas

5.11 An Introduction to Modern Cryptography

Título:	**Criptography**
Autor:	Cooper, Oli
Compañía:	
URL:	http://www.cs.bris.ac.uk/~cooper/crypto.html
Versión:	20 noviembre, 1997

Da una introducción del concepto de llaves de la criptografía moderna, y da una explicación más a detalle de cuatro de los más efectivos y populares algoritmos DES, IDEA, RSA y PGP. El concepto de cómo trabajan y la seguridad de esos algoritmos es considerada, y es comparada entre ellos.

5.12 Criptografía: Seguridad y Confidencialidad en las Redes.

Título:	**Criptografía: Seguridad y Confidencialidad en las Redes**
Autor:	Barceló Cánovas, Emma; Rodríguez, Alejandro
Compañía:	
URL:	http://aries.dif.um.es/typc/trabalum/1996-97/cripto/untitled.htm
Versión:	

Menciona los conceptos principales de la criptografía, así como de la seguridad en las capas de comunicación, nos habla de los tipos de cifrado, hace referencia al funcionamiento y debilidades de DES, IDEA, RSA y Kerberos, menciona el concepto de firma digital, habla también de algoritmos de seguridad en el correo electrónico PEM y PGP.

5.13 FSTC Electronic Check Project

Título:	**FSTC Electronic Check Project**
Autor:	Jaffe, Frank
Compañía:	BankBoston
URL:	http://www.fstc.org/projects/echeck/echeck2.html
Versión:	1995

Esta página nos relata como funcionan los cheques electrónicos, los beneficios que traen estos cheques con relación a los cheques de papel. Menciona cuatro flujos funcionales el de depósitos y aclaración, efectivo y transferencia, lockbox y el de transferencia de fondos, también hace referencia a su arquitectura técnica y las partes que se involucran en ella.

5.14 ¿Por qué es Lento el Desarrollo de Internet en Latinoamérica?

Título:	**¿Por qué es Lento el Desarrollo de Internet en Latinoamérica?**
Autor:	Benaloh, Josh, Lampson, Butler; Simon, Daniel, Spies, Terence, Yee, Bennet.
Compañía:	Cibernauta
URL:	http://www.ideal.es/cibernauta/
Versión:	1.00, 17 Octubre 2000

Muchos son los problemas que impiden un pleno desarrollo de Internet en el entorno latinoamericano

Comercio electrónico: En el terreno del comercio electrónico el B2B representa el 78% de las transacciones en Internet frente al 22% del B2C. Varios son los factores de tal diferencia.

1. El 60% de las empresas cuentan con acceso a Internet frente al 5% de los hogares particulares.
2. Baja implantación de las tarjetas de crédito en los usuarios.
3. La poca penetración de los ordenadores en los hogares. Por el contrario, la mayoría de las empresas en Latinoamérica cuenta con al menos un ordenador
4. Así como las empresas están familiarizadas con la red, no ocurre lo mismo con los consumidores que aún desconfían de Internet y la seguridad en sus transacciones.
5. La poca infraestructura en los canales de distribución. Las empresas de transporte ven más negocio en el B2B que en el B2C.
6. Los numerosos desarrollos de software para crear plataformas de comercio electrónico B2B ayuda a que las empresas se incorporen al e-business.

Además, existen otros motivos para la baja implantación del comercio electrónico

- Desconfianza en la seguridad de las transacciones.
- Miedo al fraude
- Limitado número de usuarios
- Poca visión a largo plazo. Los inversores quieren beneficios inmediatos
- Escasez de personal calificado en materia de tecnología
- Planteamientos locales (un país), nunca objetivos globales (Latinoamérica)

Problemas políticos: Muchos modelos políticos en Latinoamérica están basados en la intervención estatal. Esto quiere decir que las telecomunicaciones es un servicio ofrecido por el Estado y no por empresas privadas con lo cual la inversión en tecnología es mucho menor de lo requerido.

Problemas económicos: Las rentas per capita son muy bajas. Por poner un ejemplo, con EEUU la renta asciende al triple en el caso norteamericano. Además, existe una gran desigualdad en cuanto a la repartición de la riqueza. Tan sólo un 25% de la población cuenta con el 65% de la renta total con lo que el desequilibrio es muy grande. Esto repercute en que la penetración de internautas que coincide con ese 25% de gente con mayores posibilidades económicas y el número de usuarios se reduce enormemente.

Problemas sociales: Los latinoamericanos pagan su conexión por minutos, lo cual, encarece la navegación por Internet.

5.15 Vendedores Anónimos

Título:	**Vendedores Anónimos**
Autor:	Merchán, Iker
Compañía:	Cibernauta
URL:	http://www.ideal.es/cibernauta/
Versión:	1.00, 17 Octubre 2000

El auge del comercio electrónico genera desconfianza respecto a su seguridad

El comercio electrónico está en alza. A estas alturas, la afirmación parece una obviedad, pero, a la hora de tratar sus consecuencias, no hace sino acrecentar dudas y recelos. ¿Por qué? Muy sencillo: a diferencia de las transacciones tradicionales, los clientes de la red se ven obligados a tratar con vendedores de rostro anónimo y negocios cuya apariencia material desconocen, lo que genera una palpable desconfianza.

Ahora bien, aunque toda venta tiene sus riesgos, en un modo de hacer negocio tan novedoso como éste los usuarios pueden llegar a sentirse como los mercaderes que viajaban a América en busca de productos exóticos. Siempre con temor al ataque pirata o a vendedores sin escrúpulos. De nuevo, lo desconocido suscita temor, y más cuando el usuario ni siquiera es consciente de la ubicación física de la tienda donde ha adquirido la mercancía.

Así las cosas, uno de los recelos más extendidos entre los internautas se centra en las posibilidades de defensa que les ofrece la red, una vez que han sido víctimas de una irregularidad. Tendrían que actuar de la misma forma que lo harían en un comercio tradicional. Las empresas podemos demostrar que una compra se ha realizado enseñando los datos aportados por el propio usuario, junto al comprobante de recogida de su pedido. Si una firma fraudulenta carga más de lo debido en la tarjeta de crédito, ahí tendrá a la entidad financiera para verificar la transacción.

5.16 Guerra por el Mercado Latino de Internet

Título:	**Guerra por el Mercado Latino de Internet**
Autor:	Fernández, Alejandro
Compañía:	Cibernauta
URL:	http://www.ideal.es/cibernauta/
Versión:	1.00, 17 Octubre 2000

Las grandes empresas mundiales se preparan para atacar el 'apetitoso' mercado on line de Latinoamérica

4,8 millones de cibernautas que registraba la zona de América Latina en 1998 han crecido a unos 7,5 millones en 1999, y de acuerdo a las cifras de la firma de estudios Data Corp , estos sumarán 19 millones en el año 2003

Data Corp prevé que el comercio en Internet en esa área crecerá hasta los 8.000 millones de dólares en el 2003 desde los 167 millones de 1998.

5.17 Comercio Electrónico: el Futuro del Fraude

Título:	**Comercio Electrónico: el Futuro del Fraude**
Autor:	Schneier, Bruce
Compañía:	Criptograma / Kriptopolis
URL:	http://www.kriptopolis.com/criptograma/cg.html
Versión:	1.00, 15 noviembre, 1998

El fraude ha sido perpetrado contra todo sistema de comercio que el hombre haya inventado, desde las monedas de oro pasando por títulos de valores y cheques hasta llegar a las tarjetas de crédito. Los sistemas de comercio electrónico no serán diferentes; si es ahí donde está el dinero, ahí es donde estará el crimen. Las amenazas son exactamente las mismas.

Los sistemas de comercio electrónico no tienen que ser seguros, sino sólo mejores que los ya existentes. Desafortunadamente, existen características del comercio electrónico que contribuyen a que el fraude resulte más devastador: la facilidad de automatización y la velocidad de la propagación, estos elementos son comunes en un mundo electrónico.

La prevención del delito en el comercio electrónico es importante, pero es más importante ser capaz de detectarlo. Los sistemas de comercio electrónico deben ser capaces de detectar que el fraude ha tenido lugar y señalar al culpable. Y lo más importante, deben ser capaces de suministrar pruebas irrefutables que condenen al culpable en el juicio. En pocas palabras los sistemas actuales deben anticiparse a futuros ataques.

5.18 6 Reglas de Oro para Comprar en Internet

Título:	**6 Reglas de Oro para Comprar en Internet**
Autor:	Gómez, José Manuel
Compañía:	Criptograma / Kriptopolis
URL:	**http://www.kriptopolis.com/**
Versión:	1.00, 15 noviembre, 1998

En 1997 al menos el 90 por ciento de las personas conectadas a Internet temían que los datos de sus tarjetas de crédito, o los códigos de acceso a sus cuentas bancarias, puedan ser interceptados y utilizados para efectuarles cargos no deseados. O bien que el sitio donde efectúen su compra sea falso o fraudulento, y que el producto adquirido nunca llegue a su poder.

La utilización de Internet para transacciones comerciales es un fenómeno bastante reciente y con excelentes perspectivas de futuro, pero que necesita recorrer todavía un cierto trecho para convertirse en el entorno seguro que todos deseamos Aún así, ya es posible efectuar compras con bastante seguridad, siempre que observemos las sencillas medidas de precaución que comentamos en este artículo En cualquier caso, cierta perspectiva histórica puede ayudar a entender el estado actual de esta cuestión

5.19 First Virtual Abandona Su Sistema De Pagos Para Internet

Título:	**First Virtual Abandona Su Sistema De Pagos Para Internet**
Autor:	Gómez, José Manuel
Compañía:	Boletín 74 / Kriptopolis
URL:	**http://www.kriptopolis.com/**
Fecha:	11 septiembre, 1998

First Virtual Holdings Inc anunció el 20 de julio pasado, en nota de prensa, su intención de abandonar en un mes el sistema de pagos que le ha hecho popular en la Red.

FV fue una de las primeras empresas en ofrecer un esquema dirigido a efectuar, de forma segura, compras en Internet. El sistema FV proporcionaba a sus usuarios un identificativo personal (el famoso Virtual PIN) que había que utilizar en cada compra, en lugar del número real de tarjeta de crédito FV solicitaba confirmación e-mail al cliente antes de cargar el pago a su tarjeta.

La principal peculiaridad del sistema es que se basaba por completo en algo tan potencialmente inseguro como el correo electrónico, a pesar de lo cual no utilizaba en absoluto ningún tipo de cifrado Tal confianza en el protocolo del e-mail se debía sin duda al buen conocimiento del mismo que podían acreditar los fundadores de FV, gente que había creado en su día los protocolos MIME, POP, etc

Dado que en algunos medios se continúa considerando el sistema FV como plenamente vigente, Kriptópolis se dirigió a Rebecca Springer, directora financiera de First Virtual, quien nos confirmó que la empresa ha abandonado ya su esquema de pagos y está totalmente volcada en su nuevo proyecto IMP (Interactive Messaging Platform), basado en explotar al máximo las posibilidades del marketing personalizado vía e-mail. Al mismo tiempo, FV ha recomendado a sus 2.000 comercios adscritos y 60 000 clientes su migración al sistema CyberCash.

5.20 El Tema De La Semana: "Comercio Electrónico En Internet: ¿El Futuro Tendrá Que Esperar?"

Titulo:	**El Tema De La Semana: "Comercio Electrónico En Internet: ¿El Futuro Tendrá Que Esperar?"**
Autor:	Gómez, José Manuel
Compañía:	Boletín / Kriptopolis
URL:	**http://www.kriptopolis.com/**
Fecha:	17 julio, 1998

En este artículo se habla sobre una encuesta realizada por ITAA (Information Technology Association of America), en colaboración con Ernst&Young, a 105 empresas informáticas de primera línea. En la encuesta, se investigan los posibles factores de riesgo que pueden frenar el esperado desarrollo del comercio electrónico como factor vitalizador de la vida económica de los E.U. y del resto del mundo. Pues bien; la falta de confianza fue elegida como el primer obstáculo nada menos que por el 63% de los ejecutivos. El 45% señaló la falta de referencias claras a la hora de abordar el tema (por falta de acuerdo, educación o conocimiento de las empresas). El 36% señaló obstáculos relativos a los procedimientos de negocio ahora existentes. Diferentes porcentajes de ejecutivos apuntaron a otros factores diversos. Destacar que tan sólo un 1% no encontró ningún obstáculo a la prometida expansión ilimitada del comercio electrónico (ojo: tan sólo un 1%, en el país de las llamadas locales gratuitas y la pasión compulsiva por comprar).

Al profundizar en detalle en el principal obstáculo apuntado (la falta de confianza), un 60% señaló la preocupación por la pérdida de privacidad, un 56% a dificultades de autenticación entre clientes y empresas y otro 56% se inclinó por el miedo a la falta de seguridad de las transacciones (temor a que la infraestructura técnica no sea aún suficientemente robusta como para impedir ataques de intrusos). En general, todos estos factores le parecían muy importantes al 44%, moderadamente importantes al 42% y poco o nada importantes al 13%. Más adelante en el trabajo, al considerar las posibles barreras de tipo técnico, vuelve aparecer la preocupación por la seguridad en un 57% de encuestados. Curiosamente, el 45% de los ejecutivos consideran un impedimento grave las restricciones al uso de cifrado que impone el gobierno de EU

Las conclusiones del estudio son bastante claras:
1) El comercio electrónico se encuentra aún en estado relativamente naciente.
2) Existen aún muchos obstáculos que vencer para que el prometido boom del comercio electrónico sea -por fin- una realidad.
3) La mayoría de los inconvenientes afectan a cuestiones de confianza y seguridad.
4) Se requiere un abordaje pluridisciplinar de estos problemas, donde consumidores, empresas, industria y gobierno tendrán por delante muchos puntos que trabajar

5.21 Internet Keyed Payment Protocol (iKP)

Titulo:	**Internet Keyed Payment Protocol (iKP)**
Autor:	Linehan, M. ; Tsudik, G
Compañía:	IBM Research
URL:	**http://www.zurich.ibm.com/pub/sti/Security/extern/ecommerce/draft-tsudik-ikp-00.txt**
Fecha:	julio, 1995

IKP (Internet Keyed Payments Protocol) define la arquitectura para pagos seguros involucrando tres o más participantes. La arquitectura especifica un protocolo base, con un número de opciones que pueden ser seleccionadas para encontrar varios negocios o requerimientos de seguridad. Los pagos seguros significan que iKP emplea métodos criptográficos para minimizar los riesgos potenciales, concernientes a los pagos sobre Internet. Tres o más participantes significa que iKP direcciona escenarios, en los cuales compradores y

vendedores invocan a terceras partes tales como un sistema de tarjeta de crédito o bancos para lograr una transacción de pago

5.22 Electronic Payment Systems

Titulo:	**Electronic Payment Systems**
Autor:	Kalakota, Ravi
Compañía:	Addison-Wesley
URL:	**http://www.tc.msu.edu/tc462a/Chapter_6.html**
Fecha:	1997

Habla de los pagos electrónicos, estos son un intercambio financiero que toma lugar en línea entre compradores y vendedores. El contenido de este intercambio es usualmente una forma de instrumento financiero digital (números de tarjeta de crédito encriptados, cheques electrónicos o dinero digital) que es regresado por un banco, un intermediario, o por una persona que tenga poder legal

Esos tres factores simulan interés entre las instituciones financieras en los pagos electrónicos reducción de los costos tecnológicos, reducción de costos operacionales y de procesos, e incremento del comercio on line.

El problema crucial en el e-commerce gira alrededor de cómo los consumidores pagaran online para productos y servicios. Actualmente, los consumidores pueden ver un sin fin de productos y servicios ofrecidos por los vendedores en Internet pero no existe un sistema de pago seguro y consistente

5.23 Tik-100.501 Seminar on Network Security

Titulo:	**Practical Cryptosystems and their Strength**
Autor:	Frösen, Janne
Compañía:	Heinsinky University of Technology
URL:	**http://www.cs.hut.fi/%7Ejaf/netsec.html**
Fecha:	2.11.1995

Los criptosistemas prácticos incluyen varios algoritmos, de los cuáles muchos son usados actualmente en las aplicaciones. Algunos algoritmos son más seguros que otros, mientras que algunos ya se les han comprobado debilidades. Este documento da un breve resumen de algoritmos usados actualmente, y da más detalles de los que son más usados (DES y RSA), tratando de predecir su fortaleza en futuras aplicaciones.

5.24 Electronic Commerce Protocols and Competitive Strategies: Credit Card Transactions over the Internet

Titulo:	**Electronic Commerce Protocols and Competitive Strategies.**
Autor:	Reagle Jr, Joseph
Compañía:	Competition in Telecomunicaciones
URL:	**http://web.mit.edu/reagle/www/commerce/compete/final.html**
Fecha:	15.020

Este documento trata de direccionar la naturaleza del mercado naciente, y de los participantes y exploradores de la naturaleza estratégica y competitiva de los eventos recientes. En la segunda parte, se examinan algunas estadísticas y registros del Web, en la tercera se centra la atención en los protocolos que se han considerado estándares y se da una breve explicación de su funcionamiento. A continuación se presentan las

caracteristicas del mercado en los que se encuentran los protocolos y donde los competidores usan procesos estándar y protocolos múltiples para la ganancia competitiva

6. ARTICULOS

6.1 Analysis of the SSL 3.0 Protocol

Título: **Analysis of the SSL 3.0 Protocol**
Autor: Wagner, David; Schneier Bruce
Compañía: University of Califomia, Berkeley; Counterpane Systems
Versión:

Este artículo intenta proporcional lo práctico del protocolo SSL, la capa de aplicación y los mecanismos ampliamente aplicables para la seguridad de las comunicaciones cliente/servidor. Da un análisis técnico detallado de las fortalezas criptográficas del protocolo SSL 3 0. Un número de imperfecciones menores en el protocolo y varios de los protocolos nuevos activos en SSL; sin embargo, esos pueden ser fácilmente corregidos sin revisión de la estructura básica del protocolo.

6.2 Criptografía para Principiantes

Título: **Criptografía para Principiantes**
Autor: Angel Angel, José de Jesús
Compañía: SeguriData
Versión: 1.0

Este articulo tiene como propósito explicar algunas herramientas de seguridad informática, tratando de enfatizar la importancia de la criptografía, tratando de dar una explicación lo más sencillo posible.

El uso de técnicas criptográficas tiene como propósito prevenir algunas faltas de seguridad en un sistema computarizado. La seguridad en general debe de ser considerada como un aspecto de gran importancia en cualquier corporación que trabaje con sistemas computarizados. El hecho que gran parte de actividades humanas sea cada vez más dependiente de los sistemas computarizados hace que la seguridad juegue un papel importante.

En el reporte "Computer Crime Survey" del FBI, proporcionado por Secure Site E-News del 22 de mayo de 1999, de la compañía VeriSign, se dieron los siguientes datos

Se estudiaron 521 compañías de varias ramas de la industria y de diferentes tamaños. Estas actualmente están trabajando para que su sistema computarizado sea seguro.

El 61% de estas compañias ha tenido experiencias de pérdida debido al uso de no autorizado de su sistema computarizado
El 32 % de estas organizaciones están usando ahora métodos de identificación segura en su sitio de Internet.
El promedio de pérdida de robo o pérdida de información está sobre $1 2 M de dólares
El promedio de pérdida por sabotaje está sobre $1 1 M dólares
El 50% de todas las compañías reportaron abuso del uso de la red
El 94% de las organizaciones tiene actualmente un sitio en la Web.

A la pregunta ¿qué tipo de tecnologia de seguridad usa? Se contestó con lo siguiente

Se cuenta con un control en el acceso, el 89%.
Cuenta con archivos cifrados, el 59%.
Cuanta con sistema de passwords, el 59%.
Usa Firewalls, el 88%.
Una sistema de login cifrados, el 44%.
Usa smart cards, 37%.
Detención de intrusos, 40%.
Certificados digitales para la autenticación, 32%.

A la pregunta ¿Cuál es más frecuente origen de un ataque?
Un "hacker" independiente, un 74%.
Un competidor, un 53%.
Un empleado disgustado, un 86%.

¿Su organización provee servicio de comercio electrónico?
Sí, el 29%.

¿Su Web site ha tenido un acceso no autorizado en los últimos 12 meses?
Sí, un 18%.
No, un 44%.
No sabe un 38%.

Enseguida damos un reporte dado a conocer en unos cursos de criptografía industrial en Bélgica en junio de 1997. Donde se mide la frecuencia de incidentes de seguridad de la información relacionada con sus causas.

Frecuencia	Razón
50-60%	Errores debido a la inexperiencia, reacciones de pánico, mal uso,...
15-20%	Empleados disgustados, accidentes de mantenimiento,...
10-15%	Desastres naturales como inundaciones, incendios,...
3-5%	Causas externas: "hackers"

Otro aspecto importante a considerar es el crecimiento enorme que ha tenido la red Internet, algunos datos importantes son los proporcionados por Paul Van Oorschot de Entrust Technologies en una conferencia del ciclo The Mathematics of Public Key Cryptography en junio de 1999:

Se duplica el tráfico de Internet cada 100 días.
En enero de 1999 hubo 150 millones de personas en línea, 75 de ellas en USA.
El comercio sobre Internet se duplica cada año.
Podría llegar a $1 trillón de dólares lo comercializado en Internet en el año 2002.
A la radio le tomo 40 años, a la televisión 10 años para alcanzar 50 millones de usuarios a la red le ha tomado menos de 5

El diseñar una estrategia de seguridad depende en general mucho de la actividad que se esté desarrollando, sin embargo se pueden considerar los siguientes tres pasos generales: el primero crear una política global de seguridad, el segundo realizar un análisis de riesgos y el tercero aplicar las medidas correspondientes

Política global de seguridad: aquí se debe de establecer el estatus de la información para la empresa o la organización, debe de contener un objetivo general, la importancia de la tecnología de la información para la empresa, el periodo de validez de la política, los recursos con que se cuenta, objetivos específicos de la empresa. Debe de establecerse la calidad de la información que se maneja según su objetivo, esto quiere decir que se establezca cuando o para quien la información debe ser confidencial, cuando debe verificarse la integridad y cuando debe verificarse la autenticidad tanto de la información como de los usuarios

Análisis de riesgos: consiste en enumerar todo tipo de riesgos a los cuales está expuesta la información y las consecuencias, los posibles atacantes entre persona, empresas y dependencias de inteligencia, las posibles amenazas etc., enumerar todo tipo de posibles pérdidas, desde pérdidas directas como dinero, clientes, tiempo

etc., así como indirectas, créditos no obtenidos, pérdida de imagen, implicación en un litigio, pérdida de imagen, pérdida de confianza etcétera. El riesgo se puede calcular por la formula riesgo = probabilidad * pérdida, por ejemplo el riesgo de perder un contrato por robo de información confidencial es igual a la probabilidad de que ocurra el robo multiplicado por la perdida total en pesos de no hacer el contrato El riesgo de fraude en transacciones financieras es igual a la probabilidad de que ocurra el fraude por la perdida en pesos de que llegara ocurrir ese fraude. Si la probabilidad es muy pequeña el riesgo es menor, pero si la probabilidad es casi uno, el riesgo puede ser casi igual a la pérdida total. Si por otro lado la pérdida es menor aunque la probabilidad de que ocurra el evento sea muy grande tenemos un riesgo menor Por ejemplo la pérdida de una transacción de 300 pesos con una probabilidad muy grande de que ocurra al usar criptografía débil, el riesgo llega a ser menor por lo que depende de la politica de seguridad para que este riesgo se asuma

Medidas de seguridad: ésta parte la podemos plantear como la terminación de toda la estructura de seguridad de la información. Una vez planteada una politica de seguridad, o sea decir cuanto vale la información (en un análisis de riesgo), decir que tanto pierdo si le ocurre algo a mi información o que tanto se gana si está protegida, debemos de establecer las medidas para que cumpliendo con la politica de seguridad las pérdidas sean las menores posibles y que esto se transforme en ganancias, ya sean materiales o de imagen

Las posibles medidas que se pueden establecer se pueden dividir según la siguiente tabla:

Tipos	Protección Física	Medidas Técnicas	Medidas de Organización
Preventivas	PF	PT	PO
Detectivas	DF	DT	DO
Correctiva	CF	CT	CO

PF: guardias a la entrada del edificio, control en el proceso de entrada, protección al hardware, respaldo de datos, etc.
DF: monitor de vigilancia, detector de retardo, detector de movimiento, etc.
CF: respaldo de fuente de poder, etc.
PT: firewalls, criptografía, bitácora, etc.
DT: control de acceso lógico, sesión de autenticación, etc.
CT: programa antivirus, etc.
PO: cursos de actualización, organización de las claves, etc.
DO: monitoreo de auditoria, etc.
CO: respaldos automáticos, plan de incidentes (sanciones), etc.

En resumen, debemos mencionar que no existe un sistema computarizado que garantice al 100% la seguridad de la información, debido a la inmensa mayoría de diferentes formas con que se puede romper la seguridad de un sistema. Sin embargo, una buena planeación de la estrategia para dar seguridad a la información, puede resultar desde la salvación de una empresa hasta la obtención de grandes ganancias directas en pesos, o como ganancias indirectas mejorando la imagen y la seguridad de la empresa Uno de los objetivos principales de establecer una politica de seguridad, es el de reducir al mínimo los riegos posibles implementando adecuadamente las diferentes medidas de seguridad

6.3 NetCash: A Design for Practical Electronic Currency on the Internet

Título: **NetCash: A Design for Practical Electronic Currency on the Internet**
Autor: Medvinsky, Gennady, Neuman, Clifford B.
Compañía: Information Sciences Institute, University of Souther California
Versión: 1.0

NetCash es una estructura que soporta pagos electrónicos en tiempo real y provee anonimato sobre una red insegura Es diseñada para permitir nuevos tipos de servicios en Internet los cuales no han sido prácticos a la fecha de ausencia de seguridad, escalables, sistemas de pago anónimos potenciales.

Muestra un balance entre el anonimato incondicional de las monedas electrónicas, e instrumentos análogos como los cheques, que son más escalables que identifican a las principales partes en una transacción. Provee una estructura de que un protocolo de monedas electrónicas puede ser integrado con escalabilidad, pero no con anonimato, la infraestructura de los bancos electrónicos ha sido propuesta para la rutina de las transacciones.

Por lo antenor, este documento presenta la estructura de transacciones electrónicas que combinan los beneficios del anonimato con la escalabilidad de los protocolos en pago online no anónimos. Muestra los requerimientos de un sistema electrónico de pago, seguido de cómo funcionan.

6.4 Requirements for Network Payment: The NetCheque™ Perspective

Título:	**Requirements for Network Payment: The NetCheque™ Perspective**
Autor:	Medvinsky, Gennady; Neuman, Clifford B.
Compañía:	Information Sciences Institute, University of Souther California
Versión:	1.0

Los métodos seguros de pago son necesitados desde antes de que Internet se usara con fines comerciales. Recientemente proponer e implementar sistemas de pago sigue tres modelos: moneda electrónica, débito-crédito / transacciones seguras con tarjeta de crédito Tales servicios de pago tienen distintas fortalezas y debilidades con respecto a los requerimientos de seguridad, confiabilidad, escalabilidad, anonimato, aceptabilidad, base del cliente, flexibilidad, convertibilidad, eficiencia, fácil integración con aplicaciones, y fácil de usar NetCheque es un sistema basado en el modelo de transacciones de débito/crédito, son descritas en este documento sus fortalezas al respecto de los requerimientos mencionados.

Marco Conceptual

III. MARCO CONCEPTUAL

1. ANTECEDENTES

1.1 Origen

1.1.1 Comercio Electrónico (e-commerce)

Hoy en día, gran parte de la actividad comercial ha podido transformarse gracias a las redes de computadoras como Internet, esta transformación facilita hacer transacciones en cualquier momento, de cualquier lugar del mundo. Todo lo que está alrededor de esta nueva forma de hacer negocios es lo que se ha llamado comercio electrónico, sin duda la gran variedad de actividades que giraban alrededor del que hacer comercial se ha tenido que juntar con las nuevas técnicas cibernéticas. Así hoy tanto un comerciante, un banquero, un abogado o una matemático puede hablar de comercio electrónico enfocándose a la parte que le corresponde.

Existen diferentes niveles de hacer comercio electrónico, por lo que mencionaremos las actividades principales de dos tipos de comercio elèctronico conocidos como B2C (Business to Consumer) Negocio a Consumidor y las de B2B (Business to Business) Negocio a Negocio

Actividades B2C:

- Búsqueda de la información del producto.
- Ordenes de productos.
- Pago por bienes y servicios.
- Proveer en línea el servicio a los clientes

Actividades B2B

- Mensajes y correos electrónicos internos.
- Publicar en línea documentos corporativos.
- Búsqueda en línea de documentos, proyectos y conocimientos.
- Distribución crítica y a tiempo de información a los empleados.
- Manejar finanzas corporativas y sistemas personales.
- Administración de logísticas de manufactura.
- Suplir cadenas de administración de inventarios, distribución y almacenamiento
- Enviar procesamiento de información/reportes de ordenes para proveedores y clientes.
- Darle un seguimiento a las ordenes y a los embarques

En este trabajo más que nada me enfoco al comercio electrónico B2C, que consiste en comprar o vender usando una conexión por Internet en lugar de ir a la tienda La forma de hacer esto es muy similar a lo que tradicionalmente se hace, por ejemplo en la tienda uno entra al establecimiento, de forma electrónica se prende la computadora y una ves conectado a Internet entra a la página del negocio, enseguida un comprador revisa los productos que posiblemente compre y los coloca en una carrito, de la misma forma en la computadora se navega por la página del negocio y con el browser se revisan los productos que èste vende, al escoger estos se colocan en un carrito virtual, que no es nada más que un archivo del usuario Una vez elegido bien los productos de compra se pasan a la caja, donde se elige un sistema de pago y se facturan los productos al comprador De forma similar en la computadora se pueden borrar productos que no se quieren comprar o añadir nuevos, una vez elegidos estos se procede a una parte de la página que toma los datos y solicita el método de pago, generalmente se lleva a cabo con tarjeta de crédito

En la parte tradicional de comprar al pagar en la caja termina el proceso, en la parte por computadora aún tiene que esperarse a que sean enviados los productos. A pesar de esto las ventajas que ofrece el comercio

electrónico son magníficas, ya que es posible comprar en un relativo corto tiempo una gran cantidad de productos sin necesidad de moverse de lugar, es decir al mismo tiempo se puede comprar una computadora, un libro, un regalo, una pizza, hacer una transacción bancaria etc., de la forma tradicional se llevaría al menos un día completo y eso si los negocios están en la misma ciudad, sino, el ahorro de tiempo que representa comprar por Internet es incalculable.

Al efectuar una operación comercial por Internet se presentan nuevos problemas, por ejemplo cómo saber que la tienda virtual existe verdaderamente, una vez hecho el pedido cómo saber que no se cambia la información, cuando se envía el número de tarjeta de crédito cómo saber si éste permanecerá privado, en fin, para el comerciante también se presentan problemas similares, cómo saber que el cliente es honesto y no envía información falsa, etc. Más que nada en este trabajo me enfoco a los sistemas que utilizamos para pagar las compras realizadas por este medio y los problemas que se analizan, son los relacionados con las formas de pago electrónicas que se dan en este tipo de comercio.

1.1.2 Riesgos y Daños en una Transacción Comercial

La mayoría de la inseguridad en un sitio de e-commerce y en una transacción se darán por no cuidar los aspectos mencionados a continuación:

- Acceso no autorizado: una persona no autorizada, que no tiene acceso a un sistema de computadora, o una persona autorizada usa un sistema para ocuparlo con distintos propósitos a los que tiene por derecho.
- Instalación un atacante abandona un mecanismo para facilitar futuros ataques.
- Monitoreo de comunicaciones: un atacante capta información confidencial sin necesidad de perpetrar la computadora del usuario.
- Engaño: un atacante se entromete con los datos o procesos de comunicación.
- Denegación del servicio: un atacante causa acceso legítimo a la información para ser denegada.
- Repudiación: una parte para una transacción falsamente niega que la transacción ha ocurrido o fue autorizada, después de hecha.

Lo anterior quizá sea realizado por delincuentes que acechan en las redes de computadoras, estos pueden ser:

1 Los usuarios que están entendiendo y aprendiendo los diversos sistemas y capacidades. Esta persona no busca perjudicar o robar, sino que simplemente está buscando el conocimiento de la manera en la que funcionan las cosas y tal vez lo esté haciendo de una manera errónea. Estos no son una amenaza.

2 El delincuente que usa Internet y la Web para obtener ganancias ilegales, para fines de este trabajo lo denominaremos atacante o intruso. Conocen toda clase de formas para ocultar sus actividades. Por lo que respecta a este tipo de personas son una amenaza en el sentido de que roban software, tiempo y memoria de computadora, información de pagos y teléfonos, así como causan daño a equipo o a los datos de las transacciones.

En la mayoría de los sistemas en Internet y en cualquier otro, siempre existen agujeros de seguridad, en los que personas determinadas pueden encontrar fugas de información y obtener datos, que les ayuden a realizar actos ilícitos

Los delincuentes de computadora a su vez se clasifican en

- Hacker cualquier persona que es hábil en el manejo de las computadoras. Estos por lo general no comenten actos ilícitos
- Cracker persona que de manera específica irrrumpe en sistemas de computadoras, eludiendo las protecciones o adivinando los nombres de accesos. Estos delincuentes son una amenaza grave porque si pueden obtener el acceso como un usuario privilegiado, tienen acceso a cantidades increíbles de información de facturación, números de tarjetas de crédito y otros datos personales

- Phreaks: personas que irrumpen en sistemas telefónicos. Estas personas tratan en forma específica de obtener tiempo de llamadas de larga distancia para sí mismos, controlan la capacidad de conmutación telefónica o entran en sistemas PBX (Sistemas telefónicos digitales) automatizados de las compañías para obtener cuentas de correo de voz gratis o incursionan en los mensajes de correo de voz de las compañías.
- Phracker: es una combinación de un phreak y un cracker. Este interviene en sistemas telefónicos y sistemas computarizados, y se especializa en la destrucción total de las redes.
- Piratas de datos. estas personas roban software comercial, lo modifican para ejecutarlo sin necesidad de un número de serie u otras claves de arranque y publican sus datos en sitios warez. Un sitio warez contiene software robado colocado aparte para ser transferido a otras personas. Roban dinero de las compañías al distribuir el software, y también comprometen las computadoras de las compañías en las que establecen los sitios warez.

Fraudes

En Internet es muy fácil aparentar se cualquier persona o cualquier cosa que se desee. Por lo que es más fácil que otra persona intercepte información confidencial en Internet que en llamadas telefónicas.

La mayor parte de los fraudes contra los sistemas habituales de comercio electrónico (cajeros automáticos, sistemas de cheques electrónicos, valores almacenados.). han sido de bajo nivel. No tiene importancia lo deficiente que sea la seguridad informática y criptográfica; la mayoría de los criminales las ignoran por completo y se concentran en problemas de procedimiento, descuidos humanos y robos a la antigua usanza.

Esto implica que los nuevos sistemas de comercio no tienen que ser seguros, sino sólo mejores que los ya existentes. Existen 3 características del comercio electrónico que contribuyen a que el fraude resulte más devastador:

1. Una es la facilidad de automatización. La misma automatización que hace los sistemas de comercio electrónico más eficientes que los sistemas de papel, también hace más eficiente el fraude. Los fraudes de poco valor, que resultan despreciables en el sistema papel, se vuelven peligrosos en el mundo electrónico. Si un delincuente puede acuñar centavos electrónicos, podría conseguir un millón de dólares en una semana.

2. La dificultad de marcar la jurisdicción. El mundo electrónico es un mundo sin geografía. Un delincuente no necesita estar físicamente cerca del sistema al que está robando.

3. La velocidad de propagación, si alguien descubre cómo defraudar a un sistema de comercio electrónico y coloca en Internet un programa que lo realice, mil personas pueden tenerlo en una hora, cien mil en una semana. Esto podría fácilmente debilitar una divisa. Y sólo el primer atacante necesita conocimientos; el resto sólo tienen que usar el programa.

Los sistemas de comercio electrónico deben tener los mismos objetivos. Deberían ser capaces de detectar que el fraude ha tenido lugar y señalar al culpable. Y lo más importante, deben ser capaces de suministrar pruebas irrefutables que condenen al culpable en el juicio.

Los sistemas actuales deben anticiparse a futuros ataques. Un sistema de comercio electrónico con éxito suele permanecer en uso durante 10 años o más. Tiene que ser capaz de soportar el futuro. atacantes más capacitados, mayor poder de cálculo de los ordenadores y los mayores incentivos que presenta vencer un sistema muy difundido. No habrá tiempo para fortalecerlos cuando ya estén en funcionamiento.

El fraude en compras con tarjetas de crédito a través de llamadas telefónicas existe, y éste es realizado por el comprador o el vendedor. En Internet, al no aplicar las medidas de seguridad correspondientes, una tercera persona puede captar el número de tarjeta y usarlo para su beneficio. En estos casos el cliente no sabe que su número fue interceptado y por lo tanto no dará aviso al banco emisor de la tarjeta.

También el reproducir dinero electrónico es muy fácil y de bajo costo, el resultado puede ser una copia perfecta del original. Aunque se puede incurrir en el reuso

Se pueden evitar los fraudes, de la siguiente manera:

- Una compañía que trata de cometer fraude por lo general no se toma tiempo para crear una página apropiada. Si se compra en una tienda en línea, el observar el URL puede ser revelador, ya que la mayoría de las empresas grandes y medianas bien establecidas tienen sus nombres de dominio propios. Y ninguna compañía nunca deberá venir de dominios educativos (.edu).
- Otro tipo de fraude por lo general tiene una información de accesos por medios no computarizados limitada en sus páginas (números telefónicos y direcciones). La mayor parte de las compañías legítimas anuncian tantos medios de acceso como sea posible, y deberán tener información de correo electrónico, fax, teléfono y dirección Un número 800 es buena señal, aunque compañías pequeñas no cuentan con ello.
- Sino se confía en la solidez de un negocio, llame al código de área de la compañía y verifique si aparece en el directorio, sino aparece es posible que se trate de un negocio fraudulento.
- Llamar a la compañía es una buena señal. Si le pide al negocio que le envíe información por fax, a menudo obtendrá un indicio de su profesionalismo e información de sus servicios
- Para los caso del dinero electrónico una cosa que debe evitarse en los sistemas de pago es el reuso del dinero electrónico.

Robo

- Este se puede dar robando espacio en un servidor.
- Robar archivos de contraseñas y obtener algunas claves de acceso, para ingresar al sistema
- Robar números de tarjetas de crédito y usarlos para hacer compras ilegales
- Hurtar códigos de acceso de alguien a un sitio Web privado, conectarse como esa persona y robar datos.
- Interceptar comunicaciones entre servidores.

Para evitar esto se han creado los denominados servidores seguros, que intentan proteger la información que se envía sobre Internet por medio de la encripción de la información que viaja entre el browser del cliente y el servidor. Pero hay algo importante que mencionar, que la información no es protegida en el browser o en el servidor. Por lo que, hay tres lugares en donde los datos pueden ser interceptados:

1 En el browser
2 Entre el browser y el servidor.
3 En el servidor.

En el browser los datos pueden ser robados, cuando el cliente teclea datos importantes (tarjeta de crédito) en un campo de una forma y continúa la sesión Web. Si el cliente deja la computadora encendida y no está, cualquier persona que pase puede retroceder en las páginas del sitio de compra y observar el número de tarjeta que se introdujo Este problema se puede evitar usando:

- La capacidad de retroceder a páginas anteriores del browser hasta que llegue a la página que contiene los datos delicados Vaya hacia delante desde esta página hasta cualquier página sin información delicada Esto cambia la ramificación del cache.
- Puede usar la opción del browser de limpiar el cache

Los sitios de comercio electrónico que manejan datos de tarjeta de crédito, pueden hacer que el campo de tarjeta de crédito tenga una máscara, por lo cual el número nunca será visible en la pantalla, pero esto implica que se tenga que poner un segundo campo de verificación del número de la tarjeta por si el cliente se equivoco al ingresarlo

Cuando se envía la información de una transacción a un servidor, a menudo es desencriptado y almacenado o enviado como correo electrónico Por este medio puede ser interceptado, el evitarlo puede resultar algo costoso y complicado porque implica encriptar la información durante todo su recorrido desde el emisor hasta el receptor de la información

Para que no sea tan costoso se deben verificar algunos aspectos más que nada en el envío de información de la tarjeta de crédito, porque al ser obtenidos sus datos, pueden ser usados en beneficio del delincuente. Este número sirve para que los delincuentes cometan actos ilegales, tanto en e-commerce, como en el comercio tradicional

Trampas en el uso de Tarjetas de Crédito

- Obtener datos de una tarjeta de crédito al cobro en algún establecimiento, se llenan vouchers que pueden ser ingresados como algún pago, mientras el cajero se queda con el dinero correspondiente a esa compra, consumo o servicio.
- Robo de la tarjeta y falsificación de firma.
- Robo de la tarjeta y realizar una compra en Internet donde sólo piden los datos de la tarjeta.
- Alteración de la cantidad de la compra.
- Realizar una compra por Internet, hacen el cargo a tu cuenta y quedarse con la mercancía.

Fuente de datos en el banco

- Si se tiene bancos afiliados, y si se altera el número de cuenta no se sabe a quien pertenecen esos pagos y muchas veces el personal se aplica esos pagos.

Intercepciones por teléfono

- Por medio de la recepción de llamada, obtener los datos del cliente, y hacerle cargos mayores por su compra, quedándose con el dinero del cargo.
- Al obtener los datos del cliente hacer cargos por mercancía, ayudado por la gente de entrega de la mercancía a hurtar la misma.

1.1.3 Precisar Medidas de Seguridad en los Actores

El comercio electrónico es una clave para encontrar nuevos recursos de ingresos, expanderse dentro de nuevos mercados, reducir costos, y crear estrategias de negocios. Los actores principales en una transacción de este comercio son: el cliente, el banco y el vendedor.

Pero su infraestructura puede ser susceptible de abuso, mal uso, y fallo, causando un sinnúmero de problemas a los negocios como pérdidas financieras debido a fraudes, pérdida de oportunidades de negocios debido al trastorno de servicios, una desacreditada reputación para el negocio y pérdida de la confianza del cliente.

Por lo cual, las partes involucradas lo que buscan es que el manejo de su información de compraventa pueda cubrir estos aspectos:

- **Confidencialidad (Confidenciality):** La computadora está enviando un mensaje simplemente a la red, alguien ajeno a la red puede leerlo. De lo que se encarga este servicio es de que el mensaje transmitido pueda viajar seguro, sin que otra persona ajena a la transmisión pueda saber el contenido del mensaje.

- **Integridad (Integrity):** Cuida que los datos enviados sean iguales a los que se recibieron

- **Autenticación (Autenticity):** Nadie puede estar seguro de las personas con quien están haciendo un intercambio. No hay ninguna firma, no hay reconocimiento de voces, ninguna cara familiar. Las computadoras son excelentes para el intercambio de información. Permite comprobar que la parte emisora es quien dice ser y viceversa.

- **No repudio (No-Repudiability):** Las partes envueltas pueden negar que el intercambio tuvo lugar, porque ningún recibo de regreso, se recibe. Ellos simplemente pueden decir "yo no lo envié."

- **Control de acceso (Access control):** Protege contra las revelaciones de la información de la gente que no está autorizada a esa información.

A cada una de las partes le preocupa que su información no cubra alguna de estas propiedades y que se cuide la seguridad de la transacción, cuidando los siguientes aspectos:

- Le interesa que la información al viajar en la red se mantenga segura y que nadie intercepte su información para cometer algún ilícito con los datos.
- Que cuando viaje la información nadie altere los datos, como por ejemplo la alteración de la información del domicilio a donde se quiere que lleguen los productos o servicios de los vendedores.
- Que no se pueda revocar la transacción realizada.
- Algunas veces los vendedores y los bancos en todo momento, requieren que se autentifique la identidad del cliente.
- Asegurarse que sólo personas autorizadas tengan acceso a la información.
- Prevenir la desautorizada creación, alteración, o destrucción de datos.
- Asegurarse que los usuarios no nieguen el acceso a la información
- Asegurarse que los recursos son usados de manera legítima.

Para lograr estos objetivos y proteger la información en un canal de comunicación y dentro de una computadora, se deben tomar otro tipo de medidas de seguridad:

- Seguridad física.
- Seguridad personal
- Seguridad administrativa.
- Seguridad de datos / información.
- Seguridad online.

Sólo nos limitaremos a cubrir la parte referente a la Seguridad de datos/ información, y en ocasiones se hace referencia a algunos de los aspectos de los tipos de seguridad.

Como protegerse de los participantes en el e-commerce, para que no hagan trampas

De los bancos sospechosos:

- Ofrecen tasas extraordinanas de interes como en las cuentas de ahorro. Algunos bancos legitimados en Internet, porque les divierte ahorrar por no tener ninguna traba y montar sucursales, pueden ofrecer algunas tasas más altas. Pero una gran diferencia en tasas quizas visualice un problema.
- Falta de una calle o una dirección de correo.
- Tener un segundo nombre de dominio. Un banco legítimo a menudo tiene una dirección de bancos en Internet similar a su propio nombre, tal como "banamex.com" Los sitios fraudulentos quiza listan primero el nombre de un provedor de Internet, con el nombre de la compañía secundaria

De las empresas

- Busca el nombre de la compañía, y alguna dirección
- Información sobre sus productos o servicios
- Una empresa fraudulenta no te proporcionara los datos anteriores
- No proveer números de cuenta del banco, números de tarjeta de crédito, número del seguro social u otra información personal, sino se sabe que la compañía es legítima y que la información es necesaria para la transacción Con cada información parcial pueden hacer cargos no autorizados, deducciones de dinero de tu cuenta y hacerse pasar por ti para obtener crédito en tu nombre
- Cuando usas una tarjeta de crédito para una compra y hay algún problema, tienes los derechos de notificar al emisor de la tarjeta que tienes conflicto con el cargo, no lo tienes que pagar mientras sea investigado

De los clientes:

- No aceptar una orden de tarjeta de crédito sino está completa la información, como la dirección y el número de teléfono completo.
- La orden debe hacerse de una dirección e-mail base, no se aceptará la dirección e-mail de un proveedor gratuito (yahoo, hotmail, etc)..
- Checar los sitios de dominio de las direcciones e-mail, ya que si es un dominio legítimo se podrá identificar entrando a su página
- Si existen dudas sobre la orden de compra se llamará al teléfono indicado en la orden. Se tendrá muy en cuenta que la información del tarjetahabiente sea la correcta. Esta investigación se realizará con el cliente y con el banco emisor de la tarjeta de crédito.

1.1.4 La Compra OnLine

Para entender como se usan apropiadamente los pagos electrónicos, consideremos el siguiente proceso:

1. El comprador navega buscando articulos. Ingresá a una tienda virtual o un catálogo online el página Web del vendedor.
2. El comprador selecciona los artículos a ser comprados. Comprara precios y ganando el mejor valor basándose en la marca, precios, calidad y otras variables.
3. El vendedor presenta al comprador una forma de pedido, la cual contiene la lista de los aritulos, sus precios, y el precio total de compra incluyendo el transporte, el empaque, y los impuestos. Esta forma de pedido quizá sea entregada desde el servidor del vendedor al comprador. Algunos vendedores online quizá provean al comprador la habilidad de negociar el precio.
4. El comprador selecciona el sistema de pago (dinero electrónico, cheques electrónicos y tarjeta de crédito).
5. El comprador envia al vendedor el pedido completado y el sistema de pago elegido.
6. El vendedor solicita la autorización al banco del comprador.
7. El vendedor envía al cliente una confirmación de la orden de embargo y de pago.
8. El vendedor embarca los bienes o ejecuta la solicitud de los servicios pedidos en la orden.
9. El vendedor solicita el pago a la institución financiera del comprador.

En la siguiente sección doy las fases y pasos de una compra real en una tienda virtual en Internet.

1.1.3 Fases y Pasos de una Compra por Internet

Esta parte está desarrollada en base a las fases y pasos que se pueden dar en una compra en un tienda virtual de e-commerce. Se tomo como ejemplo una de las tiendas virtuales con mayor éxito Amazon (http://www.amazon.com/)

FASE	PERSONA	PASO
1. Ingreso a Internet	Comprador	1. Ingresa a Internet. 2. Escribe la dirección de la ubicación de la tienda virtual.
2. Selección del artículo a adquirir	Comprador	1. Entra a la tienda virtual. 2. Busca el artículo a adquirir. 3. Selecciona el artículo. 4. Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra. 5. Muestra el artículo seleccionado .
3 Alta de dirección e-mail de un cliente	Vendedor	1 Se va al botón de nuevo. 2. Pide dirección e-mail.
4 Ingreso de dirección e-mail del cliente	Comprador	1. Ingresa dirección e-mail
5. Ingreso de datos por el cliente	Comprador	1. Ingresa su nombre, apellidos, dirección y teléfono en el formulario.
6. Verificación del llenado de los datos	Vendedor	1. Checa que los campos tengan datos. 2 Muestra los datos ingresados.
7 Elección de la dirección	Comprador	1 Tiene que elegir la dirección a la cual quiere que se le envíe el producto.
8. Muestra datos del cliente y del artículo	Vendedor	1 Despliega la información del artículo a adquirir y los datos de la dirección de envío.
9 Asignación de una cantidad del artículo	Comprador	1. Asigna una cantidad de compra.
10 Señalización de las formas de envío	Vendedor	1 Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)
11 Elección de forma de envío	Comprador	1 Elige la opción más adecuada conforme a sus necesidades
12 Indica las formas de pago	Vendedor	1 Pide password y su confirmación 2 Menciona los procesos de pago

FASE	PERSONA	PASO
13. Selección de un método de pago	Comprador	1. Ingresa password y confirmación 2. Selecciona el método de pago. 3. Ingresa los datos que se requieren de la forma de pago elegida.
14. Corroboración de datos	Vendedor	1. Checa que los datos ingresados sean reales conforme al método de pago elegido.
15. Muestra de la orden de compra	Vendedor	1. Despliega la información total de la compra. 2. Acepta la compra
16. Aceptación de la orden	Vendedor	1. Informa que la orden esta lista. 2. Envía un mensaje, para informar el número de la orden.
17. Envío del producto	Vendedor	1. Checa el depósito del pago. 2. Envía el producto
18. Recepción del producto	Comprador	1. Recibe el producto

1.1.4 Procedimiento de una Compra por Internet (General)

En base al punto anterior se muestra el procedimiento de la compra, el tiempo que tardaba en realizar cada una de las operaciones y que tipo de actividad se le considera.

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS.
			Hr	Min	Seg	O	□	→	D	▽	
1	**Ingreso a Internet**	**comprador**									
1	Ingresa a Internet.				20	*					
2	Escribe la dirección de la ubicación de la tienda virtual				5	*					
2.	**Selección del artículo a adquirir**	**comprador**									
1	Entra a la tienda virtual				5	*					
2	Busca el artículo a adquirir			5		*			*		
3	Selecciona el artículo				5	*					
4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
5	Muestra el artículo seleccionado				15	*					
3.	**Alta de dirección e-mail de un cliente**	**comprador**									
1	Se va al botón de nuevo				5	*					
2	Pide dirección e-mail						*				
4.	**Ingreso de dirección e-mail del cliente**	**comprador**									
1	Ingresa dirección e-mail				10	*				*	
5.	**Ingreso de datos por el cliente**	**comprador**									
1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
6.	**Verificación del llenado de los datos**	**vendedor**									
1	Checa que los campos tengan datos.				5		*				
2	Muestra los datos ingresados				5	*					
7.	**Elección de la dirección**	**comprador**									
1	Tiene que elegir la dirección a la cual quiere que se le envie el producto				5	*					
8.	**Muestra datos del cliente y del artículo**	**vendedor**									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envío				5	*			*		
9.	**Asignación de una cantidad del artículo**	**comprador**									
1	Asigna una cantidad de compra				5	*				*	
10.	**Señala las formas de envío**	**vendedor**									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)				5	*		*			
11.	**Elección de forma de envío**	**comprador**									
1	Elige la opción mas adecuada conforme a sus necesidades				5	*				*	
12.	**Indica las formas de pago**	**vendedor**									
1	Pide password y su confirmación				5	*					
2	Menciona los procesos de pago					*		*			
13.	**Selección de un método de pago**	**comprador**									
1	Ingresa password y confirmación				30	*	*				
2	Selecciona el método de pago				5	*				*	
3	Ingresa los datos que se requieren de la forma de pago elegida			5		*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS.
			Hr	Min	Seg	O	□	→	D	▽	
14.	**Corroboración de datos**	**vendedor**									
.1	Checa que los datos ingresados sean reales conforme al método de pago elegido.				15		*				
15.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	*			*		
16.	**Aceptación de la orden**	**vendedor**									
.1	Informa que la orden esta lista.				5	*					
.2	Envía un mensaje, para informar el número de la orden.				30	*			*	*	
17.	**Envío del producto**	**vendedor**									
.1	Checa el depósito del pago.		25			*					
.2	Envía el producto.		25					*	*		
18.	**Recepción del producto**	**comprador**									
.1	Recibe el producto.		700			*					

Estas debilidades fueron tomadas en cuenta, para determinar en donde el procedimiento puede considerarse inseguro y que tipo de daño es el que causaría.

	DEBILIDADES	R	P	C
1.2	Antes de realizar una compra, se debe estar seguro de que la tienda realmente exista.	▪		
2.4	La página en la que se muestra el artículo puede no ser la de la tienda virtual, por lo que los datos que se ingresen para el proceso de compra pueden ser obtenidos por un intruso.		▪	
12	Al momento de que se ingresan los datos y se envían estos pueden ser obtenidos por un intruso.	▪		
	Si la persona que realizó la compra deja su sesión abierta, otra puede checar y anotar los datos de la tarjeta que ingreso.	▪		
	Gente experta por medio de programas para obtener información de la red, puede desencriptar los datos de la tarjeta y hacer uso de estos.	▪		
	Si los procedimientos no están bien establecidos, principalmente el de envío, puede haberse hecho el cargo sin que el producto llegue a su destino final.			▪
	El método de pago que se está utilizando es inseguro.	▪		

R **Riesgo**
P **Peligro**
C **Costo**

1.2 Historia

1.2.1 Historia de los Sistemas de Pago

El hombre ha estado comprometido en el proceso de trocar, permutar y cambiar una cosa por otra desde épocas muy lejanas El origen de estos movimientos de bienes posiblemente tuvo sus comienzos en la emigracion, el pillaje, en regalos o quizás en formas primitivas de trueque.

La primera forma de comercio fue el "comercio silencioso". En él, los participantes no tenían contacto directo. Los miembros de una familia o tribu se allegaban a un espacio abierto, desplegaban los bienes que deseaban cambiar y se escondían.

Después, se aproximaban los interesados en el trato, extendían todo lo que estuviesen dispuestos a ofrecer a cambio y también se retiraban. Aquellos que habían hecho el primer movimiento volvían y examinaban la oferta de sus vecinos. Si estaban satisfechos, tomaban los bienes ofrecidos y se iban, dejando los suyos allí. Si consideraban que el precio era insuficiente, retiraban sus propios bienes y se escondían otra vez para que la otra parte del trato examinase la nueva oferta, y así se continuaba hasta que las partes estuvieran satisfechas.

El trueque consistía en el intercambio de una cosa por otra sin la intervención de ninguna clase de dinero Requiere la doble coincidencia de deseos.

La actividad comercial es el intercambio de unos bienes y servicios por otros.

El dinero, aparentemente, no es más que un intermediario que facilita las relaciones económicas. El intercambio directo, sin dinero, resulta muy difícil.

Los orígenes del dinero, como los del comercio, se remontan a épocas anteriores. Su función como medio de cambio está relacionada con la del patrón de valor.

En tiempos homéricos el ganado sirvió como patrón de valor, y la propia palabra pecuniario procede de la palabra latina pecunia, que significa dinero; la cual procede, a su vez de pecus, ganado.

El ganado como medio de pago presenta serias desventajas, por lo que ya entonces se usaba sólo en el pago de grandes transacciones, tales como la compra de un esclavo o esposa, y en el pago del tributo. Otros bienes que llegaron a servir a la vez como patrón de valor y como medio de pago son el lienzo y los cereales.

Documentos babilónicos muy antiguos (alrededor del año 3000 A. C)., hacen una distinción legal entre bienes intercambiables, o sea bienes que podían pasar de una persona a otra con muy poco formalismo, y bienes no intercambiables, para los que se exigía un acto de transferencia formal.

Los bienes intercambiables el oro, la plata, el plomo, el bronce y el cobre, la miel, el aceite, el vino, la cerveza y la levadura, la madera y el cuero, los rollos de papiro y las armas.

En otras partes del mundo, los medios de pago fueron ornamentos u objetos con significado ritual o religioso, incluyendo modelos de utensilios y herramientas En Japón las cabezas de flechas hechas de piedras semipreciosas, y en Nueva Guinea anzuelos de madreperla. Al norte de Europa se han hallado hachas de piedra demasiado frágiles y pequeñas para cualquier uso práctico

El dinero ornamental en circulación más conocido y difundido fue, sin embargo, la concha de cauri, que se uso como medio de pago en la India, en Medio Oriente y en China, continuando en circulación en los tiempos históricos en gran parte de Asia, Africa y en las islas del Pacífico, en un área que iba desde Nigeria hasta Siam y desde Sudán hasta las Nuevas Hébridas.

Una diferencia importante entre las formas de dinero y los bienes intercambiables de Babilonia, es que estos últimos pasaban de mano en mano por el peso, mientras que los primeros pasaban por el número de cuentas, es decir, contando el número requerido en lugar de pesarlo.

Los metales preciosos llegaron a gozar de supremacía como medios de pago entre los bienes intercambiables.

Primero se usaron como barras metálicas más o menos uniformes, luego algunos gobiernos acuñaron dichos metales para preservar su pureza.

El dinero instrumental de metal del norte de Europa se estaba abriendo camino hacia el Mediterráneo. Asadores en forma de varilla, trípodes, jofainas, hachas y anillos se usaron como dinero para pagos, menos en la Grecia de Homero.

Originalmente, estos artículos eran de bronce, pero en los tiempos posthoméricos se usaron también asadores en forma de varilla de hierro.

Una de las unidades monetarias griegas más pequeñas, el óbolo, probablemente procede del nombre dado al asador de hierro (obelos), mientras que el dracma (que sigue siendo la unidad monetaria griega) originariamente era un puñado de (seis) asadores.

Entre las ruinas cretenses del siglo XIII A. C., se han descubierto discos de metal que posiblemente se usaron como medios de pago, pero las primeras monedas europeas con forma parecida a las modernas procedían de Lidia, en Asia Menor, y se acuñaron probablemente durante los siglos IX-VIII A.C. Se dice que la moneda metálica, a la imagen de la actual, se creó hacia el siglo VII A.C. en la isla griega de Egina, en el reinado del rey Fidón.

Las primeras monedas de Asia Menor eran de electrón, una aleación de oro y plata muy apreciada, formada por cuatro partes de oro y una de plata. Se cree que fueron los mercaderes los que usaban estas monedas para el comercio internacional, pues incluso las más pequeñas eran demasiado valiosas para pagos de poca cuantía.

Alrededor del año 750 A.C. se acuñaron monedas de plata en Egina, y la primera moneda acuñada en oro se atribuye a Creso, último rey de Lidia, en el siglo VI.

La invención de la moneda metálica es atribuída a los griegos, en sus aspectos esenciales de cuño, tamaño manuable, espesor, peso y valores proporcionales.

El único metal acuñado era el cobre, aunque para los pagos grandes se usaban lingotes de plata por peso, y durante mucho tiempo se usaron también cauríes, sal y pieza de seda.

Se cree que las primeras monedas de bronce aparecieron en Sicilia en el siglo V A.C. En los años 407 y 406 A.C. se acuñaron en Atenas monedas de oro y bronce respectivamente.

La Persia del siglo IV parece haber sido el primer país que puso en funcionamiento un verdadero patrón bimetálico, acuñado regularmente oro y plata.

La influencia monetaria griega se extendió por el oeste llegando a Roma donde solamente se usarón monedas de bronce bastante rudimentarias, conocidas con el nombre de ases.

El dinarius de plata es la base del sistema monetario romano, se acuño por primera vez en el año 268 a.C.

La Letra de Cambio

El desarrollo de los mercados organizados de dinero y de capital requiere no sólo la existencia de personas que posean capital, el cual están dispuestas a prestar, sino también un cierto tipo de obligaciones que puedan transferirse fácilmente de unas a otras. Los banqueros de depósitos medievales en Italia y España transferían los saldos bancarios de una cuenta a otra mediante documentos escritos, precursores del cheque moderno.

Durante el siglo XIV algunos de estos banqueros establecieron un sistema de liquidación entre ellos. Todo banco que formase parte de tal acuerdo mantenía una cuenta con los otros, cuando el cliente de uno giraba un cheque pagadero al cliente de otro, este segundo banco abonaba el valor del cheque en el haber de la cuenta de su cliente, y cargaba la misma cantidad en el debe de la cuenta del banco del cliente que lo había girado.

La letra de cambio implicaba a la vez una transacción de crédito y una transacción de cambio de monedas extranjeras.

La letra de cambio moderna es un instrumento negociable. La letra medieval era transferible, pero el comprador no adquiría necesariamente un título mejor que el que tenía la persona que lo compró.

Un banco moderno comercia dicha transacción convirtiendo la moneda exterior en moneda local a la tasa de cambio existente en el mercado, y luego carga una tasa de descuento (que depende también de la tasa de mercado) por el crédito que concede al pagar en efectivo a cambio del derecho de percibir un pago en el futuro. Los mercados medievales no estaban lo suficientemente organizados como para que tal procedimiento fuera posible y aun en el caso de que lo hubiesen estado, esto habría sido considerado una usura. El precio que el banquero medieval pagaba por una letra debe de haber incluido, a la vez, un elemento de interés, o descuento, y un pago por sus servicios como cambista, pero ambos elementos eran inseparables.

Cuando un banquero compraba una letra, adquiría después de cierto tiempo, una suma determinada en moneda extranjera, y luego tenía que invertir el proceso comprando una letra en el centro extranjero que lo titulara para recibir el pago en su propia moneda. El alcance de esta ganancia o pérdida última dependía de los términos en los que pudiese tomar este segundo trato y, dado que las tasas de cambio medievales eran propensas a violentas fluctuaciones y no existía ningún mercado organizado de futuros no podía conocer estos términos en el momento de la transacción original.

El contrato notarial era muy diferente en su forma de una letra de cambio, si bien comprendía la transacción combinada de crédito y de cambio de monedas. Esta doble transacción era una de las características de la letra medieval, y las autoridades más importantes en la materia opinan que la diferencia entre ambas era únicamente de forma.

Probablemente el camibo en la forma comenzó con el envío de una carta, junto con el contrato notarial, señalando los términos principales del trato de modo más simple y menos elaborado y , a su debido tiempo, la letra pasó a suplantar al mismo documento notarial.

A fines del siglo XIV la forma de la letra había llegado a ser altamente moderna.

Hay sólo dos diferencias entre esta letra y una moderna. La letra está girada a favor de una persona designada, y no al portador, y parece haberlo sido contra un pago en dinero más que contra la venta de bienes.

Este tipo de transacción, actualmente conocido como letra financiera, era muy común en la edad media.

El Crédito

Durante más de doscientos años la moneda de oro, plata, o para pequeñas cantidades, bronce, fue el principal medio de pago en aquellas comunidades que habían traspasado las formas primitivas de dinero.

Por otro lado, el valor de las citadas estaba estrechamente relacionado con el valor de su contenido metálico.

Frecuentemente los gobiernos impusieron un señoreaje que elevaba el valor de la moneda como dinero ligeramente por encima de su valor como metal, señoreaje que se aceptó en razón de la comodidad que suponía el uso de numerario.

Se dio la revolución en los medio de pago, ésta fue la aceptación de las deudas (obligación de pagar en moneda), como sustitutos de la moneda misma.

Tales deudas podían ser las letras de cambio de los comerciantes, aunque, por lo común, eran billetes emitidos por los bancos o créditos abiertos en sus libros.

El empréstito de dinero es probablemente tan antiguo como el dinero mismo, ya los babilónicos y los griegos desarrollaron instituciones que desempeñaban alguna de las funciones de los bancos modernos.

Los bancos griegos concertaban transferencias crediticias sobre las ciudades para evitar el riesgo que suponía transportar la especie en barcos, pero no hay ninguna prueba de que las transferencias de los depósitos bancarios formasen un sustituto de la moneda para pagos internos.

Las ciudades italianas fueron las primeras en usar, de nuevo, las transferencias de los depósitos bancarios como medio de pagos. No obstante, para pagar a través de un banco era necesario que el deudor diese instrucciones orales a su banquero y que el acreedor manifestase su conformidad en presencia de un testigo.

En los siglos XIII y XIV se reemplazó gradualmente este incomodo sistema por una orden, antecedente del cheque moderno, escrita y firmada por el deudor

Se cree que fueron los banqueros italianos los primeros que comenzaron a utilizar lo que llegó a conocerse como giro comercial, es decir, podían aceptarse depósitos y transferidos de una cuenta a otra, pero no podían hacer préstamos ni permitir que los clientes girasen al descubierto.

Sin embargo en la práctica, la tentación de conceder también préstamos fuen tan grande, que frecuentemente los banqueros hicieron empréstitos, llegando a veces, a perder el dinero de sus depositantes y no pudiendo pagarlos en numerario cuando estos lo demandaban.

Esas quiebras de los bancos privados condujeron a que la gente demandase el establecimiento de bancos públicos de giro. Los bancos públicos llegaron, bajo presión, a hacer frecuentes empréstitos a las autoridades públicas, presión a la que podían oponer resistencia en condiciones mucho peores que la banca privada.

La caracterisitca esecial de cualquier medio con el que se realicen los pagos no es el valor intrínseco de dicho medio, sino su aceptación general.

Lo más importante para la persona que tiene que cobrar algo, es la seguridad de que cualquiera que sea la cosa que reciba en pago podrá usarla para hacer frente a sus propios pagos. Con tal que satisfagan esta condición, las conchas, discos de metal, hojas de papel impresas en la forma apropiada o las meras entrada en el libro mayor pueden servir como medios de pago.

Papel Moneda

Medida de valor que siendo intrínsecamente un bien, es aceptada en mayor medida que cualquier otro bien debido al poder cancelatorio de las obligaciones, fundado en disposiciones legales. Es un instrumento fácilmente manejable y de ilimitada reproducción

Al ser reconocida también en otros países extraños a su emisión, es un medio para medir la potencialidad económica de los estados y el grado de confiabilidad que se dispensa a su unidad monetaria, su antecedente remoto lo encontramos en los certificados de depósitos bancarios de las ciudades italianas. La primera emisión de papel moneda se piensa que se realizó en Massachusetts en 1960, en forma de vales o billetes de crédito del Tesoro, para hacer frente a los apuros financieros de la vida colonial. Al poder rescatarse en su tiempo las piezas metálicas correspondientes, concluyó la experiencia con una gran depreciación

Otro antecedente lo constituye el Banco de Inglaterra en 1797, que emite billetes de banco con circulación en Londres y sus alrededores

El papel moneda empezó siendo un simple vale de almacén o recibo de la Casa de Moneda, por una cantidad determinada de metales y es, la forma más simple de moneda, cuando el papel es directamente regulado por el Estado.

Tarjeta de Crédito

Su nacimiento tuvo lugar en países Europeos. Francia, Inglaterra y Alemania utilizaban este sistema, a comienzos del siglo XX, los hoteles importantes para uso exclusivo de sus clientes fijos. Pero este tipo de tarjetas no eran exactamente iguales a las que se utilizan en la actualidad, por cuento en su relación sólo intervenían dos partes: el hotel concesionario del crédito, por una, y el cliente que gozaba del mismo, por la otra. No existía el triángulo de emisor-socio o tarjetahabiente-vendedor o empresa comercial.

La creación del Diners Club en 1950 por Ralph Scheneider y Frank Mc Namara, marca un hito en la historia de las tarjetas de crédito, esta entidad financiera es la primera que emite una tarjeta con vocación internacional viéndose coronado con el éxito su accionar en forma casi inmediata, tanto es así que en 1954 aparece Diners Club de Francia, en 1967 varios bancos franceses crean la tarjeta Carte Bleue.

En 1958 nace la tarjeta American Express, siendo ésta más una agencia de viajes que un banco.

El inicio de esta modalidad crediticia era privativo de los restaurantes, y posteriormente se extiende a empresas de ferrocarriles, estaciones de servicios, almacenes, cadenas de importantes gasolineras, sitios de diversión, etc.

El Franklin National Bank comenzó con los programas de tarjetas de crédito bancarias de nuestros días en agosto de 1951 A los tres años siguientes, más de 100 bancos, y aquellos principalmente pequeños comenzaron con los planes de tarjeta de crédito.

En 1959 los bancos de América, Trust and Savin Asociation y el Chase Manhattan Bank introdujeron los programas de tarjeta de crédito. Naturalmente varios bancos incluyeron estos programas y a fines de 1959 más de 40 bancos estaban ofreciendo estos planes. En total, 235 planes fueron establecidos durante el período de 1958 y 1959.

Los dos bancos, el de América y el Chase, perdieron dinero en los primeros años de establecidos estos planes, principalmente por su incapacidad para generar suficiente volumen.

Hasta 1965, los programas de tarjetas de crédito bancarias fueron confiados a áreas locales donde los bancos promovían negocios. Pero desde entonces los bancos desarrollaron grupos regionales y nacionales. Bajo un plan típico, hay un banco principal en una región que emite las tarjetas de crédito, opera el sistema contable central y lleva créditos bancarios giratorios que son generados.

Agentes bancarios, miembros del mismo sistema, suscriben o contratan comerciantes locales al plan Cuando se hacen compras con las tarjetas de crédito, los comerciantes envían la papeleta de venta a los agentes bancarios y estos a su vez a los principales bancos regionales Algunas veces ellos comparten los créditos giratorios, otras, sólo emiten las tarjetas a través del banco principal.

A comienzos de los 70's, casi todos los grandes bancos del país estaban ofreciendo una u otra forma de los planes de tarjeta de crédito, y varios de los planes unían a los bancos a través del Estado en sus fronteras regionales o nacionales

Tarjeta de Crédito y Moneda

En E U existen métodos para giros o transferencias por medio de tarjetas de crédito, en máquinas especiales conectadas por medio de computadoras con las cuentas de los clientes y las cuentas de los proveedores, las mismas traducen los datos de las tarjetas y de la factura y debitarán o acreditarán inmediatamente las cuentas respectivas.

La tarjeta VISA reemplaza a las actuales tarjetas gravadas, porque posee una cinta magnética situada en la parte superior, usándose en la actualidad en los cajeros automáticos y transacciones electrónicas, al igual que las smart cards o tarjetas inteligentes, que tienen un chip integrado y actualmente están surgiendo.

Todo esto revela una desmaterialización y abstracción de la moneda, en pocas palabras, es un sustituto del dinero en efectivo.

La moneda cumple una triple función dentro de las transacciones: es intermediaria en las operaciones comerciales, es un instrumento de medición de valores, es un elemento de cancelación de obligaciones y para todo ello tiene que tener aceptabilidad general, y ello implica de manera completa la confianza.

Su utilidad es tanta como la desconfianza de un vendedor con respecto a un comprador. La tarjeta de crédito disocia esos elementos al asumir la confianza y ésta puede entonces, en cierto modo, sustituir al dinero y no lo contrario.

1.2.2 Propiedades de los Sistemas de Pago Tradicionales

SISTEMAS DE PAGO	CHEQUE	DINERO EFECTIVO	TARJETA DE CRÉDITO
Transferencia	➢ Fácil entre comprador y vendedor. ➢ Es posible entre personas naturales. ➢ En general se transfiere solo una vez. ➢ Si el cheque está abierto puede transferirse más veces.	➢ Muy fácil, se transfiere indefinidamente entre personas y/o instituciones. ➢ Problemas con cantidades grandes.	➢ Fácil entre comprador y vendedor ➢ No es posible entre personas naturales. ➢ El mismo pago no se puede transferir más de una sola vez. ➢ No es anónimo, identifica plenamente al comprador y al vendedor.
Anonimato	➢ No es anónimo. Identifica al titular y a quién lo cobra	➢ Es completamente anónimo.	➢ Difícil en transacción con firma. ➢ Más fácil en transacción telefónica.
Falsificación	➢ Difícil: Lleva la firma del titular de la cuenta	➢ Difícil. Grandes inversiones, en crear un billete similar.	➢ Segura si se da aviso rápido a banco administrador. ➢ El riesgo es igual a las compras entre la pérdida y el aviso al banco
Seguridad	➢ Seguridad variable Inseguro si es al portador. Seguro si es nominativo y cerrado	➢ No es seguro, es al portador.	
Certificación o repudio	➢ No es 100% convertible • Puede no tener fondos • Cuenta puede ser cerrada por el titular para evitar pago Esto no es detectable en el momento del pago, especialmente entre particulares	➢ Certificación completa	➢ Compra se puede repudiar sino fue efectiva. ➢ Compra en persona con firma verdadera no es repudiable ➢ Compra por teléfono puede ser repudiable más fácilmente

1.2.3 Problemas con los Sistemas de Pago Tradicionales

Estos sistemas no trabajan online por la siguientes rezones:

- Falta de conveniencia. Los métodos de pago tradicional generalmente requieren que el comprador abandone una plataforma online y use el teléfono, o envíe un cheque, para realizar el pago.
- Escasez de seguridad. Para hacer un pago tradicional sobre Internet, un comprador tendría que proveer detalles de una tarjeta o cuenta de pago y otra información personal online. Dejando a un lado a Internet y, proveyendo los detalles de la tarjeta y de la cuenta de pago por teléfono y/o por correo también ocasiona riesgos en la seguridad.
- Ausencia de cobertura. Las tarjetas de crédito trabajan con vendedores asignados a un banco por lo general, y no soportan transacciones de pago persona a persona o negocio a negocio.
- Carencia de elegibilidad. No todos los compradores potenciales tienen altas tasas de crédito para permitirles accesar a las tarjetas de crédito y/o cuentas de cheques.
- Falta de soporte de las micro transacciones. Muchos pagos hechos sobre Internet son de valor bastante bajo que el costo de una llamada telefónica o el envío de una carta sea más alto que éste. El costo de manejar esos métodos de pago es demasiado alto para el vendedor.

1.2.4 Pagos Electrónicos

Los primeros sistemas electrónicos de pago emergieron con el desarrollo de las transferencias por cable. Estos servicios (Western Union) permitían una entrega individual de la moneda a un dependiente en un lugar, quien le da instrucciones a otro dependiente en otro lugar, para dar el dinero a una persona en el segundo lugar quien es capaz de identificarse como el destinatario. El efectivo fue entregado al cliente sólo después de que se le identificó. En este escenario no existe un banco; Western Union fue una compañía de telégrafos. El asegurar la confiabilidad del pago en la estabilidad financiera de la firma. La seguridad fue provista para dimensionar que Western Union tenía transmisión privada controlada usada con facilidad para enviar mensajes de transferencia de fondos, la información no se compartía con el público, y las transacciones eran privadas. Se proveía autenticación sólo por una firma al final de la transmisión, la cual era verificada por el dependiente quien recibía el dinero al final.

Durante los 60's y a principios de los 70's, la tecnología de redes privadas había permitido el desarrollo de sistemas de Transferencia Electrónica de Fondos (EFT / Electronic Funds Transfer). Estos sistemas han acortado el tiempo de transferencia de la instrucción de pago entre bancos y el proceso reducía su circulación. No cambiaron la estructura fundamental de los sistemas de pago, los sistemas de pago innovadores en las dos décadas pasadas han perseguido minimizar los costos bancarios tal como la reserva de requerimientos, la rapidez del aclaramiento de cheques y minimizar los fraudes. Sin embargo, los clientes, rara vez interactuaban con los sistemas EFT. Las innovaciones recientes en el e-commerce persiguen afectar la manera de cómo los consumidores realizan los tratos con pagos, y parece dirigirse a la transmisión electrónica en tiempo real, aclaramiento y sistemas de pago. Muchas de estas innovaciones ayudan a simplificar el pago del consumidor. Incluyen:

- Innovaciones que afectan a los clientes. Tarjetas de crédito y débito, Cajeros Automáticos (ATM / Automated Teller Machines), tarjetas de almacenamiento de valores, y bancos electrónicos.
- Innovaciones en el comercio online. Efectivo digital, cheques electrónicos, smart cards (monederos electrónicos o tarjetas inteligentes), y las tarjetas de crédito encriptadas.
- Innovaciones que afectan compañías. Los mecanismos de pago que los bancos proveen a clientes corporativos, tales como las transferencias interbancarias a través de Casas Automáticas de Aclaramiento (ACH / Automated Clearing House), las cuales permiten a las compañías pagar a sus empleados por depósito directo.

1.2.5 Cuadro Sinoptico de los Sistemas Electrónicos de Pago

- Electronic Payment Systems / Sistemas de Pago Electrónico
  - Credit Card based Systems / Sistemas basados en Tarjetas de Crédito
    - First Virtual (Primero Virtual)
    - CARI (Collect All Relevant Information / Colecta Toda la Información Relevante)
    - CyberCash (CyberEfectivo)
    - iKP (Internet Keyed Protocol / Protocolo de Llaves en Internet)
    - OpenMarket (Mercado Abierto)
    - SEPP (Secure Electronic Payment Protocol / Protocolo de Pago Electrónico Seguro)
    - SET (Secure Electronic Transactions/ Transacciones Electrónicas Seguras)
  - Electronic Checks / Cheques Electrónicos
    - FSTC Electronic Check Project (Proyecto de Cheque Electrónico FSTC)
    - NetBill (RedFactura)
    - NetCheque (RedCheque)
  - Electronic Cash Payment Systems / Sistemas de Pago de Efectivo Electrónico
    - Ecash(DigiCash)(Eefectivo)
    - CAFÉ (Conditional Access for Europe / Acceso Condicional para Europa)
    - NetCash (RedEfectivo)
    - Cybercoin (Cybermoneda)
    - Mondex
    - EMV Cash Cards (Tarjetas de Efectivo EMV)
    - VisaCash (VisaEfectivo)
  - Micropayment Systems / Sistemas de Micropago
    - Millicent
    - Subscrip
    - Payword (PagoPalabra)
    - iKP Micropayment Protocol (Protocolo de Micropago iKP)
    - Micromint

- Protocolos
  - Capa de Comunicación
    - SSL (Secure Socket Layer)
    - S-HTTP (Secure HTTP / HTTP Seguro)
    - PCT(Private Communication Technology/ Tecnología de Comunicación Privada)
  - Capa de Transporte
    - iKP (Internet Keyed Protocol / Protocolo de Llaves en Internet)
    - NSC
    - STT
    - SEPP(Secure Electronic Payment Protocol / Protocolo de Pago Electrónico Seguro)

1.3 Monografía

COMERCIO ELECTRONICO

El Comercio Electrónico o e-commerce es un servicio de Internet que surge del desarrollo tecnológico y la necesidad de cambios en el mundo empresarial, ya que permite llevar a cabo transacciones comerciales a nivel electrónico, evitando el contacto físico directo

Ventajas del Comercio Electrónico

Proveedores

presencia global
aumento de la competitividad
personalización masiva & amoldamiento
cadenas de entrega más cortas o inexistentes
reducción sustancial de costos
nuevas oportunidades de negocio
presencia global/elección global
creación de nuevos mercados
elimina las barreras comerciales

Consumidores

elección global
calidad del servicio
productos & servicios personalizados
respuesta rápida a las necesidades
reducción sustancial de precios
nuevos productos & servicios
comunicación interactiva
customización
información suficiente para toma de decisiones de compra

Seguridad

Protección de datos contra el acceso no autorizado. Los programas y datos se pueden asegurar entregando números de identificación y contraseñas a los usuarios autorizados de una computadora. Sin embargo, individuos competentes pueden llegar a acceder a estos códigos

Las contraseñas pueden ser verificadas por el sistema operativo, en primer lugar, para impedir la entrada de usuarios en el sistema, o por el software

Los datos transmitidos a través de redes de comunicaciones pueden ser asegurados mediante su cifrado para prevenir infiltraciones

Cifrado: cualquier procedimiento para convertir el texto plano en texto cifrado y el descifrado es lo contrario y convierte el texto cifrado al texto plano. Existen distintos tipos de cifrado

1. Sistemas de no llave. Estos sistemas no utilizan ninguna llave para cifrarse, se basan sólo en su método

2. Sistemas de llave privada o de una sola llave(llave secreta) o simétricos

Estos sistemas utilizan una llave compartida para el cifrado y descifrado. Por ejemplo, si X desea enviarle una factura a Y, X cifra la factura y envía la factura cifrada a Y junto con la llave. Y descifra la factura con la llave acordada para obtener la factura. Los sistemas de llave secreta o privada tienen el problema de distribución de llaves en redes grandes, desde que la llave debe distribuirse firmemente entre las dos partes. Ambas partes deben estar de acuerdo en la llave secreta sin que una tercera parte lo averigue. Cualquiera que intercepta la llave en tránsito puede leer el mensaje cifrado usando la llave.

3. Sistemas de Llave Pública

Este tipo de criptografía proporciona seguridad al comunicar mensajes sobre canales inseguros, tales como las redes. Se tienen dos tipos de llaves que una se relaciona con la otra la llave pública y la llave privada. Al cifrar la información con llave pública sólo puede descifrarse con la llave privada proporcionando el servicio de confidencialidad, por el contrario al cifrar con la llave privada puede ser sólo descifrada con la llave pública correspondiente proporcionando autenticación. La llave pública se mantiene en un recipiente central. Supongase que X desea enviar un mensaje a Y. X busca la llave pública de Y en un directorio. X usa la llave para cifrar un mensaje y se lo envía a Y. Y usa la llave privada para recuperar el mensaje. A menos que alguien tenga acceso a la llave privada de Y, el mensaje enviado a Y sólo puede ser leído por Y. La ventaja de sistemas de llave pública es que los problemas de manejo de la llave son principalmente confinados al manejo de llaves privadas. La necesidad del remitente y el receptor para acordar una llave secreta es eliminado. Todas las llaves deben tener una fecha de expiración que debe escogerse propiamente y publicada a otros usuarios

B) Firmas Digitales

La confidencialidad de datos puede lograrse a través del cifrado del mensaje. La integridad de datos es igualmente importante para el e-commerce. Las firmas digitales, también conocidas como autenticación del remitente, pueden usarse para asegurar integridad de datos. Las firmas digitales requieren un método de firma del documento y un método de verificación que la firma realmente se generó por el remitente. Supóngase que X quiere firmar un documento digitalmente antes de enviarlo. X pone su llave privada y anexa el documento dentro de una función hash para generar un único número llamado firma digital o huella digital, un modelo de bits que identifican un modelo muy grande de bits. Esto se une al documento original y es cifrado con la llave privada de X y enviado a Y. Y primero él descifra el documento que usa la llave pública de X. Entonces Y corre el mismo programa hash en el documento. Si la huella digital resultante es la misma, entonces Y puede estar seguro de que la firma digital es auténtica

Una firma digital sólo puede ser generada por alguien que conoce la llave privada. La comprobación requiere sólo el conocimiento de la llave pública. Para que, X pueda firmar un mensaje sólo X la puede generar. Y simplemente puede verificar que es la firma de X, pero no pueda forjarla. Si el documento se altera durante su transmición, las huellas digitales no serán las mismas al aplicarles la función hash. Si la firma del remitente ha forjado las huellas digitales no se emparejarán. Las firmas digitales, verifican la identidad del remitente y el receptor.

Aspectos de Seguridad

Confidencialidad(Confidenciality). La computadora está enviando un mensaje simplemente a la red, alguien fuera puede leerlo. De lo que se encarga este servicio es de que el mensaje transmitido pueda viajar seguro, sin que otra persona ajena a la transmisión pueda saber el contenido del mensaje.

Integridad(Integrity) El mensaje está enviándose encima de una red abierta, eso se conecta a millones de otras máquinas, no hay convicción que el mensaje que recibió es idéntico al mensaje enviado. Aquí se comprueba que los datos que se envía on y recibieron son los mismos.

Autenticación(Autenticity) Nadie puede estar seguro de las personas con quien ellos están haciendo un intercambio No hay ninguna firma, no voces reconocidas ninguna cara familiar Las computadoras son excelentes para el intercambio de información Permite comprobar que la parte emisora es quien dice ser y viceversa

No repudio(No-Repudiability) Las partes envueltas pueden negar que el intercambio tuvo lugar porque ningun recibo de regreso se recibe Ellos simplemente pueden decir "yo no lo envié "

Sistemas de pago

e-cash

Los sistemas e-cash permiten pagos directos hechos anónimamente, sin usar intermedianos El pago es un mensaje codificado que representa el equivalente cifrado del dinero digitalizado

Los clientes usan dinero local para comprar cierta cantidad de efectivo digital a un banco El banco envia instrucciones al la computadora del usuario, la cual envia la información a los vendedores en Internet DigiCash está intentando autorizar el sistema a los bancos porque requiere el involucramiento directo de un banco Esto sería un obstáculo para hacer este sistema global y flexible

Aclaramiento del pago

Los sistemas de aclaramiento electrónicos se basan en la seguridad de los mensajes, donde compradores y vendedores se comunican entre si mientras envían pagos via un proveedor de servicios de pago que actúa como mensajero intermediario

First Virtual Holdings Ha desarrollado un sistema que une tarjetas de crédito, bancos y agentes procesadores en Internet La ventaja de este sistema es que no requiere mensajes cifrados El sistema de pago es independiente del sistema del banco, depende de las redes "offline" proporcionadas por EDS El comprador envia un mensaje al First Virtual qué lo pasa por EDS, que transfiere una tarjeta de credito/información de la cuenta en el banco y actúa como una cámara de compensación del mensaje EDS pasa la cuenta detalladamente al vendedor Cuando la transacción es confirmada First Virtual envia un mensaje al comprador para confirmar que la transacción y el pago se efectúa

CyberCash Sistema de pago que proporciona electrónicamente los detalles de la tarjeta de crédito Uno de las caracteristicas del sistema desarrollado por CyberCash es que será ' un browser independiente '. Los usuarios de CyberCash deben transmitir primero las copias del software del CyberCash web server Una vez ordenadas se ha colocado con el vendedor, al cliente se le envia una detallada factura online. Esto contiene información de la compra, y un estado que confirma los cargos, donde el cliente agrega su número de la tarjeta de crédito Esta información se envía entonces al vendedor de menera cifrada junto con la factura original. El vendedor agrega información de identificación y se lo envia a CyberCash. CyberCash da de alta una tarjeta del crédito normal o una autonzación de débito del banco del vendedor. Después de que la petición de la autorización se ha procesado, CyberCash responde al vendedor que se ha completado la transacción. El CyberCash es automatizado y corre en el Internet file server

credit cards

Las grandes compañías de tarjetas de crédito, VISA Internacional, MasterCard y American Express, junto con Microsoft, IBM, NetScape, SAIC, GTE, Verisign y Terisa System desarrollarón un estándar para las transacciones en Internet, su nombre es SET, (Secure Electronic Transaction/Transacciones Electrónicas Seguras) que hace que las compras en Internet sean seguras, como al usar una tarjeta del crédito en una tienda normal SET se basa en tecnologías de cifrado especialmente en el RSA Data Security SET incluye certificados digitales que sirven para verificar que el tarjetahabiente real está haciendo el compra

Todas las partes están de acuerdo que la seguridad del pago no es un problema competitivo y un estándar global es la única manera de establecer segundad en Internet La adopción para vendedores y compradores será más fácil con un estándar el que también significa menos posibilidad de fraude

Primero el comprador debe registrar la tarjeta de crédito online con su banco El comprador llena una forma de registro con nombre, número de la tarjeta, fecha de expiración y dirección del cargo de la cuenta. La información es entonces cifrada y enviada de regreso al banco El emisor verificará la cuenta y entonces emitirá un certificado electrónico poniendo un firma digital en el certificado digital que demuestra que la tarjeta es válida. El comprador guarda el certificado en su computadora para el uso futuro. Los vendedores también deben registrarse para participar en el sistema. Ellos llenan una forma con información básica información online. Entonces el banco del vendedor emitirá un certificado digital que les permite realizar el Comercio Electrónico

Para poder comprar un producto, el vendedor debe mostrar al cliente que él tiene un certificado. Este puede ser hecho por e-mail, o publicar una copia en Internet para que todos podamos verla. Cuando el comprador ve que los vendedores tienen un certificado, él puede hacer un pedido electrónico a la tienda La tienda busca autorización para la cantidad de dólares de la compra. Una vez confirmada, se procasa la orden.

Protocolos de Seguridad

- SHTTP (Secure Hypertext Trasfer Protocol)

Desarrollado por EIT en Norte América entre 1994 y 1995 pero fue más renombrado hasta 1996. Sólo provee seguridad a trasferencias HTTP y es menos flexible que el SSL pero quizá no se enfoque en la importancia del mercado de las tarjetas de crédito como el SET, quizá cae entre las distintos objetivos del SSL y el SET

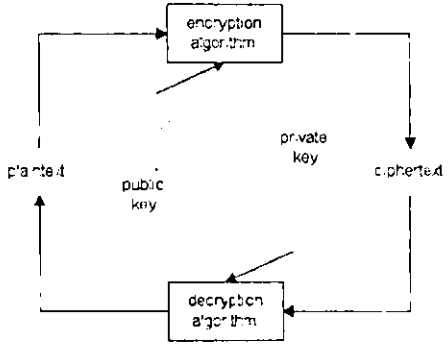
- SSL (Secure Sockets Layer)

Es una aproximación de Netscape para proveer comunicaciones seguras Es un protocolo sobre la capa TCP/UDP y abajo del HTTP, FTP, Telnet Gopher y otras aplicaciones orientadas a protocolos Este protocolo provee autenticación por medio del RSA y cifrado con el algoritmo RC4

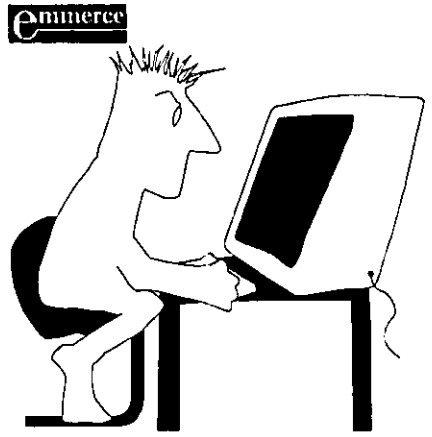
DISTINTOS SISTEMAS DE PAGO

COMERCIO ELECTRONICO

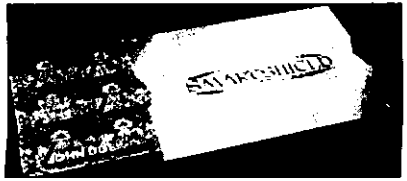
CYBERCASH



ESQUEMA DE CIFRADO CON LLAVE PUBLICA

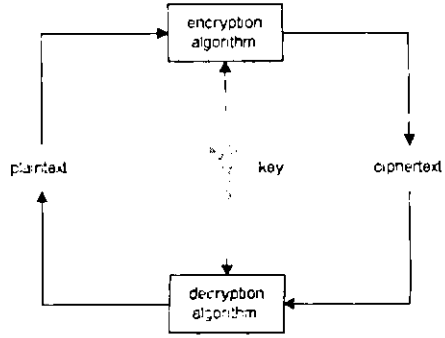


COMERCIO ELECTRONICO EN INTERNET



SMARTCARDS

SISTEMA DE PAGO MONEDA ELECTRONICA



ESQUEMA DE CIFRADO CON LLAVE SECRETA

1.4 Definiciones

En esta parte dare una definición de todos los elementos involucrados en el título de mi investigación "Seguridad en los Sistemas de Pago Electrónicos en el E-commerce".

1.4.1 Etimólogicas

1.4.1.1 Breve Diccionario Etimológico de la Lengua Castellana

Seguro Del latín secûrus 'tranquilo, sin cuidado, sin peligro'. Derivado privativo de cura 'cuidado'. Cualidad de seguro.

En Preposición derivada del latín in 'en, dentro de, en adelante, en la locución'.

Los Sistemas

De Del latín de 'desde arriba, debajo de, desde,(apartándose) de'

Pago Derivado del latín Pacare 'contentar, satisfacer' derivado de pax –cis, 'pag' Abono de una cantidad.

El Artículo, del latín ille 'aquel'

Comercio Tomado del latín commercium id. Derivado de merx, -cis 'mercancía'. Negocio, trato.

Electrónico Derivado culto del griego elektron 'ambar', por la propiedad que tiene esta sustancia de atraer eléctricamente al frotarla.

1.4.1.2 Novisimo Diccionario Español-Latino

Seguridad **Estado de las cosas que las hace firmes, ciertas, seguras y libres de todo riesgo. Securitas, firmitas, atis.**

2. Salvo conducto, fe pública. Fides, ei
3. Sosiego, tranquilidad de ánimo. Securitas, animi tranquillitas; cuararum requies.
4. Certeza, infalibilidad. Confidentia ae ceritudo, inis, securitas, atis.
5. Fianza, obligación de satisfacer por otro. Fidei cautivo; satisdatio, onis. Aqui no tenemos seguridad. No estamos seguros Non sumus hie in tuto. Dame seguridad de tu palabra. Promissi tui cedo mihi pignos. Tomar seguridad de alguno Fidem ab aliquio capere Puesto que el derecho le daba tan poca seguridad. Ubi in jure parum praesidii esset Devolver la seguridad, la calma a los espíritus Metu animos solvere. Tiembla, (esto es tiene miedo) cuando se encuentra en completa seguridad. Omnia tuta timet.

En **Significado el lugar y tiempo en que se hace algo. In.**

Los Sistemas **Del latín systema, atis. Conjunto y enlace de principios, máximas y conclusiones relativas a una materia.**

Suposición, hipótesis de cierto estado de una cosa. Systema.

Ast. La colocación y orden que tienen entre si el globo de la tierra y los cuerpos celestes. Mundi systema. El galón de oro o de plata de una sola cara Aureaargenteave fasciola

unam tantum faciem preferens. Músico. La recta ordenación o disposición de las cuerdas ó voces usadas en la música. Musicum systema. Se siguió para los comicios un sistema enteramente distinto. Comitia longe diversa fata sunt. El sistema que siguen los penpatéticos en la exposición de sus ideas. Consuestudo peripateticorum in ratione dicendi. ¿Qué sistema de defensa emplearía yo.? Quod iter defensionis ingrederer.

De Pago **Entrega de dinero que se debe. Solutio, luitio, oni; pecuniae traditio.**
2. Recompensa, premio,. Remuneratio, retributio, onis; merces, edis; relata gratia.
3 Satisfacción de la ofensa. Luitio.
4. El distrito determinado de heredades, especialmente de viñas. Satum arcvum.
5. Adjetivo Fam. Pagado. Sulutus, stasfactus, a, um. En pago adverbio Retributions causa. Buen bago me diste. Praeclaram sane mihi gratiam retulisti. Sus costumbres le darán el pago. Ulciscentur illi more sui. Dar el pago. Corresponder mal al beneficio. Preperam retribuere.

El **Articulo masculino ille.**

Comercio **El tráfico de géneros. Mercatura, ae; commercium, ii; negotiatio, onis.**
2. Comunicación de unas gentes con otras. Commercium, ii; communicatio, onis; societas, atis.
3. Cueroi i cinoañia de comerciantes. Mercatorum societas.
4 Trato secreto o ilícito entre dos personas de distinto sexo. Turpe commercium.
5. El paraje más concurrido de las gentes en los pueblos grandes. Frequens locus. Juego de naipes Chartarum ludus duplicibus pagellis instructus.

Electrónico **De eléctrico. Ambar, betún amarillo. Electrum, i; Phaetonis gutta. Abundante de Electrifer, a, um. Hecho de electro. Electrus, electrinus, a, um.**
2. Metal de cuatro partes de oro y una de plata. Electrum.

1.4.2 Diccionario de la Real Academia Española

Seguridad (del latín securitas, -atis) Cualidad de seguro.
2 Fianza u obligación de indemnidad a favor de uno, regularmente en materia de intereses
3. de seguridad loc. Adjetivo Que se aplica a un ramo de la administración pública cuyo fin es el de velar por la seguridad de los ciudadanos. Dirección General, Agente de Seguridad.
4 **Se aplica también a ciertos mecanismos que aseguran algún buen funcionamiento, precaviendo que éste falle, se frustre o se violente. Muelle, cerradura de seguridad.**

En (del latín in) Preposición que indica en qué lugar, tiempo o modo se realiza lo que significan los verbos a que se refiere. Pedro está En Acapulco, esto sucedió En Pascua; tener En depósito
2. Algunas voces, Sobre. El rey te ha dado una pensión En la renta del tabaco
3. **Indica a veces aquello en que se ocupa o sobresale una persona.** Doctor **En Medicina, trabajar En Bioquimica.**
4 A veces, indica situación en tránsito, En prensa, En proyecto.
5. Con verbos de percepción como conocer, descubrir, etc y seguida de un sustantivo, por. Lo conocí En la voz
6. Seguida de un gerundio, luego que después que, En poniendo el general los pies en la playa, dispara la artillería
7 Denota el término de algunos verbos de movimiento Caer En un pozo, entrar En casa
8. Ant. Con Alegrarse En una nueva

Los **(del latín illos, acus. Pl. m. de ille). Forma del artículo determinado en género masculino y número plural.**

2. **Acusativo del pronombre personal en tercera persona en generó masculino y número plural. No admite preposición y se puede usar como enclítico. Los mire; miraLos. Emplear en este caso la forma les, propia del dativo, es tolerable como objeto directo de persona.**

Sistema **(del latín systema) Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí.**

2. **Conjunto de cosas que ordenadamente relacionadas entre sí contribuyen a determinado objeto.**
3. Biol. Conjunto de órganos que intervienen en alguna de las principales funciones vegetativas. Sistema nervioso.
4. Ling. La lengua en su totalidad, así como cada uno de sus sectores (fonológico, gramatical y léxico) considerados como conjuntos organizados y relacionados entre sí.

acusatorio. Der. Ordenamiento procesar que veda al juzgador exceder la acusación en la condena, o le exige para hacerlo oír previamente a las partes.
astático. El formado por dos agujas imantadas que se colocan con los polos invertidos y los ejes paralelos para que aquel resulte insensible a la acción directriz de la Tierra.
degesimal. El que tienen por unidades fundamentales el centímetro, el gramo y el segundo.
cristalográfico. Fís. Y Mineral. Grupo de formas cristalinas, que queda definido por sus ejes cristalográficos y elementos de simetría que presentan.
de numeración El que permite representar y denominar cualquier número con un conjunto limitado de signos y nombres.
experto. Inform. Programa de computador que permite a éste dar respuestas semejantes a las que daría un experto en la materia.
Inquisitivo. Derecho. El que, a diferencia del acusatorio, permite al juzgador exceder la acusación y aun condenar sin ella.
Métrico decimal. El de pesas y medidas que tiene por base el metro y en el cuál las unidades de un misma naturaleza son 10, 100, 1000,10000 veces mayores o menores que la unidad principal de cada clase. Dícese comúnmente sistema métrico.
nervioso. Anatomía. Conjunto de órganos, de los que unos reciben excitaciones del exterior, otros las transforman en impulsos nerviosos, y otros conducen estos a los lugares del cuerpo en que han de ejercer su acción .
Operativo. Informática. Programa o conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático, y permite la normal ejecución del resto de las operaciones.
periódico. Química. Cuadro en el que están ordenados los elementos químicos según su número atómico y dispuesto de tal modo que resulten agrupados los que poseen propiedades químicas análogas.
planetario. Conjunto del Sol y sus planetas, satélites y cometas.
solar , sistema planetario
por sistema. Loc. Adverbio. Procurando obstinadamente hacer siempre cierta cosa, o hacerla de cierta manera sin razón o justificación Me contradice Por Sistema

De (del latín de) Preposición denota posesión o pertenencia. La casa De mi padre

2 Sirve para crear diversas locuciones de modo Almorzó **de** pie, le dieron de puñaladas; se viste **de** prestado, lo conozco **de** vista.
3. Manifiesta de donde son, vienen o sales unas cosas o las personas La piedra es **de** Colmenar, vengo **de** Pachuca, no sale **de** casa
4 Sirve para denotar la materia de que está hecha una cosa El vaso **de** plata, el vestido **de** seda
5 Señala lo contenido en una cosa Un vaso **de** agua, un plato **de** asado
6. Indica también el asunto o materia. Este libro trata **de** la última guerra, una clase de matemáticas, hablaban de la boda
7. **En ocasiones indica la causa u origen de algo. Murió De viruelas; la fiebre Del heno.**
8 Expresa la naturaleza, condición o cualidad de personas o cosas Hombre **de** valor;

entrañas **de** fiera.
9. Sirve para determinar o fijar con mayor viveza la aplicación de un nombre apelativo. El mes **de** noviembre; la ciudad **de** Guadalajara
10. Desde, punto en el espacio y en el tiempo. **de** Los Cabos a Palenque; abierto **de** nueve a una.
11. Algunas veces se usa precedida de sustantivo, adjetivo o adverbio, y seguida de infinitivo. Es hora **de** caminar; harto **de** trabajar; lejos **de** pensar
12. Seguida de infinitivo, adquiere un valor condicional **de** saberlo antes, habría venido.
13. Precedida de un verbo, sirve para formar perífrasis verbales. Dejó **de** estudiar; acaba **de** llegar.
14. Con ciertos nombres sirve para determinar el tiempo en que sucede una cosa. **de** madrugada; **de** mañana; **de** noche; **de** viejo; **de** niño
15. Se emplea también para reforzar un calificativo. El bueno **de** Pedro, el pícaro Del mozo; la taimada **de** la patrona.
16. Algunas veces es nota de ilación. **de** esto se sigue. **de** aquello se infiere.
17. En ocasiones tiene valor partitivo. Dame un poco **de** agua.
18. Precediendo al numeral uno, una, denota la rápida ejecución de algunas cosas **de** un trago se bebió la tisana; de un salto se puso en la calle acabemos **de** una vez.
19. Colócase entre distintas partes de la oración con expresiones de lástima, queja o amenaza ¡Pobre **de** mí!, ¡Ay **de** los vencidos!
20. Sirve para la creación de locuciones prepositivas a partir de adverbios, nombres, etc. Antes **de**; respecto **de**, alrededor **de**; a diferencia **de**
21. Puede también combinarse con otras preposiciones **de** a tres, **de** a bordo, **de** por sí, por **de** pronto, tras **de** sí.
22. Se usa en ciertas construcciones con el agente de la pasiva. Acompañado **de** sus amigos; dejado **de** la mano de Dios; está abrumado **de** deudas
23. Introduce algunas veces el término de la comparación. He comido más **de** lo debido; es peor **de** lo que pensaba; ahora escribe más **de** veinte artículos al año.
24. Conjunción. Lo hizo **de** intento.
25. Para. Gorro **de** dormir; ropa **de** deporte.
26. Por. Lo hice **de** miedo.

Pago Entrega de un dinero o especie que se debe.
2. Satisfacción , premio o recompensa.
3. V. Carta de pago.
4. V. balanza, de papel de pagos.
5. V. dación de pago.
   Dar el pago. Fr. fig. que se usa para avisar a uno que le sobrevendrá o sobrevino el daño correspondiente o que naturalmente se sigue a los vicios o imprudencias
6. Fig. Corresponder mal al beneficio o servicio recibido
   En pago. Loc. Adverbio. fig. En satisfacción, descuento o recompensa
   cumplir, satisfacer.

El (Del Latín ille) Artículo determinado en masculino singular

Comercio (Del Latín commercium) **Negociación que se hace comprando y vendiendo o permutando géneros o mercancías.**
2. V. artículo, balanza, banco, corredor, libertad de comercio
3. Desus. Comunicación y trato de unas gentes o pueblos con otros
4. En algunas poblaciones, lugar en que, por abundar las tiendas, suele ser grande la concurrencia de gentes.
5. Tienda , almacén, establecimiento comercial
6. Juego de naipes entre cuatro o más personas, que ponen cada una de caudal cuatro o cinco monedas. Gana el que junta tres cartas de un palo superiores a las de los demás.
7. Cierto juego de naipes entre varias personas que se juega con dos barajas
8. Fig. Conjunto o la clase de comerciantes

9. Fig. Comunicación y trato secreto, por lo común ilícito, entre dos personas de distinto sexo
10. de cabotaje, cabotaje, tráfico marítimo en las costas

Electrónico De electron. Perteneciente o relativo a electrón,

2. **Perteneciente a la electrónica (Ciencia que estudia dispositivos basados en el movimiento de los electrones libres en el vacío, gases o semiconductores, cuando dichos electrones están sometidos a la acción de los campos electromagnéticos.**

1.4.3 Diccionario Informático

1.4.3.1 Diccionario Enciclopédico de la Informática

Seguridad **Protección de la información contra su uso sin autorización; los programas y datos pueden asegurarse asignando números de identificación y contraseñas a todos los usuarios autorizados del sistema; sin embargo, el programador de sistemas también puede tener eventualmente conocimientos en dichos códigos. Las contraseñas se pueden verificar por el sistema operativo, el sistema de administración de la base de datos y otras aplicaciones autónomas que se ejecutan en la computadora (ordenador). La información que se transmite por canales de comunicación puede encriptarse o codificarse par mayor seguridad.**

Electrónico **Relativo a la rama de la ciencia que se refiere al comportamiento de los electrones. En general, es lo perteneciente a todo dispositivo que depende principalmente del funcionamiento de tubos al vacío o de gas, dispositivos transistorizados o válvulas termoiónicas. La esencia de la tecnología de las computadoras (ordenadores) consiste en el uso selectivo y la combinación de los aparatos electrónicos en donde se permite que la corriente fluya o se detenga mediante interruptores electrónicos trabajando a altas velocidades.**

1.4.4 Otros Diccionarios

1.4.4.1 Diccionario Enciclopédico Universal (EspasaCalpe)

Seguridad Sinónimo Calma, certeza, protección, fianza; Ant. Desorden , incertidumbre

1. **F. Calidad de seguro.**
2. Fianza u obligación de indemnidad a favor de uno.
3. De seguridad. Fr. Que se aplica a un ramo de la administración pública cuyo fin es el de velar por la Seguridad de los ciudadanos.

En

1. **Preposición Que indica en que lugar, tiempo o modo se determinan las acciones de los verbos a que se refiere. Pedro está En Chihuaha; esto sucedió En Navidad; Juan se disipa En profusiones.**
2. Algunas voces, Sobre El rey te ha dado una pensión En la renta del tabaco
3. Seguida de un infinitivo, Por. Le conocí En el andar

Los

1. **Artículo determinado en género masculino y número plural.**
2. Acusativo del pronombre personal de tercera persona en género masculino y número plural.
3. Emplear en este caso la forma les, propia del dativo, es grave incorrección

Sistema Conjunto de reglas o principios enlazados entre sí.
2. **Conjunto de cosas que ordenadamente relacionadas entre sí contribuyen a determinado objeto.**
3. Conjunto de órganos que intervienen en alguna de las principales funciones vegetativas y animales.

De
1. **preposición Denota posesión o pertenencia. La casa De mi padre.**
2. Explica el modo de hacer varias cosas, de suceder otras, etc. Almorzó **de** pie; le dieron **de** puñaladas.
3. Manifiesta de dónde son, vienen o salen las cosas o las personas. La piedra es **de** Zacatecas; vengo de trabajar; no sale **de** casa.
4. Sirve para denotar la materia de que está hecha una cosa. El vaso **de** plata.
5. Demuestra lo contenido en una cosa. Un vaso **de** agua
6. Indica y también el asunto o materia de que se trata ¿Habla usted **de** mi pleito?
7. **Expresa la naturaleza, condición o cualidad de personas o cosas. Hombre De valor.**
8. Conciertos nombres sirve para determinar el tiempo en que sucede una cosa. **de** madrugada.
9. Se emplea también para esforzar un calificativo. El bueno **de** Pedro.
10. Algunas veces es nota de ilación. **de** aquello se infiere.
11. Precediendo al numeral uno, una, denota la rápida ejecución de algunas cosas. **de** un trago se bebió la tisana.
12. Colócase entre dsitintas partes de la oración con expresiones de lástima, queja o amenaza ¡Pobre **de** mi hermano!

Pago(Paga) Sinónimo Sueldo. F. Acción de pagar o satisfacer una cosa.

El Art. determinado en género masculino y número singular.

Comercio Sinónimo Negocio, tienda, comunicación.
1. **Negociación que se hace comprando, vendiendo o permutando unas cosas por otras.**
2. Tienda, almacén, establecimiento comercial.

Electrónica (o) Ciencia que estudia dispositivos basados en el movimiento de los electrones libres en el vacío, gases o semiconductores, cuando dichos electrones están sometidos a la acción de los campos electromagnéticos.

1.4.5 Definición de Autores

Comercio Electrónico

Metodología comercial Moderna a la que se dinge las necesidades de organizaciones, comerciantes, y consumidores

- Bajos costos
- Mejoran calidad de género y servicios
- Aumentan velocidad de entrega de servicio

Sistemas de Pago Electrónico (Kalakota, Ravi): Los pagos electrónicos. son un intercambio financiero que toma lugar en inea ente compradores y vendedores El contenido de este intercambio es usualmente una forma de instrumento financiero digital (números de tarjeta de crédito encriptados, cheques electrónicos o dinero digital) que es regresado por un banco, un intermediario, o por una persona que tenga poder legal.

1.4.6 Definición Propia de "Seguridad en los Sistemas de Pago Electrónico en el e-commerce"

Capacidad de ciertos mecanismos, que permiten el intercambio financiero de cantidades monetarias electrónicamente entre compradores, vendedores y bancos (opcionalmente se involuctra otra entidad), por una transacción de compraventa realizada en Internet. Uno de los objetivos principales de estos mecanismos es el de proteger la información referente al pago.

1.4.7 Sinónimos

Seguridad En Los	Invulnerabilidad, protección
Sistemas De	Procedimiento, método
Pago El	Retribución, gratificación
Comercio Electrónico	Negocio, trato Electricidad, corriente

1.4.8 Antónimos

Seguridad En Los	Indefenso, inseguro
Sistemas De	anarquía
Pago El	Cobro
Comercio Electrónico	

1.4.9 Denominación en otros Idiomas

1 4 9 1 Inglés

Seguridad En Los	security in the
Sistemas De	systems of
Pago El	payment the
Comercio Electrónico	commerce electronic

1 4 9 2 Italiano

Seguridad	la sicurezza
En	Nei
Los	
Sistemas	Sistemi
De	Di
Pago	pagamento
El	
Comercio	del commercio
Electrónico	elettronico

2. MÉTODOS CRIPTOGRÁFICOS

2.1 Criptografía y Conceptos Fundamentales

La palabra criptografía proviene del griego kryptos, que significa ocultar y gráphein escribir, es decir, es la ciencia y arte de escribir para que sea indescifrable el contenido del texto escrito. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "ocultar" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después sólo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o descencriptar)

La criptografía se divide en dos grandes ramas, la criptografía de llave privada o simétrica y la criptografía de llave pública o asimétrica.

Para poder entender un poco de la criptografía, es tiempo de plantear que tipo de problemas resuelve ésta. Los principales problemas de seguridad que resuelve la criptografía son. la privacidad, la integridad, la autenticación y el no repudio

Privacidad: Se refiere a que la información sólo pueda ser leída por personas autorizadas. En la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de comunicación. Por lo tanto al cifrar (ocultar) la información cualquier intercepción no autorizada no podrá entender la información. Esto es posible si se usan técnicas criptográficas, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

Integridad: Se refiere a que la información no pueda ser alterada en el transcurso de ser enviada. En Internet las compra se pueden hacer desde dos ciudades muy distantes, la información tiene necesariamente que viajar por una línea de transmisión de la cual no se tiene control, sino existe integridad podrían cambiarse por ejemplo el número de una tarjeta de crédito, los datos del pedido en fin información que causaría problemas a cualquier comercio y cliente. La integridad también se puede solucionar con técnicas criptográficas particularmente con procesos simétricos o asimétricos.

Autenticidad: Se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba. Por internet es muy fácil engañar a una persona con quien se tiene comunicación respecto a la identidad, resolver este problema es por lo tanto muy importante para efectuar comunicación confiable. Las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes, usan quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, de algún modo ésta reemplaza a la firma autógrafa que se usa comúnmente Para autenticar mensajes se usa criptografía simétrica

No repudio: Se refiere a que no se pueda negar la autoría de un mensaje enviado

Cuando se diseña un sistema de seguridad, una gran cantidad de problemas pueden ser evitados si se puede comprobar autenticidad, garantizar privacidad, asegurar integridad y evitar el no repudio.

La criptografía simétrica y asimétrica conjuntamente con otras técnicas, como el buen manejo de las llaves y la legislación adecuada resuelven satisfactoriamente los problemas planteados anteriormente

Cifrado y Descifrado

Un mensaje normal es denominado texto claro o texto plano. El proceso de ocultar un mensaje se le llama encripción o cifrado y su resultado es el texto cifrado. El proceso en reversa (descifrado o decripción) toma el texto cifrado como entrada y regresa el texto plano original.

El texto plano es denotado por P, mientras que el texto cifrado es denotado por C. La función de encripción E opera en P para producir C:

$$E(P) \quad C$$

En el proceso inverso, la función de decripción D opera en C para producir P:

$$D(C) \quad P$$

Un algoritmo criptográfico, también llamado cifrador, es una función matemática usada para cifrar y descifrar. Todos los algoritmos modernos de cifrado usan una llave, denotada por K. El valor de esta llave afecta a las funciones de cifrado y descifrado, así que ellos pueden ser escritos como:

$$EK(P) \quad C$$
$$DK(C) \quad P$$

El principal propósito de la criptografía ha sido guardar el texto plano escondiéndolo de sus adversarios. El criptoanálisis es la ciencia de recuperar el mensaje de texto plano sin el conocimiento de la llave. Los ataques a un cnptosistema pueden ser:

1. Texto cifrado o solo ataque. En este ataque, el criptoanalista tiene el texto cifrado C de muchos mensajes M, los cuales han sido cifrados usando la misma llave de cifrado. De esto el criptoanalista intenta deducir ambos el texto plano P y la llave K.

2. Ataque de texto plano conocido: El criptoanlista tiene acceso no sólo al texto cifrado C de muchos mensajes M pero también al correspondiente texto plano P. De esta forma quizá sea posible descubrir la llave K usada para encriptar los mensajes M

3. Ataque de texto plano escogido: El criptoanalista tiene acceso al texto cifrado C y asociado al texto plano P para muchos mensajes M, puede ganar acceso al texto cifrado C correspondiente al texto plano P que ha escogido. Esos bloques podrían ser escogidos para producir más información acerca de la llave K u otro monedero en una línea particular de ataque

4 Texto cifrado escogido: El criptoanalista es capaz de escoger repetidamente texto cifrado C para ser decriptado, y tienen acceso al texto plano P resultante. De esto ellos pueden tratar de deducir la llave K.

Se pueden atacar por medio del método de fuerza bruta, el cual es una prueba de los valores de todas las llaves posibles hasta que la correcta es encontrada.

Ciclo de Vida de una Llave

Las llaves deben tener una fecha de expiración. De esta forma, es más difícil que los algoritmos que las utilizan sufran algún ataque. Por ejemplo:

1 Un intruso puede almacenar texto cifrado con objeto de averiguar la llave. Si la llave expira, el texto cifrado almacenado ya no sirve
2 La llave puede haber sido ya averiguada, pero el ataque puede ser, hasta la fecha, pasivo.

3. Las técnicas de análisis de los algoritmos criptográficos (como resolver el problema de la factorización en el caso del algoritmo RSA, por ejemplo) avanza constantemente. El tamaño de las llaves debe ir incrementándose para evitar este tipo de riesgos (por tanto hay que cambiar la llave).

Cuando una llave ha sido averiguada por intrusos, se dice que ha sido comprometida.

El ciclo de vida de una llave incluye los siguientes períodos:

1. **Generación** y, quizá, registro de la llave o par de llaves. La llave o par de llaves deben ser generadas por su propietario o por la entidad que vaya a utilizar las llaves para proteger sus comunicaciones con el usuario. Un problema frecuente radica en que los algoritmos generadores aleatorios de llaves no son suficientemente "buenos". Si la llave es utilizada con algoritmos de criptografía de llave asimétrica, la llave pública puede ser registrada (generando un certificado).
2. **Distribución de las llaves.** En el caso de criptografía de llave simétrica, la llave debe ser entregada al interlocutor de forma que no pueda ser interceptada por terceros. En caso de utilizar llaves asimétricas, la distribución de esta llave está libre de problemas. Sin embargo, debe poder asegurarse que la llave corresponda a quien dice ser su propietario (mediante un certificado, o bien obteniendo la llave de una organización en la que se tenga plena confianza).
3. **Emisión y expiración.** La fecha de emisión determina a partir de qué instante va a ser válida la llave. En general, se trata del momento en el que ha sido generada (o certificada, en su caso). La expiración puede tener lugar al final de una comunicación concreta o en una fecha determinada. En el caso de la criptografía de llave pública, debe verificarse siempre en el certificado que la llave siga siendo válida.
4. **Retirada.** Si se sospecha, por cualquier motivo, que la llave ha sido comprometida, ha de acudirse a la autoridad de certificación para comunicárselo y que ésta proceda a certificar una nueva llave.
5. **Terminación.** Una vez que la llave finaliza su ciclo de vida, se almacena y es reemplazada por una nueva.

Operaciones usadas por Algoritmos

- **Substitución:** En esta operación se reemplazan los bits en texto plano con otros bits decididos por el algoritmo, para producir el texto cifrado. Un carácter de texto plano podría corresponderle un número de caracteres de texto cifrado (substitución homofónica), o cada carácter de texto plano es substituido por un carácter de posición correspondiente en una longitud de otro texto (cifrado generado).
- **Transposición o permutación:** No altera ninguno de los bits de texto plano, en vez de esto mueve sus posiciones dentro de éste. Si el resultado de texto cifrado es entonces pasar a través de muchas transposiciones, el resultado final, es altamente inseguro.
- **XOR:** es una operación or exclusiva. Es un operador booleano por lo que si uno de dos bits es verdadero, entonces el resultado también lo es, pero si ambos son verdaderos o falsos el resultado es falso

```
0 XOR 0 = 0
1 XOR 0 = 1
0 XOR 1 = 1
1 XOR 1 = 0
```

2.2 Criptografía Simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la llave correspondiente que llamaremos llave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía se conoce también como criptografía de llave secreta.

Existe una clasificación de este tipo de criptografía en tres familias, la criptografía simétrica de bloques (block cipher), la criptografía simétrica de flujo (stream cipher) y la criptografía simétrica de resumen (hash functions)

Aunque con ligeras modificaciones, un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas.

La criptografía simétrica ha sido la más usada en toda la historia, ésta ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar, de tal modo que sólo conociendo una llave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de iteracciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, DES.

2.2.1 DES

En mayo de 1973 la National Bureau of Standards (oficina nacional de estándares o NBS por sus siglas en inglés) publicó una solicitud de propuestas para algoritmos criptográficos para proteger la transmisión y almacenamiento de datos.

La NBS esperó, pero no hubo respuestas, al menos no inicialmente. Fue hasta el 6 de agosto de 1974 que la IBM entregó su algoritmo candidato. Este algoritmo, conocido internamente en la IBM con el nombre código de "LUCIFER", fue evaluado por la NBS y adoptado con una modificación como el nuevo Estándar de Encriptamiento de Datos (Data Encription Santdard o DES) hasta el 15 de julio de 1977.

El algoritmo satisface los siguientes criterios:

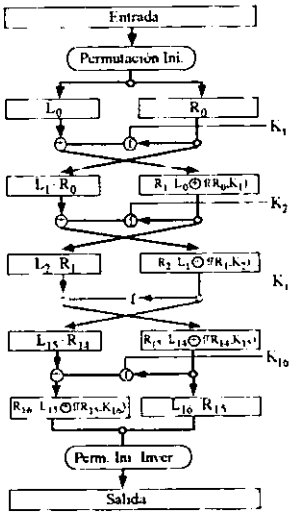
- Provee un alto nivel de seguridad.
- La seguridad depende de las llaves, no de la privacidad del algoritmo.
- La seguridad es capaz de ser evaluada.
- El algoritmo es completamente especificado y fácil de entender.
- Es de uso eficiente y adaptable.
- Debe ser disponible para todos los usuarios.
- Debe ser exportable.

Algoritmo

DES es un algoritmo de cifrado en bloque con una longitud de llave de 64 bits, opera en un solo pedazo de datos a la vez, cifrando bloques de 64 bits (8 bytes) de texto plano para producir 64 bits de texto cifrado. Siendo simétrico, la misma llave es usada para encriptar y decriptar, y usa el mismo algoritmo para los procesos antes descritos.

Se lleva acabo una permutación inicial, el bloque de 64 bits de texto plano P se divide en dos bloques de 32 bits uno izquierdo L_0 y otro derecho R_0, y realiza 16 vueltas de cifrado bajo el control de la llave. La primera iteración reordena los bits del bloque de entrada de 64 bits para aplicar un arreglo de permutaciones. La última iteración es el inverso de su permutacion. La penúltima iteración al final intercambia los 32 bits del lado izquierdo con los 32 bits de lado derecho.

En cada iteración, el algoritmo toma dos entradas de 32 bits y produce dos salidas de 32 bits. La salida de la izquiera es simplemente una copia de la entrada de la derecha. A la entrada de la derecha se le aplica la función f y la llave por el paso K_n, a la salida se le aplica un or exclusivo (XOR) junto con la entrada de la izquierda que es el resultado del lado izquierdo de la siguiente iteración. La complejidad radica en la función f, que hace un número de sustituciones y permutaciones usando cajas S (para las sustituciones) y cajas P (para las permutaciones). El descifrado en este algoritmo usa la misma secuencia de paso, pero las llaves usadas en cada una de las iteraciones son aplicadas en orden inverso.



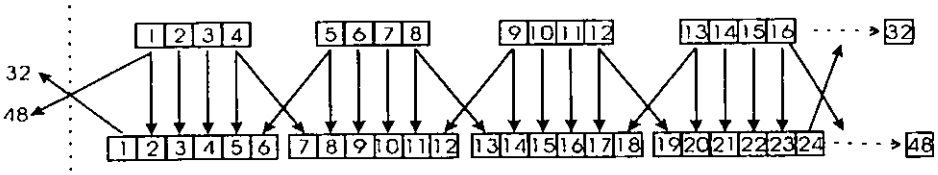
Cada iteración consite en:

Transformación de la llave: Los 64 bits de la llave son reducidos a 56 removiendo cada 8 bits un bit (los 8 bits sobrantes son usados como bits de paridad). Dieciseis diferentes subllaves de 48 bits son creadas en cada iteración. Esto se logra dividiendo la llave de 56 bits en dos mitades, y entonces circularmente cambian entre ellos 1 ó 2 bits, dependiendo de la iteración. Después, 48 de estos bits son seleccionados. Porque se cambian, diferentes grupos de bits de llave son usados en cada subllave.

Expansión de la permutación: Después de la transformación de la llave, cualquier mitad del bloque será operada para sufrir una permutación de expansión. En esta operación, la expansión y la transposición se logran simultaneamente permitiendo que el primer y cuarto bit en cada bloque de 4 bits aparezcan dos veces en la salida.

La permutación de expansión logra tres cosas.

1. Incrementar el tamaño de los bloques de 32 a 48 bits, el mismo numero de bits son el conjunto de subllaves.
2. Produce un gran cadena de datos para las operaciones de substitución que subsecuentemente lo comprimen
3. En las substituciones subsecuentes el primer y el cuarto bits aparecen en las cajas S, ellas afectaran dos substituciones



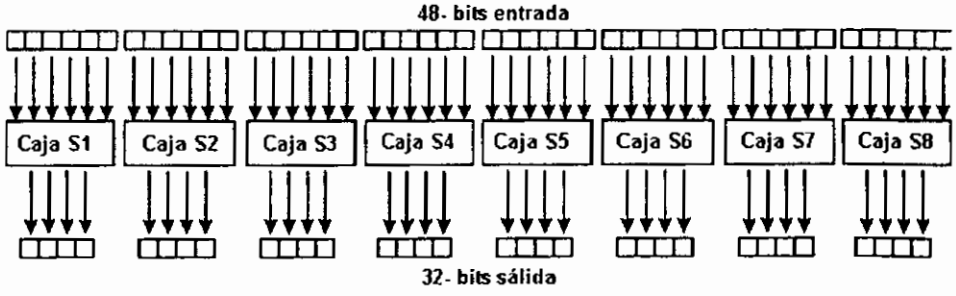
XOR: El bloque de 48 bits resultante se le aplica el XOR con el apropiado subconjunto de llaves para esa iteración

Subtstitución: Hay 8 cajas de substitución, llamadas cajas S. La primer caja S opera con los primeros 6 bits del bloque expandido de 48 bits, la segunda con los 6 siguientes, y así sucesivamente. Cada caja S opera desde una tabla de 4 filas y 16 columnas, cada entrada en la tabla es un número de 4 bits. El número de 6 bits es tomado por la caja S como entrada para buscar la apropiada entrada en la tabla. El primer y sexto bits son combinados para formar un número de 2 bits correspondientes al número de fila, y el segundo y quinto bits son combinados para formar un número de 4 bits que corresponde a una columna. El resultado obtenido de la substitución es de ocho bloques de 4 bits que son combinados dentro de un bloque de 32 bits.

La relación es no lineal en las cajas S que provee DES con su seguridad, los demás procesos dentro del algoritmo DES son lineales.

Después de que las iteraciones han sido completadas, los dos bloques de 32 bits son recombinados para formar una sálida de 64 bits, la permutación final es ejecutada, y el bloque de 64 bits resultante es el texto cifrado con encripción DES para el bloque de texto plano de entrada

Decripción: Se usa el mismo algoritmo de encripción para descifrar el texto, lo único cambiante es que el subconjunto de llaves es usado en cada iteración de modo inverso.



Dependiendo de la naturaleza de la aplicación DES tiene 4 modos de operación para poder implementarse: ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, CBC (Cipher Block Chaining Mode) para mensajes largos, CFB (Cipher Block Feedback) para cifrar bit por bit ó byte por byte y el OFB (Output Feedback Mode) el mismo uso pero evitando propagación de error.

Seguridad del DES:

En la actualidad no se ha podido romper el sistema DES desde la perspectiva de poder deducir la llave simétnca a partir de la información interceptada, sin embargo con un método a fuerza bruta, es decir probando alrededor de 2^{56} posibles llaves, se pudo romper DES en Enero de 1999. Lo anterior quiere decir que, es posible obtener la llave del sistema DES en un tiempo relativamente corto, por lo que lo hace inseguro para propósitos de alta seguridad. La opción que se ha tomado para poder suplantar a DES ha sido usar lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la llave, esto a tomado la forma de un nuevo sistema de cifrado que se conoce actualmente como 3-DES o TDES

Si se toma un tiempo límite de dos horas para romper un archivo encriptado con DES, entonces se tiene que verificar todas las posibles llaves (2^{56}) en dos horas, lo cuál es aproximadamente de 5 trillones de llaves por segundo. Mientras éste quizá parezca un gran número, considerando que un chip de Circuitos Integrados Específicos de Aplicación (ASICs) puede probar 200 millones de llaves por segundo, y quizá muchos de esos puedan ser ejecutados al mismo tiempo

Otro método más reciente es el criptoanálisis diferencial. Este método reduce el número de llaves que deben ser probadas, pero requiere que tengas 2^{47} de texto plano escogido encriptado con la llave que quieres recuperar

Esto es altamente improbable que alguien esté de acuerto en encriptar 2^{47} de texto plano escogido con su llave secreta DES, este ataque es infactible en la práctica.

2.2.2 Triple DES

Sucesor del DES que muestra 3 llaves DES de 56 bits usadas como entrada para un arreglo de tres chips DES (o bloques de sw). El modelo a seguir en la encripción es encripta-decripta-encripta (EDE) con el modelo DED usado en el proceso contrario. En una variación del Triple DES, K_1 es igual a K_3 dando una llave de longitud de 112 bits. A este modo se le denomina como "Triple DES de 2 llaves", oponiendose al "Triple DES de 3 llaves" en el que K_1, K_2 y K_3 son distintas.

3-DES usa una llave de 168 bits, aunque se ha podido mostrar que los ataques actualmente pueden romper a 3-DES con una complejidad de 2^{112}, es decir efectuar al menos 2^{112} operaciones para obtener la llave a fuerza bruta, además de la memoria requerida.

Se optó por 3-DES ya que es muy fácil Interoperar con DES y proporciona segundad a mediano plazo

2.2.3 IDEA

IDEA (International Data Encryption Algorithm) fue creado en 1990 por Xuejia Lai y James Massey, fue llamado el Estándar de Encripción Propuesta (PES/ Proposed Encryption Standard). En 1991, Lai y Massey fortalecieron el algoritmo contra el análisis diferencial y llamaron al resultado Improvisando PES (IPES/Improved PES). Este último nombre fue cambiado por el de IDEA. Es un algoritmo de cifrado de bloque, que usa una llave secreta simétrica. Y fue reforzado para el ataque del criptoanálisis diferencial de Biham y Shamir para ser IDEA en 1992.

Usa una llave de 128 bits para operar en bloques de texto plano de 64 bits. El mismo algoritmo es usado para encriptar y decriptar, consiste en 8 iteraciones, usando 52 subllaves. Cada iteración usa seis subllaves, las cuatro restantes se usan en la transformación de la sálida. Esta basado en el concepto de "mezclar operaciones de diferentes grupos algebraicos". Los tres grupos algebraicos de los cuales son mezcladas las operaciones son:

- XOR
- Suma, ignorando algún desbordamiento (suma modulo 2^{16})
- Multiplicación, ignorando algún desbordamiento (multiplicación modulo $2^{16}+1$)

Esas operaciones operan en sub-bloques de 16 bits, haciendo eficiente el algoritmo hasta en procesadores de 16 bits

Las subllaves se crean primeramente, la llave de 128 bits es dividida en ocho llaves de 16 bits para proveer las primeras ocho subllaves. Los bits de la llave original son cambiados 25 bits a la izquierda, y son nuevamente divididos en ocho subllaves. Esta permutación y la división es repetida hasta que las 52 subllaves (K1-K52) han sido creadas. Los bloques de texto plano (P1-P4) son divididos en cuatro, una iteración consiste en los siguientes pasos

(OP = Bloque de salida)

```
OP1   P1 * K1  multiplica el 1er subbloque con la 1era subllave
OP2   P2 + K2  suma el 2  sub-bloque con la 2  subclave
OP3   P3 + K3
OP4   P4 * K4  multiplica el 4er subbloque con la 4era subllave
OP5   OP1 XOR OP3 (se aplica el XOR al resultado de los pasos 1 y 3)
```

```
OP6    OP2 XOR OP5
OP7    OP5 * K5 (multiplica el resultado del paso 5 con la 5ª subllave)
OP8    OP6 + OP7  (suma el resultado de los pasos 6 y 7)
OP9    OP8 * K6 (multiplica el resultado de los pasos 8 con la 6ª subllave)
OP10   OP8 + OP9
OP11 = OP1 XOR OP9 (se aplica el XOR al resultado de los pasos 1 y 9)
OP12 = OP3 XOR OP9
OP13 = OP2 XOR OP10
OP14 = OP4 XOR OP10
```

La entrada a la siguiente iteración, son los cuatro subbloques OP11, OP13, OP12, OP14 en ese orden.

Después de la octava iteración, los cuatro bloques finales de salida (F1-F4) son usados en la transformación final para producir cuatro subbloques de texto cifrado (C1-C4), que son unidos para formar el bloque final de 64 bits de texto cifrado.

```
C1   F1 * K49
C2 = F2 + K50
C3 = F3 + K51
C4   F4 * K52
TextoCifrado  C1 & C2 & C3 & C4.
```

Rompiendo el IDEA (Cracking)

Su llave es de 128 bits, dos veces más grande que la del DES, lo cual significa que sometiendose a prueba la mitad de llaves tomaría 2^{17} encripciones; el ataque por fuerza bruta queda obviamente fuera de la posibilidad de ser el que rompa el algoritmo. Usando un ataque de fuerza bruta, hay 2^{128} posibles llaves. Si un billón de chips pudieran probar un billón de llaves por segundo, para tratar de romper un mensaje encriptado con IDEA, tomaría 10^{13} años. Biham y Shamir han examinado los cifrados IDEA para debilitarlo sin tener éxito. Es más seguro que el DES.

2.2.4 RC2, RC4 y RC5

RC en honor del Código Ron, pero realmente es una abreviatura de "Rivest Cipher". El RC1 nunca fue más allá del estado de diseño, y el RC3 fue roto antes de que fuera liberado. Sin embargo RC2 fue liberado y usado en varios productos comerciales. Es un cifrado de bloque de 64 bits con una llave de longitud variable. RC4 usa también una llave de longitud variable, pero opera como un cifrado de flujo. En septiembre de 1994, el código para implementar el RC4 fue puesto en una red de un grupo de noticias e implementaciones que ahora fácilmente puede ser obtenido. Este conocimiento fue usado en 1995 para realizar un exitoso ataque de fuerza bruta con un solo mensaje de texto cifrado encriptado con el RC4 de 40 bits.

RC5 es un sistema parametrizado. Se puede cambiar el tamaño del bloque, la longitud de la llave, y el número de vueltas. El algoritmo básico es un bloque cifrado, pero las versiones de flujo también pueden ser definidas. Usado en los protocolos de los sistemas de pago.

2.2.5 KERBEROS

Es un sistema distribuido de autenticación usado por muchas organizaciones para manejar la seguridad de las contraseñas. Permite probar la identidad de los participantes que se comunican sobre la red.

El nombre de Kerberos proviene del perro de las tres cabezas que en la mitología griega cuidaba las puertas del Hades. Fue diseñado por Steve Miller y Clifford Neuman con sugerencias de Jeff Schiller y Jerry Saltzer. Fue originalmente diseñado en el Instituto Tecnológico de Massachussets MIT (Massachussets Institute of

Technology), y esta basado en el trabajo de Needham y Schroeder sobre autenticación mediada por un Centro de Distribución de llaves (KCD), el cual en una comunicación entre dos partes actúa como intermediario o arbitro y genera la llave de sesión enviandola a dos o más entidades participantes.

En la actualidad se tienen dos versiones de kerberos la versión 4 y la 5, las cuales se ven afectadas por el ataque directo a las contraseñas. Sin embargo esta vulnerabilidad es especialmente problemática en la versión 4, ya que dicho ataque afecta el acceso a Internet y a los ciclos de reserva del CPU

Los participantes en Kerberos son:

- Usuario (user) : Persona que empieza a usar un programa o servicio.
- Cliente (client) : Un cliente también usa algo, pero éste no necesariamente es una persona, éste puede ser un programa. También un cliente requiere y obtiene un servicio.
- Servidor (server) : Es el que proporciona servicios a los clientes.
- Servicio (service) : Especificación abstracta de algunas acciones a ser ejecutadas.
- Maestro y esclavo : Es posible correr el software de autenticación de kerberos en más de una máquina. Sin embargo, siempre hay solamente una copia definitiva de la base de datos de kerberos. La máquina en la cual se aloja esta base de datos es llamada la máquina maestro, o solamente el maestro. Otras máquinas pueden poseer copias de solamente lectura de la base de datos de kerberos, y estas son llamadas esclavos.
- Estaciones de Trabajo (workstation) : Están representadas por cada una de las computadoras conectadas en red.
- Intruso o atacante (hacker) : Cualquier ente que tenga como objetivo suplantar a una de las partes para obtener algún beneficio en su favor.

Kerberos usa cifrado simétrico (también llamado cifrado convencional), en particular DES, método en el cual el cifrado y descifrado se realiza usando una única llave. Asume una arquitectura distribuida cliente/servidor y emplea uno o más servidores Kerberos para proporcionar un servicio de autenticación

El problema que intenta resolver kerberos es el siguiente: restringir los accesos sólo a usuarios autorizados y poder autenticar los requerimientos a servicios, asumiendo un entorno distribuido abierto, en el cual los usuarios en estaciones de trabajo acceden a servicios de servidores distribuidos a través de una red. En el entorno de trabajo que considera Kerberos, una estación de trabajo no puede ser confiable para identificar a los usuarios correctamente para servicios de red. En particular existen las tres amenazas siguientes.

- Un usuario puede ganar accesos a una estación de trabajo en particular y simular ser otro usuario operando desde otra estación de trabajo.
- Un usuario puede alterar direcciones de red de una estación de trabajo, para que las solicitudes enviadas de la estación de trabajo alterada parezcan venir de una estación de trabajo impersonalizada.
- Un usuario puede observar disimuladamente los intercambios y usar un ataque de repetición para ganar la entrada al servidor o para interrumpir operaciones.

En muchos de estos casos, un usuario podría ganar accesos a servicios y datos que no está autorizado a acceder. Kerberos proporciona un servidor de autenticación centralizado cuya función es autenticar usuarios frente a servidores y autenticar servidores frente a usuarios.

Debe cumplir con requerimientos siguientes:

- **Seguro:** En una red el intruso no debe ser capaz de obtener la información necesaria para hacerse pasar por un usuario. Debe ser suficientemente fuerte como un intruso potencial
- **Confiable:** Para todos los servicios que confían en Kerberos para el control de acceso, falta disponibilidad del servicio de Kerberos, significa falta de disponibilidad de los servicios soportados.
- **Transparente:** Idealmente, el usuario no debe darse cuenta que la autenticación se está llevando a cabo, más allá del requerimiento para introducir una contraseña.
- **Escalable:** El sistema debe ser capaz de soportar números largos de clientes y servidores. Además, esto requiere una arquitectura modular distribuida

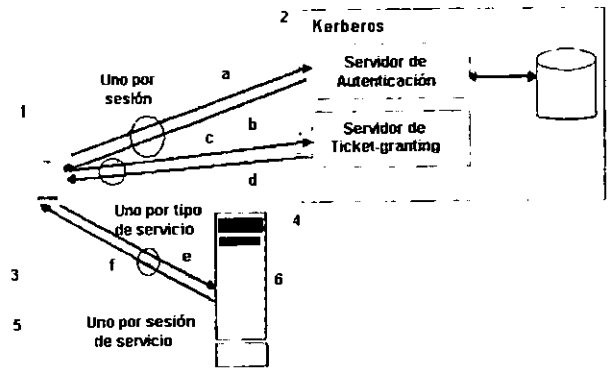
El funcionamiento de kerberos puede ser divido en cuatro etapas:

1. **Conexión al sistema:** un cliente se autentica frente a kerberos recibiendo un boleto y una llave de sesión correspondiente al intercambio entre el cliente y kerberos, cifrados con una llave secreta derivada de la contraseña del usuario.

2. **Solicitud de acceso al servidor:** para cada nuevo servicio a ser utilizado por el cliente, debe ser solicitado un boleto y una llave de sesión para ese nuevo intercambio entre el cliente y el servidor Esa información es enviada al cliente, cifrada con una llave de sesión entre el cliente y Kerberos.

3. **Acceso al servidor :** el cliente inicialmente envía el boleto recibido para el intercambio con el servidor deseado. Debido a que ese boleto está cifrado con una llave secreta del servidor, el mismo deberá descifrarla y así tendrá acceso a la llave de sesión entre el cliente y el servidor, que será válida por un período limitado (un tiempo de vida), que generalmente es de 8 horas. Después de este procedimiento, la comunicación entre ellos podrá ser llevada a cabo de una manera confidencial.

4. **Mantenimiento de la Base de Datos de kerberos :** comprende el almacenamiento de las llaves secretas del cliente y del servidor.



a Solicitud de un boleto de acceso
b Boleto y llave de sesión
c Solicitud de un boleto de acceso al servicio
d Boleto y llave de sesión para servicio
e Solicitud del servicio
f Autenticador del servidor

Protocolo(versión 4)

A) Intercambio de Servicio de autenticación para obtener un boleto de sesión

B) Intercambio de Servicio concediendo un boleto : para obtener un boleto_de_servicio.

(3) C → TGS : $ID_v \| boleto_{tgs} \| Autenticador$
*[*Opciones* || ID_v || *Tiempo* || *Noce*$_c$ || $boleto_{tgs}$ || $Autenticador_c$]
$boleto_{tgs} = E_{K_{tgs}}[K_{c,tgs} \| ID_c \| AD_c \| ID_{tgs} \| TS_2 \| Tiempo\_de\_Vida_2]$
*[$E_{K_{tgs}}$ [*banderas* || $K_{c,tgs}$ || *Reino*$_c$ || ID_c || *AD* || *Tiempo*]]
$Autenticador_c = E_{K_{c,tgs}}[ID \| AD_c \| TS_3]$
*[$E_{K_{c,tgs}}$ [*ID* || *Reino* || *TS*$_3$]]

(4) TGS → C : $E_{K_{c,tgs}}[K_{c,v} \| ID_v \| TS_4 \| boleto_v]$
*[*Reino*$_c$ || ID_c || $boleto_v$ || $E_{K_{c,tgs}}$ [$K_{c,v}$ || *Noce*$_c$ || *Reino* || *ID*]]
$boleto_v = E_{K_v}[K_{c,v} \| ID_c \| AD \| ID_v \| TS_4 \| Tiempo\ de\ Vida_4]$
*[E_{K_v} [*banderas* || $K_{c,v}$ || *Reino*$_c$ || ID_c || AD_c || *Tiempo*]]

C) Intercambio de autenticación Cliente/Servidor para obtener un servicio.

(5) C → V : $boleto_v \| Autenticador_c$
*[*Opciones* || $boleto_v$ || $Autenticador_c$]
$boleto_v = E_{K_v}[K_{c,v} \| ID_c \| AD \| ID_v \| TS_4 \| Tiempo\_de\_Vida_4]$
* [E_{K_v} [*banderas* || $K_{c,v}$ || *Reino* || ID_c || AD_c || *Tiempo*]]
$Autenticador_c = E_{K_{c,v}}[ID \| AD_c \| TS_5]$
* [$E_{K_{c,v}}$ [ID_c || *Reino* || TS_5 || *Sublave* || *#Secuencia*]]

(6 V → C : $E_{K_{c,v}}[TS_5 + 1]$
*[$E_{K_{c,v}}$ [TS_5 || *Sublave* || *#Secuencia*]]

Nota: Lo que se encuentra entre *[] e itálicas, son los cambios de la versión 5 de Kerberos.

En el mensaje (1):

C	Cliente
AS	Servidor de autenticación
ID_c	Identificador del usuario (en o sobre C)
ID_{tgs}	El AS determina que usuario solicita acceso al TGS
TS_1	El AS permite verificar que el reloj del cliente se sincronice con el del AS

En el mensaje (2):

E_{Kc}	El cifrado es basado en la contraseña del usuario, siendo capaces el AS y el cliente verificar la contraseña y de esta forma se protege el contenido del mensaje (2).
$K_{c,tgs}$	Copia de la llave de sesión accesible al cliente; creada por el AS Para permitir el intercambio seguro entre el cliente y el TGS, sin requerir estos compartir una llave permanente.
ID_{tgs}	Confirma que este boleto es para el TGS
TS_2	Se informa al cliente que el tiempo del boleto fue emitido
Tiempo_de_Vida$_2$	Informa al cliente del tiempo de vida de ese boleto.
$boleto_{tgs}$	Boleto para ser usado por el cliente para accesar al TGS.
AD_c	Dirección de red del cliente

En el mensaje (3)

V	Servidor
ID_v	Identificador del servidor (V)
$boleto_{tgs}$	El TGS asegura que el usuario ha sido autorizado por el AS
$Autenticador_c$	Generado por el cliente para validar el boleto

En el mensaje (4)

$E_{Kc,tgs}$	La llave compartida solamente por C y TGS, protege el contenido del mensaje (2)
ID_v	Se confirma que el boleto es para el servidor V
TS_4	Informa al cliente que el tiempo del boleto fue emitido
$boleto_v$	Boleto para ser usado por el cliente para accesar al servidor V
$boleto_{tgs}$	Boleto reusable para que el usuario no tenga que volver a teclear su contraseña.
E_{Ktgs}	El boleto es cifrado con la llave conocida solamente por el AS y el TGS.
$K_{c,tgs}$	Copia de la llave de sesión accesible a TGS; usada para descifrar el autenticador, y por consiguiente el boleto es autenticado
ID_c	Indica el dueño del boleto
AD_c	Previene el uso de un boleto de otra estación de trabajo.
ID_{tgs}	El servidor se asegura que ha descifrado el boleto adecuado
TS_2	El TGS informa que el tiempo del boleto fue emitido.
Tiempo_de_ Vida$_2$	Previene de una repetición después de que el boleto ha expirado.
$Autenticador_c$	El TGS asegura que el boleto presentado sea igual al del cliente para quien fue emitido el boleto; tiene un tiempo de vida muy corto para prevenir una repetición.
$E_{Kc,tgs}$	El autenticador es cifrado con la llave conocida solamente por el cliente y el TGS
ID_c	Debe ser igual el ID en el boleto para autenticar éste.
AD_c	Debe ser igual la dirección de red en el boleto para autenticar éste.
TS_2	El TGS informa que el tiempo de este autenticador fue generado

En el mensaje (5)

$boleto_v$	El servidor se asegura que el usuario ha sido autenticado por el AS.
$Autenticador_c$	Generado por el cliente para validar el boleto

En el mensaje (6):

$E_{Kc,v}$	C se asegura que el mensaje es de V
$TS_5 + 1$	C se asegura que no sea una repetición de una contestación anterior.
$boleto_v$	Reusable para que el cliente no necesite pedir uno nuevo al TGS para cada acceso al mismo servidor
E_{Kv}	El boleto es cifrado con la llave conocida solamente por el TGS y el servidor
$K_{c,v}$	Copia de la llave de sesión accesible al cliente, usada para descifrar el autenticador y por consiguiente autenticar el boleto.
ID_c	Indica quien es el dueño correcto del boleto.
AD_c	Previene el uso de un boleto de otra estación de trabajo que el boleto que inicialmente fue solicitado.
ID_v	El servidor se asegura que ha descifrado el boleto adecuado
TS_4	El servidor informa que el tiempo del boleto fue emitido
Tiempo_de_ Vida$_2$	Previene de una repetición después de que el boleto ha expirado.
$Autenticador_c$	El servidor se asegura que el boleto presentado sea el mismo que el del cliente para quien el boleto fue emitido; tiene un tiempo de vida muy corto para prevenir un ataque por repetición
$E_{Kc,v}$	El autenticador es cifrado con la llave conocida solamente por el cliente y el servidor
ID_c	Debe ser igual el ID en el boleto para autenticar éste
AD_c	Debe ser igual la dirección de red en el boleto para autenticar éste.
TS_5	El servidor informa que el tiempo de este autenticador fue generado

Funcionamiento Versión 4

(1) y (2) El cliente envía un mensaje a el AS solicitando accesos a el TGS. El AS responde con un mensaje, cifrado con una llave derivada de la contraseña del usuario (K_c), que contiene el boleto El mensaje cifrado también contiene una copia de la llave de sesión, $K_{c,tgs}$, donde los subíndices indican que ésta es una llave de

sesión para C y TGS. Porque esta llave de sesión esta dentro del mensaje cifrado con K_c, solamente el cliente del usuario puede leer ésta. La misma llave de sesión es incluida en el boleto, el cuál sólo puede ser leído por el TGS. Así, la llave se sesión ha sido firmemente entregada tanto a C como a TGS.

El mensaje (1) incluye la fecha y hora TS_1 ("timestamp"), para que el AS conozca que el mensaje es oportuno (a tiempo). El mensaje (2) incluye varios elementos del boleto en una forma accesible a C. Esto permite a C confirmar que este boleto es para el TGS y saber el tiempo de expiración del boleto.

(3) Ahora, teniendo el boleto y la llave de sesión, C está preparado para dirigirse al TGS. C envía a TGS un mensaje que incluye el boleto más el ID del servicio solicitado (ID_v). Además, C transmite un autenticador, el cual incluye el ID, la dirección del usuario de C, la fecha y hora. A diferencia del boleto, el cuál es reusable, el autenticador es proyectado para usarse solamente una vez y tiene un muy corto tiempo de vida. Ahora, el TGS puede descifrar el boleto con la llave que éste comparte con el AS. Este boleto indica que el usuario C ha sido suministrado con la llave de sesión $K_{c,tgs}$. En efecto, el boleto dice, "cualquiera que usa $K_{c,tgs}$ debe ser C". El TGS usa la llave de sesión para descifrar el autenticador. El TGS puede entonces verificar el nombre y la dirección del autenticador con el boleto y con la dirección de red del mensaje entrante. Si todo hace juego, entonces el TGS está seguro de que el emisor de el boleto es en verdad el dueño real del boleto. En efecto, el autenticador dice "A veces TS_3, Yo uso $K_{c,tgs}$ por este medio". Nota que el boleto no demuestra la identidad de cualquiera pero es una manera de distribuir llaves de forma segura. Este es el autenticador que proporciona la identidad del cliente. Porque el autenticador puede ser usado solamente una vez y tiene un corto tiempo de vida, la amenaza de un intruso de robar tanto el boleto como el autenticador para una presentación posterior no es valida.

(4) La contestación del TGS, sigue la forma del mensaje (2). El mensaje es cifrado con la llave del mensaje compartida por TGS y C e incluye una llave de sesión para ser compartida entre C y el servidor V, el ID de V, y la fecha y hora del boleto. El boleto en sí mismo incluye la misma llave de sesión.

(5) C ahora tiene un boleto otorgado para servicio reusable para acceder al servidor V. Cuando C presenta este boleto, éste también envía un autenticador. El servidor V puede descifrar el boleto, recuperando la llave de sesión, y descifrando el autenticador si estos coinciden permite el acceso.

(6) Si se requiere autenticación mutua, el servidor V regresa el valor de la fecha y hora ("timestamp") de el autenticador (TS_5), incrementado por 1, y cifrado con la llave de sesión. C puede descifrar este mensaje para recuperar la fecha y hora incrementada. Porque el mensaje fue cifrado por la llave de sesión, C está seguro de que esto puedo haber sido creado solamente por V. Los contenidos del mensaje aseguran a C que esto no es una repetición de una contestación anterior.

Finalmente, en la conclusión de este proceso, el cliente y el servidor comparten una llave secreta. Esta llave puede ser usada para cifrar mensajes futuros entre dos partes o para intercambiar una nueva llave de sesión aleatoria para tal propósito.

Funcionamiento Versión 5

En el mensaje (1) el cliente solicita un boleto de sesión. Este incluye el ID del usuario y del TGS. Los siguientes elementos son adicionados:

- Reino: indica el reino del usuario.
- Opciones : usadas para solicitar que ciertas banderas se pongan en el boleto de regreso
- Tiempo: usado por el cliente para solicitar las escenas de tiempo siguientes en el boleto.
  - de ("from") : la forma de tiempo de salida deseado por el boleto pedido
  - hasta ("till") : el tiempo de expiración solicitado para el boleto pedido
  - rtime : renovado-hasta el tiempo solicitado.
- Noce un valor aleatorio para ser repetido en el mensaje (2) para asegurar que la contestación está reciente y no ha sufrido ninguna repetición por un intruso

El mensaje (2) regresa un boleto de sesión, identificando información del cliente, y un bloque cifrado usando la llave cifrada basada en la contraseña del usuario. Este bloque incluye la llave de sesión para ser usada entre el cliente y el TGS, el tiempo especificado en el mensaje 1, el valor aleatorio del mensaje 1, y la información que identifica al TGS. El boleto por sí mismo incluye la llave de sesión, información que identifica cliente, los valores de tiempo solicitado, y banderas (ó marcas) que reflejan el estatus de este boleto y las opciones solicitadas. Estas banderas introducen nueva funcionalidad significativa a la versión 5

El mensaje (3) para ambas versiones incluye un authenticador, un boleto, y el nombre del servicio solicitado. Además de esto la versión 5 incluye el tiempo solicitado, opciones para el boleto y un valor aleatorio, todos con funciones similares a las del mensaje (1). El autenticador es esencialmente el mismo que el usado en la versión

El mensaje (4) tiene la misma estructura que el mensaje (2), regresando un boleto, más información necesitada por el cliente, el cual es el mensaje más reciente cifrado con la llave de sesión ahora compartida por el cliente y el TGS.

Finalmente para el intercambio de autenticación cliente/servidor, nuevas características aparecen en versión 5. En el mensaje (5), el cliente puede solicitar como una opción que la autenticación mutua se requiera. El autenticador incluye nuevos cambios y son los que se mencionan a continuación :

- Subllave : la elección del cliente de cifrar una llave a ser usada para proteger esta sesión de la aplicación específica. Si este campo es omitido, la llave de sesión de un boleto ($K_{c,v}$) es usada.

- Número de secuencia . Un campo opcional que especifica el número de secuencia de arranque, a ser usado por el servidor durante los mensajes enviados a el cliente durante esta sesión. Los mensajes pueden ser secuencias numeradas para detectar repeticiones.

Si la autenticación mutua es requerida, el servidor responde con el mensaje (6). Este mensaje incluye la fecha y hora ("timestamp") del autenticador. En versión 4, la fecha y la hora fue incrementada por uno. Esto no es necesario en versión 5, porque la naturaleza del formato de los mensajes es tal que no le es posible a un adversario crear el mensaje (6), sin el conocimiento de las llaves de cifrado apropiadas. Si el campo subllave, esta presente en el $Autenticador_c$, sustituye el campo subllave, en el mensaje (5). El campo de número de secuencia optativo especifica el número de sucesión de arranque a ser usado por el cliente.

Análisis Comparativo Entre La Versión 4 Y 5 De Kerberos

La versión 5 intenta solucionar las limitaciones de la versión 4 en dos áreas : fallas del entorno y deficiencias técnicas. La versión 4 de kerberos fue desarrollada para usarse con el ambiente del proyecto Atenea y, por consiguiente, no se cubrieron completamente las necesidades de propósito general. Así se produjeron las siguientes fallas del entorno:

1 - Dependencia del sistema de cifrado: La versión 4 requiere del uso de DES. En versión 5, el texto es cifrado con un identificador del tipo de cifrado, así que cualquier técnica de cifrado puede ser usada. Las llaves cifradas son etiquetadas con un tipo y una longitud, permitiendo que la misma llave sea usada en algoritmos diferentes y permitiendo la especificación de diferentes variaciones en un algoritmo dado

2 - Dependencia del protocolo de Internet . La versión 4 requiere el uso direcciones IP (de direcciones del protocolo de Internet (IP)).Otro tipo de direcciones, tal como la dirección de red ISO, no son soportadas. Las direcciones de red (o direccionamientos de red) de la versión 5 son identificados con tipo y longitud, permitiendo el uso de cualquier tipo de direccionamiento (o dirección de red).

3 - Ordenamiento del mensaje en bytes . En versión 4, el emisor de un mensaje emplea un ordenamiento de bytes propio del mensaje eligiendo y etiquetando el mensaje para indicar el byte menos significativo en una dirección más baja o el byte más significativo en una dirección más baja. Esta técnica se lleva a cabo pero no sigue convenciones establecidas. En versión 5, todas las estructuras del mensaje se definen usando una Anotación de Sintaxis Abstracta y las reglas de Codificación Básicas (BER), lo cual proporciona un ordenamiento o clasificación del mensaje en bytes sin ambigüedad.

4.- Tiempo de vida del boleto : Los valores del tiempo de vida en versión 4 son codificados en cantidades de 8-bits en unidades de 5 minutos. Así, el tiempo de vida máximo que puede ser expresado es 2^8 x 5 = 1280 minutos. Esto puede ser inadecuado en algunas aplicaciones (por ejemplo en simulaciones de larga duración que requieren credenciales validas de kerberos durante la ejecución). En la versión 5, los boletos incluyen explícitamente el tiempo de inicio y de fin, permitiendo boletos con tiempo de vida arbitrarios.

5 - Reenviar autenticación : La versión 4 no permite publicar credenciales a algún cliente para ser reenviadas a algún otro host y usadas por algún otro cliente. Esta capacidad habilitaría a un cliente acceder a un servidor y que éste tenga acceso a otro servidor en beneficio del cliente. Por ejemplo, un cliente emite una solicitud a un servidor de impresión y entonces accesa al archivo del cliente de un servidor de archivos, usando las credenciales del cliente para accesar. La versión 5 provee esta capacidad.

6.- Autenticación mutua del reino: En versión 4, la interoperabilidad entre N reinos requiere del orden de N^2 relaciones Kerberos a Kerberos. La versión 5 soporta un método que requiere menos relaciones.

Además de las limitaciones de entorno, existen deficiencias técnicas en la versión 4 del protocolo. Estas deficiencias son las siguientes

1. Doble cifrado : Los boletos proporcionados a los clientes son cifrados dos veces, una vez con la llave secreta del servidor destino y luego por una llave secreta conocida por el cliente. El segundo cifrado no es necesario y computacionalmente no es económico.

2. Cifrado PCBC : En la versión 4 el cifrado hace uso del modo no estándar de DES, conocido como encadenando bloques planos y cifrados PCBC (plain-and-cipher block Chaining). Se ha demostrado que este método es vulnerable a un ataque que involucre el intercambio de bloques de texto cifrado. PCBC fue propuesto para proveer un chequeo de integridad como parte de la operación de cifrado. La versión 5 proporciona mecanismos de integridad explícitos.

3. Llaves de sesión : Cada boleto incluye una llave de sesión que es usada por el cliente para cifrar el autenticador enviado al servicio asociado con el boleto. Además la llave de sesión puede subsecuentemente ser usada por el cliente y el servidor para proteger mensajes transmitidos durante esta sesión. De esta manera, como el mismo boleto debe ser usado repetidas veces para obtener el servicio desde un servidor particular, existe el riesgo que un adversario repita el mensaje desde una sesión anterior al cliente o al servidor. En la versión 5, es posible que el cliente y el servidor negocien una llave de subsesión, la cual es usada solamente para una conexión.

4. Ataques a las contraseñas. Una vulnerabilidad compartida por ambas versiones es el ataque a las contraseñas. El mensaje desde el AS al cliente incluye material cifrado con una llave basada en la contraseña del cliente. Un adversario puede atrapar ese mensaje e intentar descifrarlo intentando con varias contraseñas posibles. Si se descubre la contraseña del cliente, el adversario podrá usarlo posteriormente para obtener credenciales de autenticación de kerberos. La versión 5 proporciona un mecanismo conocido como preautenticación, el cual dificultaría el ataque a las contraseñas, pero no lo prevendría.

Seguridad de Kerberos

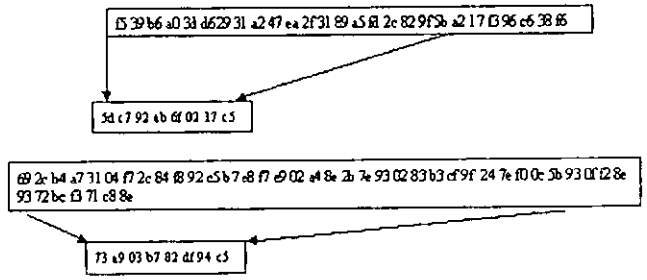
Aunque kerberos 5 introduce preautenticación, esto es se requiere que el usuario de alguna evidencia para saber que la llave compartida K es verídica, antes de que el servidor de autenticación emita un boleto de sesión (TGT). Esta evidencia se da en la forma de una etiqueta de tiempo T cifrada. El servidor de autenticación envía su respuesta a C sólo si T descifrada esta en el tiempo correcto dentro de cierta tolerancia. Aunque esto evita que un atacante solicite un boleto de sesión (TGT), no protege contra algún espía que capture $E_k(T)$ ó $E_k(TGT)$. Ambas cantidades constituyen texto plano verificable que puede ser usado para montar un ataque a diccionario. Aunque esto es una mejora relativa, un atacante con un rastreador de red puede llevar a cabo un ataque por diccionario, fuera del control de una máquina central, contra cualquier solicitud de autenticación capturado en la red

Entre los ataques más potentes a la criptografía simétrica están el criptoanálisis diferencial y lineal, sin embargo no han podido ser muy eficientes en la práctica por lo tanto, por el momento después de que un sistema criptográfico es publicado y se muestra inmune a estos dos tipos de ataques (y algunos otros más), la mayor preocupación es la longitud de las llaves.

2.3 Funciones Hash

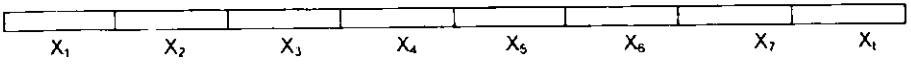
Algoritmos simétricos, que proveen dos servicios principales. El primero es que el contenido del mensaje sea guardado confidencialmente de los intrusos, quienes no pueden descifrar el mensaje encriptado, y segundo, la integridad del mensaje es asegurada. Esta puede ser garantizada desde que el mensaje no puede ser alterado sino se tiene la llave. Son usadas también para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función hash les asocia una cadena de longitud 160 bits que los hace más manejables para el propósito de firma digital.

De forma gráfica la función hash efectúa lo siguiente



Su funcionamiento consiste en tomar como entrada una cadena de longitud arbitraria, digamos 5259 bits, luego divide este mensaje en pedazos iguales, digamos de 160 bits, como en este caso y en general el mensaje original no será un múltiplo de 160, entonces para completar un número entero de pedazos de 160 bits al último se le agrega un relleno, digamos de puros ceros En nuestro caso en 5259 caben 32 pedazos de 160 bits y sobran 139, entonces se agregaran 21 ceros más.

Entonces el mensaje toma la forma $X = X_1, X_2, X_3, \ldots, X_t$ donde cada X_i tiene igual longitud (160 bits por ejemplo)



Posteriormente se asocia un valor constante a un vector inicial IV y

$H_0 = IV$

Ahora se obtiene H_1, que es el resultado de combinar H_0 con X_1 usando una función de compresión f

$H_1 = f(H_0, X_1)$

Posteriormente se obtiene H_2, combinando H_1 y X_2 con f

$$H_2 = f(H_1, X_2)$$

Se hace lo mismo para obtener H_3

$$H_3 = f(H_2, X_3)$$

Hasta llegar a H_t

$$H_t = f(H_{t-1}, X_t)$$

Entonces el valor hash será $h(M) = H_t$

De alguna forma lo que se hace es tomar el mensaje partirlo en pedazos de longitud constante y combinar de alguna forma pedazo por pedazo hasta obtener un solo mensaje de longitud fija.

Se provee la integridad sin confidencialidad, usando un dispositivo conocido como message digest (resumen del mensaje). Aplicando un algoritmo hash a lo largo del mensaje para producir un pequeño message digest. La llave secreta puede ser aplicada al hash y el resultado enviado con el mensaje a través de la red. El hash es encriptado para llegar a ser un Verificador de la Integridad del Mensaje (MIC/ Message Integrity Check), el cual es agregado al mensaje antes de la transmisión, desde que la encripción sólo está siendo aplicada a una pequeña cantidad, y el message digest es mucho más fácil que la encripción, este proceso puede ser considerablemente más rápido que encriptar el mensaje entero.

También podemos aplicar integridad en este caso, cuando llega el mensaje, el receptor computa un hash del mensaje usando el mismo algoritmo. Si éste marca el MIC decriptado que viene con el mensaje, entonces el mensaje no ha sido manipulado.

Las funciones hash (o primitivas hash) pueden operar como: MDC (Códigos de Detección de Modificaciones / Modification Detection Codes) ó MAC (Códigos de Autenticación de Mensajes / Message Authentication Codes).

Los MDC sirven para resolver el problema de la integridad de la información, al mensaje se le aplica un MDC (una función hash) y se manda junto con el propio mensaje, al recibirlo el receptor aplica la función hash al mensaje y comprueba que sea igual al hash que se envió antes.

Es decir, se aplica un hash al mensaje M y se envía con el mensaje (M, h(M)), cuando se recibe se le aplica una vez más el hash (ya que M es público) obteniendo h'(M), si h(M)=h'(M), entonces se acepta que el mensaje se a transmitido sin alteración

Los MAC sirven para autenticar el origen de los mensajes (junto con la integridad), un MAC Es decir, se combina el mensaje M con una llave privada K y se les aplica un hash h(M,K), si al llegar a su destino h(M, K) se comprueba de integridad de la llave privada K, entonces se demuestra que el origen es sólo el que tiene la misma llave K, probando así la autenticidad del origen del mensaje.

Las propiedades que deben de tener las primitivas hash son:

1) **Resistencia a la preimagen**: significa que dada cualquier imagen, es computacionalmente imposible encontrar un mensaje x tal que h(x)=y. Otra forma como se conoce esta propiedad es que h sea de un solo sentido.
2) **Resistencia a una 2° preimagen**: significa que dado x, es computacionalmente imposible encontrar una x' tal que h(x)=h(x') Otra forma de conocer esta propiedad es que h sea resistente a una colisión suave.
3) **Resistencia a colisión** significa que es computacionalmente imposible encontrar dos diferentes mensajes x, x' tal que h(x)=h(x') Esta propiedad también se conoce como resistencia a colisión fuerte

Para ilustrar la necesidad de estas propiedades veamos los siguientes ejemplos:

Consideremos un esquema de firma digital con apéndice, entonces la firma se aplica a h(x), en este caso h debe ser un MDC con resistencia a una 2° preimagen, ya que de lo contrario un atacante C que conozca la firma sobre h(x), puede encontrar otro mensaje x' tal que h(x) = h(x') y reclamar que la firma es del documento x'.

Si el atacante C puede hacer que el usuario firme un mensaje, entonces el atacante puede encontrar una colisión (x, x') (en lugar de lo más difícil que es encontrar una segunda preimagen de x) y hacer firmar al usuario a x diciendo que firmo x'. En este caso es necesaria la propiedad de resistencia a colisión.

Por último si (e,n) es la llave pública RSA de A, C puede elegir aleatoriamente un y y calcular $z = y^e \bmod n$, y reclamar que y es la firma de z, si C puede encontrar una preimagen x tal que z = h(x), donde x es importante para A. Esto es evitable si h es resistente a preimagen.

Las funciones hash más conocidas son las siguientes: las que se crean a partir de un cifrado de bloque como DES, MD5, SHA-1, y RIPEMD 160

Actualmente se ha podido encontrar debilidades en las funciones hash que tienen como salida una cadena de 128 bits, por lo que se ha recomendado usar salidas de 160 bits. Así mismo se han encontrado ataques a MD5 y SHA-0 (antecesora de SHA-1), esto ha dado lugar que se dirija la atención sobre la función hash RIPEMD-160.

El ataque más conocido (a fuerza bruta) a una función hash es conocido como "birthday attack" y se basa en la siguiente paradoja, si hay 23 personas en un local existe una probabilidad de al menos 1/2, de que existan dos personas con el mismo cumpleaños. Aunque parezca muy difícil esa posibilidad se puede mostrar que en general al recorre la raíz cuadrada del número de un conjunto de datos, se tiene la probabilidad de al menos ½ de encontrar dos iguales.

Al aplicar esto a una función hash, es necesario recorrer entonces la raíz cuadrada de 2^{160} mensajes para poder encontrar dos con el mismo hash, o sea encontrar una colisión. Por lo tanto una función hash son salidas 2^{160} tiene una complejidad de 2^{80}, y una función de 128 bits de salida tiene una complejidad de 2^{64}, por lo que es recomendable usar actualmente salida de 160 bits. Las dos funciones hash más conocidas son el MD5 y SHA.

2.3.1 MD5

Este algoritmo es uno de las series (incluyendo MD2 y MD4) de los algoritmos de message digest desarrollados por Ron Rivest. Este agrega un campo de longitud a un mensaje, y lo rellena hasta formar múltiplos de bloques de 512 bits. Cada uno de esos bloques es alimentado a través de procesos de 4 iteraciones, envolviendo una rotación y un rango de operaciones Booleanas produciendo un valor encadenado que es la entrada dentro del procesamiento del siguiente bloque de 512 bits. La salida del hash es una cadena de valor de 512 bits producido en el procesamiento del último bloque del mensaje.

2.3.2 SHA (Secure Hash Algorithm)

El Instituto Nacional de Estándares y Tecnología de los E.U. (NIST), liberaron una serie de estándares criptográficos en 1993. El mensaje primeramente es aumentado o rellenado con el MD5, y entonces es alimentado en cuatro iteraciones, las cuales son más complejas que las usadas en el MD5. La cadena de valores es pasada de una iteración a la siguiente, es de longitud de 160 bits, lo cual significa que el resultado del message digest es también de 160 bits.

2.4 Criptografía Asimétrica o de Llave Pública

La criptografía de llave pública fue propuesta en 1976 por Whitfield Diffie y Martin Hellman para resolver los problemas de administración de llaves. En la criptografía de llave pública, cada persona obtiene un par de llaves, llamadas llave pública y privada. La llave pública es publicada y ampliamente distribuida mientras la llave privada nunca es revelada. La necesidad por el intercambio de la llave privada es eliminada, todas las comunicaciones sólo envuelven a la llave pública. La llave privada no es nunca compartida o transmitida.

Por lo tanto cuando el usuario A desea enviar un mensaje encriptado a B, A busca la llave pública de B (Kpu_B) en un directorio público u obtiene esto por algún otro medio, usa esto para encriptar el mensaje, y lo envía a B. B entonces usa su llave Privada(Kpr_B) para desencriptar el mensaje. Alguien que tenga acceso a la llave pública de B puede enviarle un mensaje encriptado, pero nadie aparte de B puede desencriptarlo.

Propiedades:

Se asume que Kpu es la llave de cifrado y que Kpr es la llave de descifrado.

1. Cifrado (aplicando el algoritmo con la llave de cifrado) seguida por el descifrado de un mensaje M resulta en M:

   Kpr(Kpu(M)) M

2. Ambos Kpu y Kpr son fáciles de computar.
3. Públicamente revela Kpu, el usuario no revela como se computa Kpr.

Actualmente la Criptografía asimétrica es muy usada, sus dos principales aplicaciones son el intercambio de llaves privadas y la firma digital. Los fundamentos de la criptografía asimétrica pertenecen a la teoría de números.

La criptografía asimétrica o de llave pública se divide en tres familias según el problema matemático del cual basan su seguridad. La primera familia basa su seguridad en el Problema de Factorización Entera PFE, los sistemas que pertenecen a esta familia son, el sistema RSA, y el de Rabin Williams RW. La segunda familia es la que basa su segundad en el Problema del Logaritmo Discreto PLD, a esta familia pertenece el sistema de Diffie Hellman DH de intercambio de llaves y el sistema DSA de firma digital. La tercera familia es la que basa su seguridad en el Problema del Logaritmo Discreto Elíptico PLDE, en este caso hay varios esquemas tanto de intercambio de llaves como de firma digital que existen como el DHE (Diffie Hellman Elíptico), DSAE, (Nyberg-Rueppel) NRE, (Menezes, Qu, Vanstone) MQV, etc Para efectos de esta investigación los únicos criptosistemas de llave pública que analizaremos serán RSA y Diffie Hellman, más adelante veremos lo que es un certificado y firma digital.

2.4.1 RSA

RSA es nombrado en honor a sus creadores Rivest, Shamir y Adleman, fue el primer algoritmo efectivo de llave pública, y por años ha resistido intensas pruebas de criptoanalistas en todo el mundo. Estos algoritmos confían en que sea computacionalmente infactible recuperar la llave privada a partir de la llave pública Confiando en el hecho de que es fácil factorizar dos grandes números primo, pero extremadamente difícil factorizarlas de regreso para obtener el resultado

Factorizar un número significa encontrar sus factores primos, los cuales son números primos que necesitan ser multiplicados para producir ese número Por ejemplo

```
10    2 * 5
60    2 * 2 * 3 * 5
7[illegible]    3391 * 23279 * [illegible] * 1[illegible]4569 * 10668181328684267
```

Se basa en la aritmética modular, en la posibilidad de calcular inversos multiplicativos. Es decir:

Dado un entero e en el rango [0, n-1], a veces es posible hallar un entero único d en el rango [0, n-1] tal que

$$e.d \bmod n = 1$$

Por ejemplo 3 y 7 son inversos multiplicativos módulo 20 porque:

$$3.7 \bmod 20 = 21 \bmod 20 = 1$$

Puede demostrarse que el entero *e* perteneciente a [0, n-1] tiene un inverso multiplicativo único mod n cuando e y n son primos relativos, es decir, cuando:

$$mcd(e,n) = 1$$

El número de enteros positivos que son primos relativos con n es una función denotada como $\varphi(n)$. Para n = pq y, p y q primos, se demuestra que:

$$\varphi(n) = (p-1)(q-1)$$

Para un número $P \in [0, n-1]$ la ecuación

$$[1]\quad C = P^e \bmod n$$

es inversa de

$$[2]\quad P = C^d \bmod n$$

si

$$ed \bmod \varphi(n) = 1 \text{ donde } \varphi(n) = (p-1)(q-1)$$

El cifrado se realiza con la ecuación [1] con e y n como llaves, y el descifrado se realiza con la ecuación [2] con d y n como llaves. Puesto que la llave (e,n) es pública, sólo el número d del par (d,n) es privado. Si d se elige como primo relativo en $\varphi(n)$, y e se elige como inverso multiplicativo de d, entonces el texto plano cifrado en [1] puede descifrarse usando d en [2]

Algoritmo

1 Elegir dos primos grandes p y q cada uno superior 10^{100}
2 Calcular n=pq y $\varphi(n) = (p-1)(q-1)$
3 Elegir un número d como un número aleatorito grande que sea primo relativo con $\varphi(n)$, es decir, tal que mcd(d, $\varphi(n)$)=1
4 Hallar e tal que ed mod $\varphi(n) = 1$

Si el texto plano P es más largo que n entonces hay que truncar el texto en cadenas de tamaño n

En términos muy generales es así como funciona el sistema RSA. Sin embargo en la realidad existen dos formas que son las más comunes, estas formas depende de la aplicación y se llaman el esquema de firma y el esquema de cifrado

Seguridad de RSA

Actualmente, no hay un método más eficiente para romper RSA que el conocido como factorización de grandes números n. Está probado que, actualmente no existe un algoritmo para factorizar un número de 200 dígitos en un tiempo razonable

Los posibles procedimientos criptoanalíticos que se pueden aplicar para vulnerar este algoritmo son

a) Factorización de n.

La factorización de n permite vulnerar el método ya que se puede obtener h(n) y fácilmente d. Por otra parte el algoritmo más rápido de factorización conocido debido a R. Schroeppel (no publicado), factoriza un número n en:

$$\exp(\sqrt{\ln(n)\ln(\ln(n))}) \text{ pasos}$$

Si suponemos que un paso de este algoritmo en una computadora llevará 1 microsegundo, el tiempo de factorización según Schroeppel sería el indicado en la siguiente tabla:

Dígitos	N° de Operaciones	Tiempo
50	1.4×10^{4}	3.9 horas
75	9.0×10^{6}	104 días
100	2.3×10^{8}	74 años
200	1.2×10^{13}	3.8×10^{5} años
300	1.5×10^{17}	4.9×10^{9} años
500	1.3×10^{19}	4.2×10^{11} años

Se recomienda utilizar n de longitud 200 dígitos, al objeto de proporcionar un alto grado de seguridad. El método, en función de la longitud de n, proporciona diferentes niveles de seguridad que pueden ser convenientes en función del grado de secreto que se dé a la información a cifrar

b) Cálculo h(n) sin Factorizar n

Si se obtiene h(n) se vulnera el sistema calculando d como número asociado de e (público) mod h(n) mediante el algoritmo de Euclides modificado. Este procedimiento es equivalente a factorizar n, pues si se conoce h(n) se puede elementalmente encontrar p y q.

Así,

$(p+q)$ se obtiene de n y $h(n) = n-(p+q)+1$ y

$(p-q)$ $\sqrt{(p+q)^2 - 4n}$,

por tanto:

$q = [(p+q) - (p-q)]/2$ y $p = n/q$

y por consiguiente se vulneraría el método.

c) Determinar d sin factorizar n o calcular h(n)

d debe elegirse entre un gran conjunto de números de forma que la búsqueda exhaustiva resulte no factible. Por otra parte, conocido d se puede factorizar n fácilmente, pues,

$$e.d = 1 \quad k.h.n.$$

y Miller ha demostrado como factorizar n conocido un múltiplo cualquiera de h(n) Con ello, se llega a la conclusión de que, si n es grande, no se puede determinar d de forma más fácil que factorizando n

d) Determinar la función D de alguna forma

Por último, se piensa que M se podría obtener calculando la raíz e-ésima de C, según

$$M = \sqrt[e]{C} \bmod n.$$

Pero se cree que este problema pertenece a la clase de problemas NP completos según los autores del algoritmo.

Ejemplo del Cifrado RSA

Supuesto que el usuario A quiere entrar en el sistema, entonces, elige los enteros primos p=5 y q=11 resultando n = p.q = 5.11 = 55.

Así, h(55) = 4.10 = 40. A continuación, se selecciona la clave privada d = 23. Como el m.c.d. (e,23) = 1; se cumple que e.23 = 1 mod 40, obteniéndose e = 7, siendo e el inverso multiplicativo de 23 módulo 40.

Sea el mensaje "STOP" que se codifica numéricamente, como 20 21 16 17 y se cifra por bloques de letras, en este caso se hace letra a letra. Así, para la "S"

$$C = M^e \bmod n = 20^7 \bmod 55 \quad (((1)^2.20)^2.20)^2.20 \bmod 55 = 15$$

Utilizando el algoritmo de la exponenciación rápida, que exprensando e en binario, en este caso, $e = 7 = 111_2$ permite la evaluación de la exponenciación de M.

Para el caso que se trata, al ser d = 23, en binario 10111, C se descifraría como

$$M = C^d \bmod n = 15^{23} \bmod 55 = (((1).15)^2.15)^2.15)^2.15 \bmod 55 \text{ dando } M = 20.$$

2.4.2 Diffie-Hellman

Es un algoritmo de llave pública comúnmente usado para el intercambio de llaves. Considerado seguro cuando la longitud de las llaves es grande y se usa un apropiado generador de números primos. Su seguridad se confía a la dificultad del problema del logaritmo discreto (que es equivalente computacionalmente a factorizar grandes enteros).

Su funcionamiento es el siguiente:

1) Se asume que A y B tienen conocimiento previo (público) de dos números p, primo grande (512 bits) y g > g > p.

2) A y B escogen un número aleatorio de 512 bits y lo guardan en secreto sean S_a y S_b.

3) A calcula $T_a = g^{Sa} \bmod p$ B calcula $T_b = g^{Sb} \bmod p$

4) A y B obtienen el mismo resultado

[illegible] $\bmod p$.

Problema del logaritmo discreto Deducir S de T

Su seguridad es sensitiva a la elección de un primo fuerte y su generador. El tamaño del exponente secreto es también crítico para la seguridad. Una recomendación es hacer el exponente aleatorio dos veces más grande que la llave de sesión a generar

2.5 Firmas Digitales

La confidencialidad de datos puede lograrse a través del cifrado del mensaje. La integridad de datos es importante para el e-commerce. Las firmas digitales, también conocidas como autenticación del remitente, pueden usarse para asegurar integridad de datos. Las firmas digitales requieren aplicar un método de firma y un método para verificar que la firma realmente se generó por el remitente. Suponga las necesidades de X para firmar un documento digitalmente antes de enviarlo. X reúne su llave privada y el documento en un programa hash genera un numero unico llamado firma digital o una huella digital. Esto se une al documento original y es encriptado con la llave privada Kpr_X y enviado a Y. Y primero decripta el documento que usa la llave pública Kpu_X. Entonces Y corre la misma función hash en el documento. Si el resultado es el mismo, entonces Y es cierto y dice que la firma digital es auténtica.

Una firma digital sólo puede ser generada por alguien sabiendo la llave privada Kpr. La comprobación requiere sólo el conocimiento de la llave pública Kpu. Para que, X pueda firmar un mensaje X debe generar la firma. Y simplemente puede verificar que es firma de X, pero no puede generarla. Esto es similar a las firmas escritas a mano, donde es posible reconocer una firma como auténtica sin poder generarla. Si el el documento se altera mientras se está transmitiendo, los resultados de las firmas no serán iguales a los resultados obtenidos al aplicar la función hash en el documento.

Existen dos tipos de esquemas sobre firma digital, el que se denomina esquema de firma digital con apéndice y el esquema de firma digital con mensaje recuperable. También cualquier esquema de firma cuenta con dos partes, la primera parte se denomina proceso de firma (similar al cifrado) y la segunda parte proceso de verificación de la firma (similar al descifrado).

El esquema más usado y conocido es el esquema de firma con apéndice y consiste en los siguientes puntos:

Proceso de Firma

1) El mensaje a firmar es M, se le aplica una función hash que reduce su longitud de forma única a un mensaje H(M) de longitud de 128 ó 160 bits, lo que permite ver cualquier mensaje de cualquier longitud como una cadena de caracteres de longitud constante.

2) H(M) se somete también a un proceso de codificación, por lo tanto se obtiene un número h(M), al que se le aplica la fórmula con la potencia d, equivalentemente con la llave privada del firmante.

3) Se envía entonces el mensaje firmado s

$$s \equiv h(M)^d \bmod n$$

Proceso de Verificación

1) El que recibe s, se supone conoce el mensaje M, aplica la función de verificación que depende de la llave pública de quien se dice propietario del mensaje

$$h' \equiv s^e \bmod n$$

2) Ahora se aplica la función hash al mensaje M y si h(M)=h' entonces acepta la firma

En un esquema con mensaje recuperable no es necesario saber el mensaje, después de que la firma es aceptada el mensaje puede recuperarse a partir de la firma Ejemplo

Tomemos los mismos parámetros del ejemplo en el esquema de cifrado, p=3, q=5, m=2, φ=8, e=3, d=3

Proceso de Firma

1) La firma del documento m es: $s = m^d \bmod n = 2^3 \bmod 15 = 8$
2) El mensaje firmado es entonces (m,s) = (2,8)

Proceso de verificación

3) Aplicando la función de verificación $s^e \bmod n = 8^3 \bmod 15 = 2$
4) Como 2 (obtenido de la fórmula anterior) = 2 (el mensaje enviado)
5) Entonces la firma es válida

Los mensajes de autenticación protegen a dos usuarios del intercambio de mensajes contra un tercer usuario. No obstante, no protege a los dos usuarios cuando se trata del enfrentamiento entre ambos.

Por ejemplo, se supone que el usuario A envía un mensaje autenticado al usuario B mediante un sistema de autenticación con una función Hash (realiza un resumen del mensaje transformándolo en 128 bits). Las siguientes disputas pueden ocurrir entre ambos

- El usuario B puede generar un mensaje y reclamar que proviene de A. B tan sólo ha de crear el mensaje falso, aplicar la función Hash y encriptar el resultado con la llave secreta de A y B, anteriormente intercambiada.
- A puede negar haber enviado un mensaje. Porque es posible que B lo haya creado, y no hay manera alguna de probar que A en realidad no ha enviado el mensaje.

Estos ejemplos pueden darse en situaciones de transferencias bancarias y otras operaciones monetarias, convirtiéndose dicha situación en un peligro. En estas situaciones donde no hay confianza entre el emisor y el receptor, algo más que la autenticación es necesario. La solución más atractiva al problema planteado es la firma digital. La firma digital es semejante a la firma escrita de un documento. Ésta ha de tener las siguientes propiedades :

- Ha de ser posible verificar el autor, la fecha y el tiempo de la firma.
- Ha de ser posible autenticar los contenidos durante el proceso de firma.
- La firma ha de ser verificada por tres partes, para resolver conflictos o disputas

Por lo tanto la función de firma digital incluye la función de autenticación.

Con las propiedades anteriormente descritas como base, se pueden formular los siguientes requerimientos para una firma digital :

- La firma ha de ser una parte extraída del mensaje que se quiere firmar.
- La firma ha de utilizar alguna información exclusiva del emisor, para prevenir una invención de un mensaje o una denegación.
- Ha de ser relativamente fácil producir una firma digital.
- Ha de ser relativamente fácil reconocer y verificar la firma digital.
- Ha de ser computacionalmente infactible generar una firma digital, ya sea construyendo un nuevo mensaje para una firma digital existente o construyendo una firma digital engañosa dado un mensaje
- Debe de ser práctico retener una copia de la firma digital almacenada.

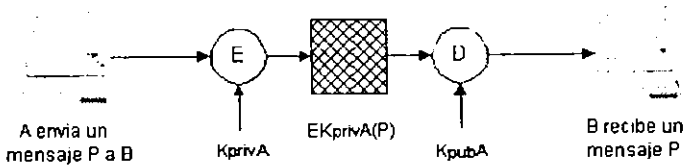
Ejemplos de firmas.

Donde.

K Algoritmo de Llave Publica.
E Encriptar / **D** : Desencriptar.
Kpriv Encriptación utilizando la Llave Privada
Kpub. Encriptación utilizando la Llave Pública

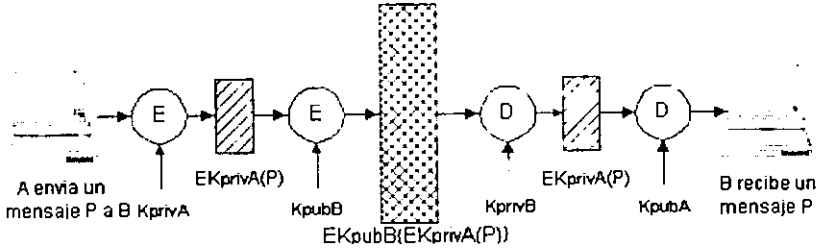
P : Mensaje.
H( ) : Función Hash = Resumen del Mensaje

1. Firma digital formada encriptando con la llave privada $Kpriv_A$ del emisor :



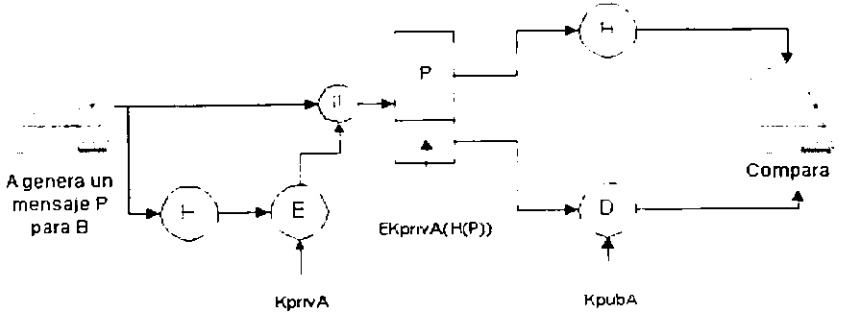
Firma Digital y Autentificación

2. Firma digital formada encriptando con la llave privada del emisor $Kpriv_A$ más confidencialidad :



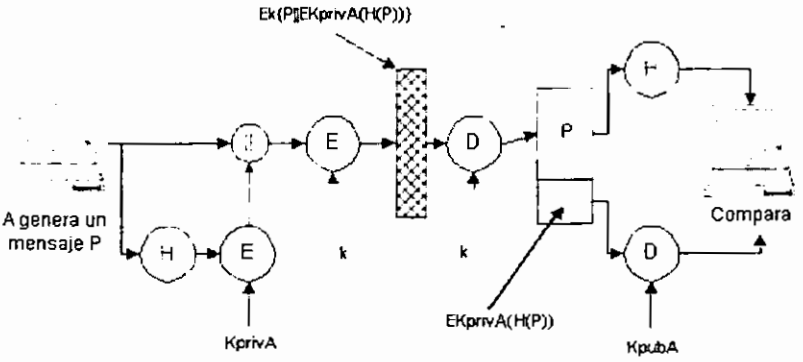
Firma Digital, Autentificación y Confidencialidad

3. Firma digital creada encriptando el resultado de una función Hash H() con la llave privada $Kpriv_A$ del emisor :



Firma Digital , Autentificación

4. Firma digital creada encriptando el resultado de una función Hash H() con la llave privada $Kpriv_A$ del emisor, más confidencialidad utilizando Criptología Convencional k:



Firma Digital, Autentificación y Confidencialidad

Los esquemas ilustrados anteriormente tienen en común una debilidad. La validez de los esquemas depende en gran medida de la seguridad con la que se mantiene en secreto la llave privada del emisor. Si un emisor desea negar haber enviado un mensaje algo comprometido, puede exponer que ha perdido la llave privada o que le ha sido robada y alguien ha generado una firma digital con ella.

Los problemas asociados con la firma digital directa pueden ser enderezados utilizando un tercer individuo como árbitro.

Al igual que con los esquemas de firma directa, existe una gran variedad de esquemas de firmas digitales arbitradas. En términos generales todos ellos operan de la siguiente manera. Cada mensaje firmado por un emisor X hacia un receptor Y se dirige primeramente a un árbitro A, que somete el mensaje y su firma a un número de pruebas para comprobar su originalidad y contenido. El mensaje es entonces fechado y enviado a Y con una indicación que demuestra que el mensaje ha sido verificado satisfactoriamente por el árbitro. La presencia de A resuelve el problema planteado por los esquemas de firma directa.

Firma Electrónica con el RSA

La implantación de la firma electrónica puede realizarse empleando el cifrado RSA.

Supuestos dos usuarios A y B del criptosistema de llave pública RSA con llaves o algoritmos de cifrado ($EKpu_A$,$DKpr_A$) y ($EKpu_B$,$DKpr_B$) donde E representa la clave de cifrado pública y D la de descifrado secreta.

Cuando B envía un mensaje a A lo haría de la forma siguiente: B → M →A

1) Emplea su algoritmo de descifrado llave privada $DKpr_B$ para firmar el mensaje

2) Cifra la firma S con el algoritmo de llave pública $EKpu_A$ de A.

2.6 Certificados y Autoridades de Certificación (AC)

El nacimiento del certificado digital fue a raíz de resolver el problema de administrar las llaves públicas, y que la identidad del dueño no pueda ser falsificada. La idea es que una tercera entidad intervenga en la administración de las llaves públicas, y asegure que las llaves públicas tengan asociado un usuario claramente identificado.

Las tres partes más importantes de un certificado digital son:

1) Una llave pública
2) La identidad del implicado: nombre y datos generales.
3) La firma privada de una tercera entidad llamada autoridad certificadora, que todos reconocen como tal y que válida la asociación de la llave pública en cuestión con el tipo que dice ser.

Uno de los problemas con la criptografía de llave pública es la confianza. Si alguien quiere suplantar a otra persona, lo único que necesita hacer es generar una llave pública/privada y publicar la llave pública con el nombre de otro. La mejor solución a este problema es el uso de certificados y autoridades de certificación.

- Certificados digitales o de llave pública. Es un documento digital que atestigua que una llave pública corresponde a la identidad de una persona, servidor o entidad determinados. Desafortunadamente este documento también se puede falsificar, lo que hace necesario el concepto de autoridad de certificación (AC)
- Autoridad de Certificación (AC). Es una autoridad en quien se puede confiar, vigila la identidad de personas o servidores para quien emite certificados. Es esencial que las llaves públicas de una AC se distribuyan desde un servidor confiable.

En su forma más simple, un certificado consiste en una llave pública y el nombre de su propietario. Este certificado es firmado por una autoridad de certificación (Certification Authority / CA), cuya llave pública es fácilmente verificable. Adicionalmente, puede contener la fecha de expedición del certificado, la de expiración de la llave, el nombre del notario electrónico que emitió el certificado y un número de serie. De todo ello calcula la firma con la función hash adecuada y la cifra con su llave privada.

Los certificados pueden adoptar múltiples formas. El formato más difundido está definido por la norma del ITU-T X.509 (versión 3), la cual forma parte del servicio de directorio diseñado por ISO para el modelo OSI. En el certificado se incluyen.

- versión de la norma X.509 usada.
- número de serie del certificado.
- emisor del certificado.
- algoritmo utilizado por la autoridad de certificación (algoritmo de llave asimétrica y función hash usada)
- periodo de validez.
- nombres que identifican unívocamente al dueño del certificado y a la autoridad de certificación
- la llave pública del dueño del certificado, junto con la información de los algoritmos utilizados.
- datos opcionales.
- la firma digital de la autoridad de certificación

El acceso a la información almacenada en un servidor, se puede controlar asignando certificados de usuarios a cuentas o grupos de usuarios, y asignando permisos de control de acceso a la cuenta de usuario o de grupo utilizando el mecanismo estándar de la Lista de control de acceso (ACL), que debería formar parte de los servidores. Una ACL permite o limita el acceso a un recurso de Internet basado en elementos como los nombres de usuarios, contraseñas y grupos.

La autenticación de clientes usando un canal seguro y certificados requiere.

- El protocolo de canal seguro ha de ser capaz de autenticar bidireccionalmente, es decir, tanto el cliente como el servidor deben manejar certificados

- El ciente debe ser capaz de verificar los certificados del cliente, solicitar y almacenar certificados personales y entregar un certificado personal al servidor cuando se lo solicite.
- El servidor debe ser capaz de solicitar un certificado al servidor, verificar los certificados del cliente y casar los certificados del cliente recibidos con la lista de control de acceso estándar usada en el servidor.

La autenticación de clientes mediante certificación tiene las siguientes ventajas:

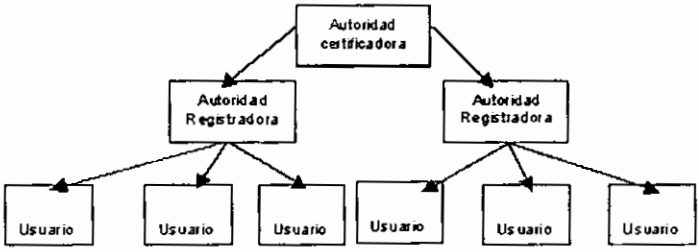
- No se envían contrasceñas desde el cliente al servidor. Como los certificados son información pública, los usuarios se auténtican sin enviar por la red información confidencial como son las contraseñas.
- Mejor forma de identificar al usuario. Los certificados contienen información que se puede comprobar sobre la identidad del usuario, en lugar de la autenticación basada en una dirección IP del usuario, un nombre de dominio o la dirección de correo electrónico. La dirección IP puede ser asignada dinámicamente en la configuración de la red, y se puede suplantar fácilmente los nombres de dominio y las direcciones de correo.
- Mejora la expenencia del usuario usando una única conexión. Los usuarios se conectan a muchos servidores diferentes de forma que no tienen que conectarse cada vez. Tan sólo tienen que conectarse una vez a la aplicación cliente y presentar su certificado al servidor para darle la información de identificación.
- Mejor autenticación. Como los certificados se basan en la tecnología de llave pública, se consigue una mejor autenticación: hay una parte pública que el usuario tiene, que se distribuye libremente a otros (el certificado) y contiene la identidad del usuario y su llave pública, y hay una parte privada que el usuario conoce, la llave privada y la contraseña que la protege.
- Administración más sencilla. Cuando se usa la autenticación mediante certificación se puede simplificar la administración y reducir los costos. Se consigue por la capacidad de los servidores de conceder acceso a los usuarios que presentan un certificado emitido por una autoridad certificadora. Cuando se configuran los servidores de esta forma no necesitan mantener una Lista de control de acessos (ACL). En otras configuraciones se disponen de mecanismos para que el administrador configure asociaciones para cada par certificado-usuario.

Un servidor y emisor de certificaciones es el medio para emitir, anular, reasignar y adminsitrar certificados. Un servidor debería seguir los estándares para aceptar solicitudes de certificados, el cual es el estándar de criptografía de llave pública PKCS.10. El formato estándar de certificados es el X.509.

El servidor emisor de certificados debería mantener una base de datos de información como la lista de revocación de certificados (LRC), información de los certificados emitidos, copias de los certificados, información sobre políticas de emisión de certificados e información sobre los emisores que pueden firmar certificados. El sistema de emisión debe permitir una fácil creación de una lista de emisión jerárquica. El emisor del nivel de root debe administrarse fácilmente.

2.7 Infraestructura de Llaves Públicas

Teniendo ya un certificado digital que es generado con la ayuda de un algoritmo de llave pública ahora el problema es como administro todos estos, la estructura más básica es la siguiente:



El papel de la Autoridad certificadora (AC) es de firmar los certificados digitales de los usuarios, generar los certificados, mantener el status correcto de los certificados, esto cumple el siguiente ciclo:

1) La generación del certificado se hace primero por una solicitud de un usuario, el usuario genera sus llaves pública y privada, y manda junto con los requerimientos de la solicitud, su llave pública para que ésta sea certificada por la AC
2) Una vez que la AR (es la AC regional) verifica la autenticidad del usuario, la AC vía la AR firma el certificado digital y es mandado al usuario
3) El status del usuario puede estar en: activo, inactivo o revocado. Si es activo el usuario puede hacer uso del certificado digital durante todo su período válido
4) Cuando termina el período de activación del certificado el usuario puede solicitar su renovación.

Entre las operaciones que pudiera realizar una AC están:

- Generar certificados
- Revocar certificados
- Suspender certificados
- Renovar certificados
- Mantener un respaldo de certificados

Entre las que pudiera realizar una AR están:

- Recibir las solicitudes de certificación
- Proceso de la autenticación de usuarios
- Generar las llaves
- Respaldo de las llaves
- Proceso de Recobrar las llaves
- Reportar las revocaciones

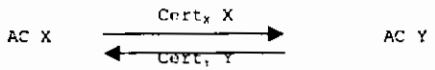
Y las actividades de los usuarios

- Solicitar el certificado
- Solicitar la revocación del certificado
- Solicitar la renovación del certificado

Una vez que algún usuario tiene un certificado digital puede usarlo para poder navegar por la red con nombre y apellido en forma de bits, esto permite entrar al mundo del comercio electrónico, al mundo de las finanzas

electrónicas y en general a la vida cibernética con personalidad certificada. El usuario dueño de un certificado digital tiene la potencialidad de poder autentificarse con cualquier otra entidad usuaria, también puede intercambiar información de forma confidencial y estar seguro de que ésta es integra, así estar seguro que contactos vía el certificado digital no serán rechazados. Los primeros usuarios de certificados digitales fueron los servidores, actualmente son quienes más los usan, sin embargo también se ha incrementado el número de personas que los usan.

Si suponemos que algún tipo de aplicación funciona ya con certificados digitales, ésta tendrá una AC y las correspondientes AR, sin embargo es común que haya mas autoridades certificadoras y que sus usuarios puedan interoperar con sus respectivos certificados, a esto se le conoce como certificación cruzada y opera de la siguiente forma:



1) Las diferentes AC pueden estar certificadas enviándose una a otra sus respectivos certificados que ellas mismas generan
2) Entonces la AC X tendrá el certificado de la AC Y y viceversa, podiendo generar un certificado para Y que genera X y otro para X que genera Y
3) Ahora como un usuario A de la AC X puede comunicarse con un usuario B de la AC Y
4) El usuario B envía a A el certificado de B que genera Y (Cert y B) junto con el certificado de Y que el mismo se genera (Cert y Y)
5) Ahora A puede validar a B (Cert y B) usando el certificado de Y que genera X

En la práctica se ha demostrado que el estatus de un certificado cambia con gran frecuencia, entonces la cantidad de certificados digitales revocados crece considerablemente, el problema está en que cada vez que se piensa realizar una comunicación y es necesario validar un certificado, se debe de comprobar que éste no esta revocado. La solución que se ha venido usando es la de crear una lista de certificados revocados LRC y así verificar que el certificado no está en esa lista, para poder iniciar la comunicación. El manejo de las listas de certificados revocados ha llegado a tener un gran costo, que sin embargo aún no se ha reemplazado por otra técnica a pesar que se han propuesto ya salidas al problema.

Las operaciones de la administración de los certificados digitales puede cambiar de acuerdo a las leyes particulares de cada país o entidad.

3. SISTEMAS ELECTRÓNICOS DE PAGO

3.1 Sistemas De Pago Basados En Tarjeta De Crédito

3.1.1 Tipos de Tarjetas

- **Por su presentación**
  - Código de barras
  - Banda magnética
  - Chip integrado
  - Impresas
- **Por su modo de almacenamiento**
  - Con memoria
  - Tarjetas chip
- **Por su modo de acceso**
  - Con contacto
  - Sin Contacto
- **Por su uso**
  - Control de acceso
  - Educación
  - Servicios de Salud
  - Pago electrónico
  - Servicios sociales
  - Transporte
  - Teléfono
  - Bancos
  - Identificación
  - Débito
- **Por su forma de pago**
  - Crédito
  - Débito
  - Cargo
  - Viajes y entretenimiento
- **Por el crédito que conceden**
  - Acreditativas
  - Crédito en un Sentido Estricto
- **Por el tipo de entidad emisora**
  - Bancarias
  - No Bancarias
  - Mixtas
  - Propias
- **Por el ámbito objetivo**
  - Universales
  - Particulares
- **Por el ámbito territorial**
  - Internacionales
  - Nacionales
  - Locales
  - Para un establecimiento en particular
- **Por el ámbito temporal**
  - Limitadas por el tiempo
  - Ilimitadas por el tiempo

3.1.2 Clasificaciones de Tipos de Tarjetas

a) Por el crédito que conceden.

1. Tarjetas en que el titular abona a fin de mes, en este caso no existe un verdadero crédito, la finalidad pareciera ser solamente facilitar los pagos. Estas son las denominadas: "tarjetas acreditativas".
2. Tarjetas que realmente otorgan un crédito a los titulares de las tarjetas. Estas son las que se denominan tarjetas de crédito en un "sentido estricto".

b) Por el tipo de la entidad emisora. Estas tarjetas pueden ser:

1. Bancarias, o sea tarjetas emitidas por un banco o por un grupo de bancos.
2. No bancarias, o sea las emitidas por sociedades comerciales, cuya única actividad es precisamente este tipo de operaciones.
3. Mixtas, son las emitidas por una sociedad comercial, apoyada por un banco o grupo de bancos.
4. Propias de un establecimiento comercial, son las que constituían el sistema primitivo de las tarjetas de crédito, las mismas son expedidas por dicho establecimiento que las utiliza como una credencial que distingue e identifica a determinados clientes: constituye un símbolo que exterioriza el crédito otorgado. El usuario de este tipo de tarjetas sólo la puede utilizar en el establecimiento que se la otorgó.

c) Por el ámbito objetivo

1. Tarjetas universales, mediante las cuales se pueden obtener todo tipo de bienes y servicios, sirviendo como ejemplo de ello la tarjeta American Express, Visa, etc.
2. Tarjetas particulares, que son las utilizadas para servicios particulares, como por ejemplo, gastos de hotel, viajes aéreos, alquiler de coches, compra de gasolina, compra en grandes almacenes.

d) Por el ámbito territorial de validez.

1. Internacionales, son las que se pueden utilizar en todo el mundo, como por ejemplo: Visa, Diners, Master Charge, etc.
2. Nacionales, son aquellas que solamente pueden utilizarse dentro del país expedidor.
3. Locales, se utilizan sólo dentro de una localidad determinada.
4. Para un establecimiento en particular, como la de Liverpool, Sears, etc.

e) Por el ámbito temporal.

1 Limitadas por el tiempo, la mayoría de las tarjetas se expiden por el lapso de un año y se van renovando automáticamente. Al final del período el ente emisor envía al titular una nueva tarjeta, sin mediar ningún requerimiento de este último. De este tipo son las emitidas por Visa, American Express.
2 Ilimitadas en el tiempo, dichas tarjetas no caducan nunca

f) Por su forma de pago.

1 Crédito, los pagos son asociados a una cuenta en especial con alguna forma de instalación de un esquema de pago o un giro de la línea de crédito. Las tarjetas típicamente tienen un límite de crédito definido por el emisor de la tarjeta y la tasa de interés será recaudada con pagos uniformes y ésta es la mayoría de las veces la tasa base de préstamo.
2 Débito, están ligadas a cuentas de cheques y ahorros. Un pago no puede ser hecho sino hay fondos disponibles.
3 Cargo, trabajan de forma similar como una tarjeta de crédito en las que el pago es contra una cuenta con un

propósito en especial. La principal diferencia es que las facturas para un cargo de tarjeta, deben ser pagadas al final del periodo de facturación. No hay límite de crédito.

4. Viajes y entretenimientos, son tarjetas de cargo que se usan en aerolíneas, hoteles, restaurantes compañías de rentas de coches, o para una compra en particular.

3.1.3 Tipos de Pago con Tarjetas de Crédito

1. Pagos usando los detalles de la tarjeta de crédito en claro. Es el método más fácil de pago con tarjeta de crédito, es el intercambio de los detalles de la tarjeta de crédito sin encriptar sobre una red pública tal como la línea telefónica o Internet. El bajo nivel de seguridad inherente al diseño de Internet hace que este método sea problemático (algún hacker puede leer el número de la tarjeta de crédito), y hay programas que pueden verificar el tráfico en Internet por los números de tarjetas de crédito y enviar los números a sus programadores. La autenticación es también un problema significativo, y el vendedor es usualmente responsable de asegurar que la persona que usa la tarjeta de crédito es el propietario.

2. Pagos usando los detalles de la tarjeta de crédito encriptados. Aunque los detalles de la tarjeta de crédito sean encriptados antes de ser enviados sobre Internet, todavía hay ciertos factores a considerar antes de enviarlos. Uno de esos factores es el costo de una transacción de tarjeta de crédito, la cual no aceptará pagos de bajo valor (micropagos.)

3. Pagos usando la verificación de una tercera parte. Una solución para los problemas de seguridad y verificación es la introducción de una tercera parte que colecte y apruebe pagos de un cliente a otro.

3.1.4 Ventajas y Desventajas de la Tarjeta de Crédito para los Participantes

1. Ventajas de la Tarjeta de Crédito para el Titular

a) No le es preciso llevar dinero en efectivo a fin de realizar los gastos en su lugar habitual de residencia o cuando viaja.
La tarjeta es nominativa, ofrece evidentemente una mayor seguridad en caso de pérdida e inclusive de robo.

b) La tarjeta posibilita pagar de una sola vez las compras del mes, esto genera además una economía de tiempo otorgando asimismo al titular un crédito, de hecho nada despreciable, ya que el mismo abona en plazos que varían.

El ente emisor envía resúmenes de cuentas, en los que se reproducen detalladamente las compras correspondientes al periodo transcurrido, facilitando de esta forma la buena organización de la contabilidad

c) Permite actividades no previstas con antelación como viajes, compras, etc.

d) La titularidad de una tarjeta de crédito importa un prestigio

e) Mediante la tarjeta se pueden realizar pagos u obtener servicios no sólo para el titular de la misma, sino en beneficio de terceras personas.

Las tarjetas de crédito, mediante extensiones de las mismas, sean personales o empresariales, permiten su uso a familiares del titular en el primer caso, o a ejecutivos o empleados bajo la responsabilidad de éstos en el segundo caso.

Además no necesita coleccionar facturas, sólo tendrá que guardar los cupones respectivos. Esto facilita el control de gastos para la empresa y evita que los empleados puedan economizar en beneficio propio, los gastos de representación

Los entes emisores realizan una delicada selección de solicitantes de tarjetas, basándose en:

1. Importancia de los ingresos.
2. Regularidad en los mismos.
3. Seriedad financiera.

2. Desventajas de la Tarjeta de Crédito para el Titular

a) Posibilidad de pérdida o robo de la tarjeta o uso indebido de ella. Esto supone graves riesgos, y por lo tanto el titular debe comunicar inmediatamente la pérdida de la tarjeta al organismo emisor, y quedará exento en principio de la responsabilidad.
b) Pago de cuota anual. Algunos entes emisores obligan al titular de la tarjeta a pagar una cuota por disponer de la tarjeta.
c) Posibilidad de comprar sin tener que desembolsar dinero, ya que el titular gasta más de lo debido.
d) Investigación previa sobre la situación financiera del candidato, es incomodo.
e) Hay ciertas entidades emisoras que limitan los valores de compra.

3. Ventajas de los Vendedores

a) Tienen garantizado el cobro de las facturas, siempre y cuando respeten todas las condiciones de funcionamiento del sistema: firma del cupón por parte del comprador, transcripción de los datos de las tarjetas, remisión de dicho cupón al organismo emisor dentro de los plazos determinados.
b) Evita los depósitos de dinero, sólo subsiste el pago del emisor al vendedor que se efectúa mediante giros bancarios o envío de cheques.
c) Evita el riesgo que significa recibir un cheque, ya que el mismo puede venir de vuelta por falta de fondos, o por cualquier otro motivo. El vendedor sabe que siempre que cumpla con el sistema el ente emisor le va a abonar.
d) Obtiene un aumento de su clientela.

4. Desventajas de los Vendedores

a) El pago de una comisión sobre las ventas efectuadas. La entidad emisora descuenta al vendedor una cantidad en concepto de servicios sobre el importe total de la factura.
b) El vendedor no tiene con el sistema de tarjetas la posibilidad de disimular sus ventas y beneficios al fisco.
c) Las exigencias que el ente emisor impone a los establecimientos en algunas oportunidades se toman complicadas y generan inconvenientes (control por parte del vendedor de la firma del titular, del boletín de cancelación, etc.)

5. Ventajas del Emisor (por lo general Banco)

a) Las tarjetas de crédito sirven para atraer clientela. En el caso de los bancos, es uno de los servicios de mediación de pagos y que trae consigo un aumento de los depósitos en cuenta corriente. En el caso de otro establecimiento que expida su propia tarjeta para compras en sus locales, este servicio puede atraer clientela por las comodidades que supone para el cliente, etc.
b) Es un modo de colocación rentable de dinero a corto plazo. La entidad emisora cobra por dos lados: del comerciante (descuento en las facturas) y del titular (interés por la concesión de crédito y cotización anual.)
c) El sistema de tarjetas de crédito sirve para evitar una multiplicidad de pagos. Las diferentes facturas de un cliente titular de tarjetas se pagan una sola vez a fin de mes. Esto constituye una disminución de los gastos, de errores contables, de personal y material.
d) La tarjeta de crédito hace innecesario el cheque y evita los inconvenientes y gastos de éste.
e) Gracias a la tarjeta de crédito se consiguen clientes fijos.

6. Desventajas del Emisor

a) Posibilidad de abusos en el empleo de tarjetas de crédito La entidad emisora sortea el riesgo de posibles abusos de personas insolventes (que utilizan su tarjeta para mayores gastos de los que pueden realizar) y de actos fraudulentos, como robos y falsificaciones. Únicamente quedará exenta de responsabilidad en caso de culpa o negligencia del titular o del comerciante.

b) Costo elevado de los programas de tarjetas de crédito. La entidad emisora deberá hacer frente a los siguientes gastos.

1. Gastos de publicidad.
2. No puede entregar la tarjeta a todo el que se la pida por los riesgos, por lo cual se ve obligado a seleccionar a los titulares y esto requiere gastos de investigación, secretaria, etc.
3. Recibe, clasifica las facturas, las paga y cobra luego su importe al titular de la tarjeta. Para esto necesita material y equipo costoso. Requiere personal competente y especializado.

3.1.5 First Virtual (FV)

First Virtual (FV) Holdings, Inc. , en octubre de 1994 crea un sistema de pago llamado VirtualPIN que no usa el cifrado. El objetivo era realizar ventas de información de bajo valor a través de la red sin la necesidad de un software especifico para el cliente o hardware especial. El sistema no es completamente a prueba de fraudes, pero en el contexto de su objetivo de mercado no es de gran importancia.

FV está construido en la cima de los protocolos de Internet existentes (e-mail, telnet, FTP y HTTP.) Estos protocolos son inseguros en el sentido de que no realizan pruebas de identidad. Se basa en el intercambio de mensajes e-mail y la honradez del cliente.

FV sirve como un corredor de transacciones de tarjeta de crédito entre compradores y vendedores. Ambos vendedores y compradores requieren registrarse con First Virtual (FV), antes de que alguna transacción tome lugar El registro se asegura por medio de una tarjeta de crédito.

En el registro del comprador se dan los detalles de su tarjeta de crédito y su dirección electrónica. El intercambio comienza llenando una forma WWW y dando una clave de acceso, la cual es confirmada por FV y agrega un sufijo a la clave de acceso para formar el VirtualPin. El siguiente paso es que el comprador realice una llamada telefónica a FV para dar su número de tarjeta de crédito. Esto permite establecer un vínculo entre el VirtualPIN y la tarjeta de crédito, sin que se use el número de la tarjeta de crédito a través de la red.

Los vendedores se registran de manera similar que los compradores, a diferencia que ellos dan los detalles de su banco a FV y éstos dan al vendedor un VirtualPIN. Se transfieren los detalles del banco enviando un comprobante convencional a la cuenta del banco asociada al chequeo. Una vez que esto está hecho, el vendedor puede pedir a FV que procese las transacciones del cliente registrado en FV y, después deducir un cargo por transacción, deposita los fondos en la cuenta del vendedor usando los servicios del banco ACH (Automated Clearing House.)

El comprador ingresa al sito Web del vendedor FV y selecciona el artículo que desea comprar. El comprador ingresa el VirtualPIN, el cual es enviado hacia el vendedor. El vendedor checa que el VirtualPIN sea válido preguntándole al servidor FV. Puede ser hecho varias veces, como un rango de peticiones manuales automatizadas con un diálogo con el servidor FV. Si el VirtualPIN no está en la lista negra, entonces el vendedor entrega la información al comprador, por e-mail, regresándola por el WWW, o algún otro medio.

El vendedor reenvía la información acerca de la transacción, incluyendo el VirtualPIN del comprador, al servidor First Virtual. El pago no se hace, porque el sistema se basa en la filosofía "intenta antes de comprar". El siguiente paso es que el servidor FV envié un e-mail al comprador preguntando si la información fue satisfactoria.

Hay 3 posibles respuestas a esta pregunta

- Acepta, en el caso de que el pago proceda;
- Rechaza, indica que los bienes no fueron recibidos o que el comprador no está feliz por su pago;
- Fraude, los bienes no fueron pedidos por el comprador. Y envia el VirtualPIN a la lista negra

Al final de cada 90 días, la cuenta de la tarjeta de crédito del comprador es facturada por los cargos que han sido acumulados durante ese periodo Entonces la cuenta de cheques del vendedor aparecerá con un saldo acreedor por los pagos del artículo vendido. FV ejecuta la contabilidad para el comprador y el vendedor, tomando un porcentaje de la transacción como comisión. Pero si el comprador se siente insatisfecho con el producto, el comprador tiene 90 días para reportar la insatisfacción a FV

Es poco probable que si un VirtualPIn es comprometido por los atacantes en la red, que las compras falsas puedan ser hechas en el tiempo en el que el VirtualPIN llega a la lista negra. Desde que la petición de autorización de pago es enviada al comprador por e-mail, en este tiempo podría obtener pocos minutos quizá en un dia o más. También, la negación del servicio o disfrazando atacantes en el sistema e-mail podría prolongarse este período poco substancialmente.

Un número de tarjeta de crédito robada, podría ser usada para colocar el VirtualPIN asociado con la dirección e-mail controlada por el atacante, la cual quizá permita largos períodos donde las transacciones falsas pueden ser cargadas.

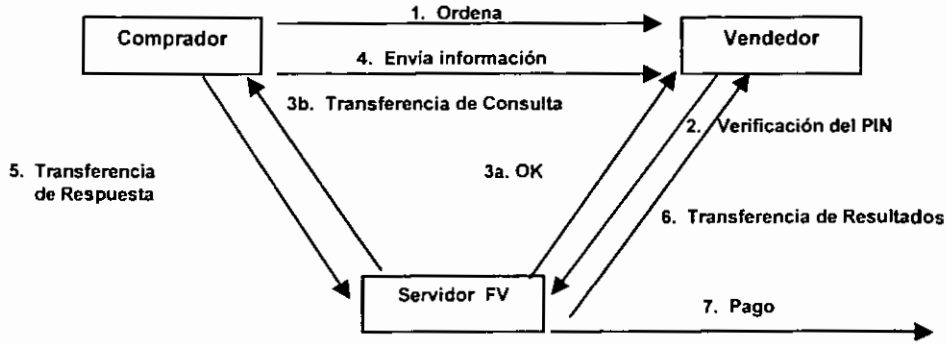
La exposición al fraude es de poca importancia si el sistema de pago es usado para la información de artículos. En este contexto, aunque un fraude ha sido cometido, el vendedor habrá perdido una venta en vez de incurrir en una gran pérdida financiera. La experiencia en el primer año de operación del sistema muestra una baja tasa de fraude. Desde el punto de vista de la compañía de tarjetas, FV asume el papel del vendedor en el que ellos son los primeros en establecer la relación con el adquirente, y el valor de todas las transacciones acreditadas a su cuenta en primera instancia antes de ser distribuidas usando las transferencias del banco ACH.

Ventajas

- Es simple.
- No hace uso de la encripción.
- El simple intercambio no necesita de un software en el front end.
- El software del back end no es complejo.
- Los compradores son virtualmente protegidos del fraude. Los cargos no son procesados contra su cuenta sin su confirmación.
- Las compras son esencialmente anónimas. El vendedor nunca da el nombre del comprador a FV.
- Es fácil llegar a ser un vendedor FV.
- FV tiene muy bajas tasas de interés de procesamiento, comparadas con los otros esquemas de pago en Internet o algún procesamiento de tarjetas de crédito.
- Se puede utilizar para pequeñas transacciones.

Desventajas

- Antes de poder usar el sistema vendedores o compradores, deben haberse registrado y haber tenido una cuenta en el banco (vendedor) o una tarjeta de crédito (comprador). Hay, otras cualidades no demandadas por los vendedores, en contraste con las estipulaciones típicamente hechas por los adquirentes de tarjetas de crédito, y esto hace que el sistema sea más atractivo para vendedores a quienes les gusta tener un limitado volumen de transacciones.
- Los vendedores asumen todo el riesgo.
- Extremadamente largo el período de espera entre el depósito de pago en la cuenta del vendedor y cuando se realizo la venta.
- Poca seguridad.
- No existe privacidad.



Compra con First Virtual

Vulnerabilidades

a) Engaño de IP (IP Spoofing)

Es una técnica en la cual una máquina conectada a Internet pretende ser otra, esencialmente roban su dirección IP. Es fácil para el atacante robar el tráfico que intentaba ir a otra máquina. De esta manera, todo el tráfico que intenta ir de una máquina puede llegar a la máquina del atacante.

Al momento de que la máquina criminal se hace pasar por otra, e intercepta las consultas de e-mail de FV. Si un atacante puede interceptar y responder tales consultas desde FV, él puede causar algunas transacciones financieras para ser consumadas sin la aprobación del tenedor de la cuenta

Esta técnica es limitada ya que es una tecnología cruda, que generalmente intercepta todo el tráfico de IPs a la máquina objetivo, y por lo tanto conduce al usuario de la máquina real a ver una pérdida o degradación de su servicio de Internet Por esta razón, generalmente detecta poca rapidez, en este caso puede a menudo ser rastreada por el delincuente. Por lo tanto el engaño IP es realmente inusual para un criminal cuando éste puede ser instalado por un breve momento y después removido. Este no es el caso con las transacciones FV, porque el tiempo asincrono (aleatorio) de las consultas de e-mail hacen esto imposible para un criminal, para saber precisamente cuando ocurrió el engaño.

Además, el engaño de IP es menos usual para un criminal que no sabe que máquina engañar. En orden de usar este engaño contra un tenedor de cuenta FV, un criminal primero deberá robar el Virtual PIN. El entonces debe determinar la dirección e-mail asociada con el Virtual PIN robado, la cual no es una asociación obvia y no siempre es fácil de hacer. Lo siguiente, el debe usar el engaño IP para interceptar el tráfico que intenta ingresar a la máquina de la víctima, y debe establecer el engaño lo suficientemente bien para interceptar el e-mail. Pero brevemente minimiza el riesgo de detección. El quizá sea capaz de consumar una sola transacción falsa. Sin embargo, tendrá otros riesgos para renovar el engaño cada vez que el quiera realizar una transacción fraudulenta

b) Administradores del Sistema Irrumpiendo

Un administrador del sistema sin escrúpulos, puede usar esto para accesar a las cuentas e-mail en el sistema, para comprometer algunas cuentas FV asociadas con los usuarios de las direcciones e-mail

Alguna gente cree que los sistemas basados en criptografía tienen este problema, pero esas gentes están en un error, ya que el administrador del sistema es la persona que instala el software de confianza en el sistema del

usuario final. El puede fácilmente instalar lo que parece ser una nueva versión de un software de encripción confiable, pero realmente roba toda la información vital antes de encriptarla y transmitirla.

El administrador del sistema ha sido siempre la persona poderosa en el mundo de la computación. Ellos pueden leer archivos privados, el mail, falsificar e-mails, falsificar evidencia que te hagan parecer un criminal, y todas las clases de otras cosas desagradables. Con el advenimiento del comercio electrónico, el rol de un administrador del sistema es inevitablemente el más importante, pero no en el sistema FV.

Nota: First Virtual Holdings Inc. en 1998 anunció que el sistema de pagos dejaría de existir, por lo cual este sistema actualmente no está vigente, pero se considera porque fue uno de los primeros sistemas de pago en ofrecer un esquema dirigido a efectuar, de forma segura, compras en Internet. El sistema FV proporcionaba a sus usuarios un identificativo personal (el famoso Virtual PIN) que había que utilizar en cada compra, en lugar del número real de tarjeta de crédito. FV solicitaba confirmación e-mail al cliente antes de cargar el pago a su tarjeta.

Procedimiento de Compra por Internet (First Virtual)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
1.	**Registro del Vendedor en First Virtual (FV)**	**vendedor**									
.1	Dan los detalles de su banco a FV, enviando un comprobante de la cuenta.										
2.	**FV asigna un VirtualPIN**	**FV**									
.1	Reciben los detalles de la cuenta del banco del vendedor										
.2	Asignan un VirtualPIN al vendedor										
3.	**Registro del Comprador en FV**	**comprador**									
.1	Da los detalles de su tarjeta de crédito y dirección electrónica a FV										
.2	Llena una forma WWW										
.3	Da una clave de acceso										
4.	**FV asigna un VirtualPIN**	**FV**									
.1	Reciben los detalles de la tarjeta de crédito del comprador										
.2	Confirma la clave de acceso del comprador										
.3	Agrega a la clave de acceso un sufijo para formar el VirtualPIN										
5.	**Dar detalles de tarjeta de crédito**	**comprador**									
.1	Realiza llamada telefónica a FV para dar su número de tarjeta de crédito										
6.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.1	Escribe la dirección de la ubicación de la tienda virtual				5	*					
7.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
8.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
9.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
10.	**Ingreso de datos por el cliente**	**comprador**									
1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario			5		*				*	
11.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos				5		*				
.2	Muestra los datos ingresados				5	*					

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
12.	**Muestra datos del cliente y del artículo**	**vendedor**									
	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	•			•		
13.	**Asignación de una cantidad del artículo**	**comprador**									
.1	Asigna una cantidad de compra.				5	•				•	
14.	**Señala las formas de envío**	**vendedor**									
.1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional).				5	•		•			
15.	**Elección de forma de envío**	**comprador**									
.1	Elige la opción más adecuada conforme a sus necesidades.				5	•				•	
16.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación				5	•					
.2	Menciona los procesos de pago					•		•			
17.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación				30	•	•				
.2	Selecciona First Virtual.				5	•				•	
.3	Ingresa su VirtualPIN.			5		•				•	
.4	Se envía al vendedor										
18.	**Corroboración del VirtualPIN**	**vendedor**									
.1	Checa que el VirtualPIN sea válido preguntando al servidor FV				15		•				
19.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	•			•		
20.	**Aceptación de la orden**	**vendedor**									
.1	Informa que la orden está lista.				5	•					
21.	**Envío del producto**	**vendedor**									
.1	Entrega la información al comprador por e-mail, WWW o algún otro medio.										
22.	**Recepción del producto**	**comprador**									
.1	Recibe el producto.		700			•					
23.	**Confirmación de la transacción**	**vendedor**									
.1	Reenvía la información de la transacción, junto con el VirtualPIN del comprador al servidor FV.		25			•					
24.	**Preguntar si fue recibido el producto**	**FV**									
.1	Envía un e-mail al cliente preguntando si fue satisfactoria la información pedida.										
25.	**Respuesta sobre la compra**	**comprador**									
.1	Responde acepto (rechazo o fraude)		25					•	•		
26.	**Cobro de la compra**	**FV**									
.1	Al final de cada 90 días se le hace un cargo por las compras que se han realizado en ese periodo										
.2	Se le abona al vendedor el cargo de la compra.										
.3	Toma un porcentaje de la cuenta del comprador y vendedor como comisión										

3.1.6 CARI (Collect all relevant information/Colección de toda la información relevante)

Diseñado en el ITP (Information Technology Partners/Socios de Tecnología de Información), Milford, CT, USA. Este método se basa en el uso de la tarjeta de crédito del comprador, obteniendo sus datos por medio de un teléfono usando un "voice robot/robot de voz", porque se piensa que el comprador rehuye a transmitir su información por la red.

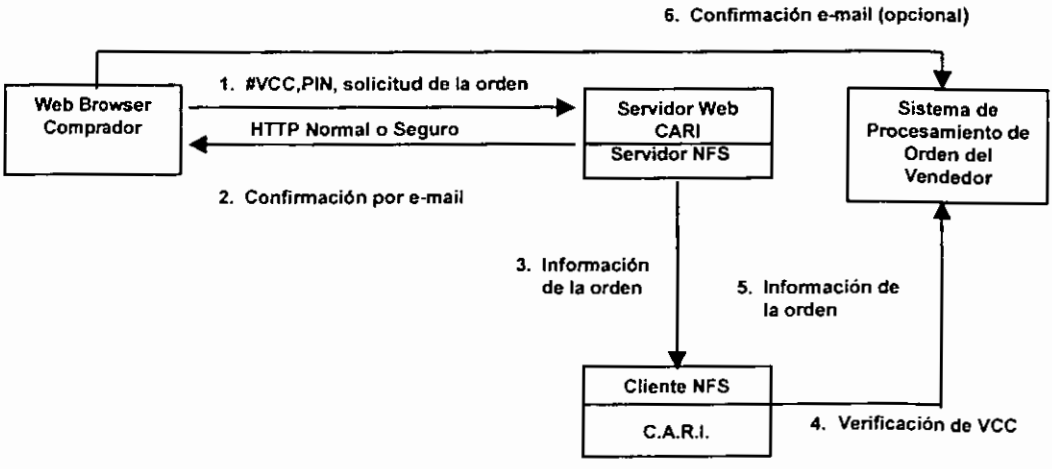
Primero el comprador debe obtener y activar una tarjeta de crédito virtual (VCC), ésta consiste en un rango de números aleatorios asignados por CARI que harán relación al número real de la tarjeta de crédito y a sus detalles (nombre que aparece en la tarjeta de crédito real, la dirección e-mail (para confirmar la compra), la dirección de envío, y el número telefónico). El VCC es protegido por un número de identificación personal (PIN), que previene el ingreso de otro número VCC de usuario por accidente durante una compra. Al obtener un VCC puede ser ocupado en cualquier tienda con conexión al servidor Web de CARI.

El VCC y el PIN son pasados al vendedor en una forma Web en el período de compra. Esto permite a CARI trabajar con todos los Web browsers y Softwares del servidor Web.

Esta información no es encriptada en HTTP. Sin embargo, provee seguridad a ambas partes el tener la capacidad de seguridad de HTTP (SSL), donde la conexión al HTTP Web es encriptada, y así la información podría ser protegida.

Para activar el VCC, los usuarios deben dar los detalles por teléfono de la tarjeta de crédito real a CARI. Una vez que la tarjeta real es verificada, el tono VCC es activado y el usuario puede iniciar la compra.

La principal ventaja de CARI es que el número de la tarjeta de crédito nunca viaja por Internet.



Procedimiento de Compra por Internet (CARI)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de una tarjeta de crédito virtual (VCC)**	**comprador**									
.1	Llama a CARI para dar sus datos de la tarjeta de crédito.										
2.	**Asignación de una VCC**	**CARI**									
.1	Recibe los datos de la tarjeta de crédito										
.2	Asigna una VCC y un PIN										
3.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda virtual con conexión al servidor CARI				5	*					
4.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
5.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
6.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*			*		
7.	**Ingresa de datos del cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*			*		
8.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados.				5	*					
9.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
10.	**Muestra datos del cliente y del artículo**	**vendedor**									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	*			*		
11.	**Asignación de una cantidad del artículo**	**comprador**									
.1	Asigna una cantidad de compra.				5	*				*	
12.	**Señalización de las formas de envío**	**vendedor**									
.1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional).				5	*		*			
13.	**Elección de forma de envío**	**comprador**									
.1	Elige la opción más adecuada conforme a sus necesidades				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
14.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación				5	*					
.2	Menciona los procesos de pago					*		*			
15.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación.				30	*	*				
.2	Selecciona CARI				5	*				*	
.3	Ingresa la VCC y el PIN			5		*				*	
16.	**Corroboración de datos**	**vendedor**									
.1	Checa que los datos ingresados sean reales conforme al método de pago elegido.				15		*				
17.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	*			*		
18.	**Aceptación de la orden**	**vendedor**									
.1	Informa que la orden está lista.				5	*					
.2	Envía un mensaje, para informar el número de la orden				30	*			*	*	
19.	**Envío del producto**	**vendedor**									
.1	Checa el depósito del pago.		25			*					
.2	Envía el producto.		25					*	*		
20.	**Recepción del producto**	**comprador**									
.1	Recibe el producto.		700			*					

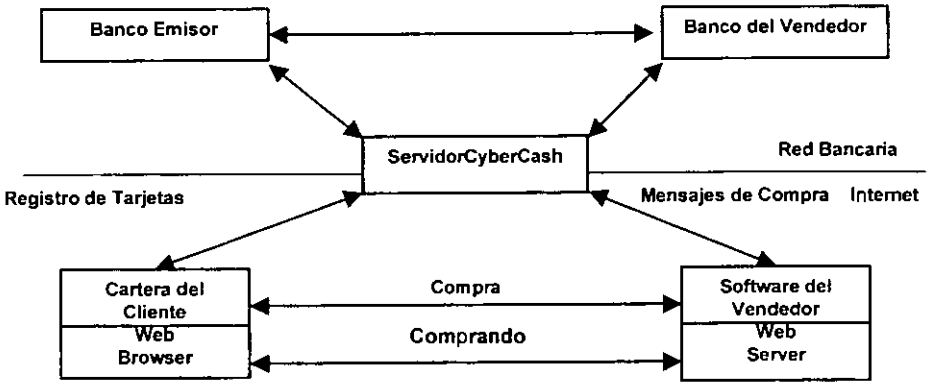
3.1.7 CyberCash (CyberEfectivo)

CyberCash, Inc. Dr Reston, Virginia. fue fundado en agosto de 1994 con el motivo de proveer software y servicios de solución para asegurar las transacciones financieras sobre Internet. Sirve como un conducto a través de los pagos que pueden transportarse rápidamente, fácilmente y seguramente entre compradores, vendedores y sus bancos. Aquí no se necesita que el comprador y el vendedor tengan alguna relación existente.

Como tercera parte neutral solo le concierne asegurar la entrega de pagos de una parte a otra.

Este sistema proporcionará varios servicios de pago por separado en Internet incluyendo, a la tarjeta del crédito y al dinero electrónico. Consiste en un software de cartera.

Un servidor de entrada une a la infraestructura financiera existente. Este es conectado a Internet de un lado y del otro a muchos bancos y procesadores de transacciones de tarjetas bancarias. Los mensajes de compra contienen los detalles de las tarjetas de crédito de los clientes y son enviados hacia el servidor de entrada del vendedor en el periodo de compra. La compra con la tarjeta de crédito es autorizada y capturada en los bancos que hay en la red. Los resultados de la transacción son remitidos a través del gateway CyberCash al vendedor. Si la transacción fue exitosa, el vendedor puede enviar los bienes al cliente. CyberCash no es un adquirente, ni emisor, o banco, pero provee una entrada que significa seguridad entre el paso de mensajes de Internet y los bancos de la red y viceversa.



Modelo CyberCash

Cartera CyberCash: Software usado por el cliente para realizar sus compras con su tarjeta de crédito, esto se logra escondiendo los detalles de los pasos del pago y mensajes durante la compra La cartera corre junto al Web browser

El software usa 56-bits DES (Data Encryption Standard / Estándar de Encripción de Datos) y 768-bits RSA para proteger los detalles de la tarjeta de crédito almacenados en el disco duro del usuario y en el protocolo de pago CyberCash.

Persona CyberCash: Cada usuario CyberCash escoge un único ID CyberCash y una clave de acceso. El ID es registrado contra el servidor de pago CyberCash y mapea a las llaves pública y privada del usuario.

El ID y la clave de acceso son usados para abrir la cartera, donde los datos de la tarjeta y las llaves secretas son almacenadas en forma encriptada. El ID también actúa como un mapeador entre el identificador del usuario y la llave pública del usuario dentro del sistema, tal como un certificado excepto que no hay una firma de autorización de una tercera parte. Finalmente, el ID y la clave de acceso pueden ejecutar un close-out de emergencia en caso de fraude. Cualquier intento de compra usando la tarjeta de crédito del consumidor es bloqueado, una vez que el close-out ha sido iniciado por contacto de CyberCash con la correcta clave de acceso

Aspectos de Seguridad

a) Autenticación e Identidad de la Persona

La autenticación de mensajes se basa en la encripción de llave pública como la provista por RSA. El Servidor CyberCash mantiene archivos de llave pública asociada con cada cliente y vendedor. Puede autenticar cualquier información firmada digitalmente por el cliente o vendedor, sin tener en cuenta la seguridad de la ruta de los datos en su camino al servidor. La llave privada correspondiente, la cual se necesita para crear tales firmas digitales, será guardada por el cliente o vendedor y nunca se revelará a otras partes. En el software del cliente, la llave privada sólo se guarda en forma encriptada protegida por una contraseña.

Mientras la verdadera identidad del cliente o vendedor CyberCash es reconocida por su par de llaves pública/privada, tales llaves también son difíciles para ser recordadas o tecleadas por la gente. Así que, las interfaces del usuario utilizan cortos ID's alfanuméricos seleccionados por el usuario o vendedor para los propósitos de una persona específica. CyberCash agrega dígitos verificadores al ID solicitado para minimizar la oportunidad de error accidental en la selección de la persona. El poseer un ID de una persona sin la correspondiente llave privada no es de ningún beneficio en el sistema actual.

Individuos u organizaciones quizá establecezcan una o más personas CyberCash. Así, un individuo puede tener varias personas CyberCash sin relación o compartir una persona CyberCash con otros individuos. Este enfoque proporciona un grado de privacidad consistente con presencia en Internet y con transacciones en efectivo específicamente. Sin embargo, poseedores de la persona que desean usar una tarjeta de crédito para las compras junto con su persona CyberCash, deben conocer el criterio de identificación online de como lo requiere la organización que emite tarjetas

El control de la persona está disponible sólo para una entidad que posee la llave privada para esa persona. Sin embargo, una provisión especial es asociar una contraseña de cierre de emergencia con una persona CyberCash. En el recibo de la contraseña de cierre de emergencia, aún cuando se recibió de canales inseguros como el teléfono o el e-mail ordinario, CyberCash suspenderá la actividad para la persona CyberCash. Esta contraseña de cierre de emergencia puede ser guardada separadamente de y con menos seguridad que la llave privada para la persona; la contraseña de emergencia no puede ser usada para desviar fondos. Esto proporciona alguna protección contra pérdida o malversación de la llave privada o de la contraseña bajo la cual la llave privada se ha guardado encriptada. En el sistema de efectivo, la contraseña de emergencia quizá transfiera el balance de la persona a una cuenta del banco designada.

b) Privacidad

La encripción de mensajes usa el Estándar de Encripción de Datos (DES/Data Encryption Standar). Se planea reencriptar en especial información sensible, como los números PIN, y los maneja para que la versión de texto plano leíble nunca exista en el sistema de CyberCash excepto momentáneamente, antes de reencriptar bajo otra llave.

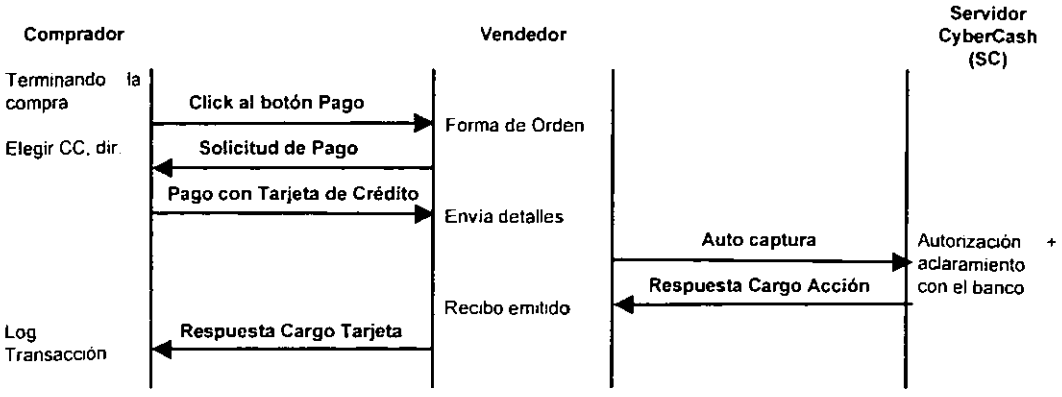
El proceso de cargos de la tarjeta a través del sistema CyberCash, se organizó para que el vendedor nunca vea el número de la tarjeta de crédito del cliente, a menos que el banco del vendedor libere esta información o que se requiera para la resolución de una disputa. Además, el servidor no mantiene un almacenamiento permanente de números de tarjeta. Sólo están presentes mientras una transacción que involucra tarjetas está en marcha. Esto reduce la oportunidad de malversar el número de la tarjeta.

Una compra CyberCash

Habiendo completado la compra y por lo tanto habiendo acordado el precio en el sitio Web del vendedor, el consumidor da un click en el botón de pago en el sitio, el cual invoca el software CyberCash del vendedor. El vendedor regresa una factura en línea de los artículos adquiridos que incluye información de la compra como artículos adquiridos, precio y el ID de la transacción a través del Web browser del comprador. Este mensaje causa que la cartera CyberCash sea desplegada en la máquina del comprador, y sean pasados los detalles de la compra.

El comprador agrega la tarjeta de crédito que el desee usar para pagar e información adicional, la cual ya ha sido registrada con el software. Estando de acuerdo con los detalles de la orden presentada, entonces se da un click al botón de pago de la cartera. Este inicia el protocolo de pago CyberCash. Los detalles de la tarjeta son seguramente enviados al vendedor. Es entonces cuando la información de la factura y de la tarjeta de crédito es firmada digitalmente por el software de CyberCash del cliente, encriptada, se pasa junto con un código hash de la factura, al vendedor. El vendedor autoriza y aclara el pago con la red financiera vía el servidor de pagos CyberCash. El vendedor regresa el recibo con información de la autorización adicional y es encriptada, firmada electrónicamente por el vendedor, y enviada al Servidor CyberCash

Las firmas digitales son usadas por las tres partes (tarjetahabiente, vendedor, y gateway de pago) para la autenticación y no repudiación durante la compra. El Servidor CyberCash puede autenticar todas las firmas y, puede estar seguro que el cliente y el vendedor están de acuerdo en la factura y en la cantidad de cargo. El servidor CyberCash entonces envía la información pertinente al banco adquirente, junto con una solicitud a nombre del vendedor para una operación bancaria específica, como una autorización de cargo. El banco decripta la información y entonces procesa los datos recibidos como si procesara una transacción normal de tarjeta de crédito. La respuesta del banco es regresada al servidor CyberCash, el cual devuelve un recibo electrónico al vendedor, al recibirla el vendedor se apresura para enviársela al cliente. La transacción se completo.



Pasos de una compra CyberCash

Mensajes CyberCash

Son transportados independientes así que pueden ser enviados por el HTTP del Web, el protocolo SMTP del e-mail, o algún otro protocolo de transporte. Cada mensaje consiste de:

- Encabezado: Identifica el inicio de un mensaje CyberCash e incluye información de la versión.

El encabezado consiste en una sola línea que se parece a:

```
$$-CyberCash-0.8-$$
```

o así

```
$$-CyberCash-1.2.3-Extra-$$
```

Incluye un número de campos separados con el carácter menos " -"

1. "$$" cadena literal con la inicial $ en columna 1.
2. "CyberCash" cadena literal (caso insensitivo).
3. x.y o x.y.z número de la versión del formato del mensaje. x es el número de la versión primaria y es un número de la subversión. z, si presenta, el número de una subsubversión.
4. "extra" cadena alfanumérica adicional optativo.

El primer número de versión es 0.7 y contando. La cadena "Extra" se usa dentro de ambientes seguros para que el subcomponente pueda poner una nota.

Las partes del cuerpo del mensaje (transparente y oculto) consiste de un par de atributos en formatos evocadores del formato del encabezado del correo electrónico normal. Hay sin embargo, algunas diferencias

Inicia con nombres de atributos y están compuestos de letras y guiones internos, excepto que algunas veces acaban con un guión seguido por un número. El número se usa cuando hay lógicamente un índice vector de valores. Los nombres del atributo son frecuentemente etiquetas. Si la etiqueta acaba con un ":", entonces el proceso está hecho. Mientras la existencia de arrastrar espacios es significante. Sin embargo, si la etiqueta se termina con un ";", esto indica un campo de forma libre donde los caracteres de la nueva línea, y dirigen a algún espacio en blanco, después del espacio inicial indica una continuación de línea.

Se ignoran líneas de espacios en blanco y no significan un cambio a un diferente modo de manejo de la línea.

Después de haber encontrado una línea inicial **$$**, puede tratar con cualquier línea conforme al primer carácter Si es alfanumérico, es una nueva etiqueta que debe terminarse con un ":" o ";" e indica un nuevo par de valores de etiqueta. Si es un espacio en blanco, indica la continuación del valor para la nueva línea de la etiqueta precedente. Si es "$", debe ser la línea final del mensaje. Si es #, es un comentario y debe ignorarse

- Transparente. Es la parte de texto plano del mensaje. Puede contener información de la orden de compra, el ID de la transacción, fecha, y el identificador de la llave usada para encriptar la parte oculta del mensaje. El identificador de la llave permite al receptor saber cual llave seleccionar para desencriptar la parte oculta. Contiene información que no es privada

  Esta parte incluye cualquier dato en texto claro asociado con la transacción financiera, así como con la información necesitada por CyberCash y otros para decriptar la(s) partes ocultas. Siempre incluye un campo de la transacción, que es el número de la transacción generado por el solicitador y que se repite en la respuesta. Siempre incluye un campo de fecha, que es la fecha local y tiempo del solicitador y es repetido en la respuesta. En todos los demás casos es un registro inicial para establecer un ID de persona, incluye ID de la persona solicitadora.

En mensajes limitados por el servidor, hay una "cyberkey:" campo que identifica el servidor de llave pública fue usado para encriptar la llave de sesión.

- Oculto: La parte oculta del mensaje consiste en un solo bloque de caracteres codificados usando codificación base64. Los datos en la sección oculta siempre son encriptados antes de la codificación. Contiene los datos financieros encriptados. Esta parte no se presenta en algunos mensajes. Cuando se presenta usualmente provee protección contra alteraciones para la parte en claro.

  La etiqueta "oculta" o "vendedor-oculta", precede a la parte oculta dependiendo de si los datos fueron encriptados por el software del cliente o el vendedor.

  En mensajes entrantes al servidor, los datos son ocultos con la encripción DES-CBC, los encripto bajo una llave de transacción aleatoria y entonces esa llave DES es encriptada con RSA bajo una llave pública del servidor. RSA encripta la llave de DES que aparece como la primera parte de la campo codificado base64 y no se saca como un valor separado en el mensaje. La salida correspondiente de la respuesta del servidor simplemente puede ser encriptada con DES bajo la llave de transacción, como hay bastante información en texto claro para identificar la transacción, y el cliente o el vendedor habrán recordado la llave de transacción del mensaje entrante.

  Una firma no es generalmente necesaria en la parte oculta de una respuesta del mensaje. El conocimiento de la llave de la transacción es adecuada para autenticación. Para que alguien falsifique la respuesta, tendrá que conocer la llave privada del servidor para ser capaz de obtener la llave de la transacción. Se asume que si alguien alterara con la respuesta la parte oculta, la probabilidad que habría de decriptar algo es insignificante. Mientras alguien puede alterar la parte transparente, esto normalmente no tiene ningún efecto o significa que el cliente no encontró la llave de la transacción, este caso es un ejemplo de rechazo de servicio por un mensaje dañando.

- Avance: Usado para indicar el final del mensaje CyberCash. También contiene un checksum de transmisión para que el receptor cheque que el mensaje que recibió está intacto. Este checksum es implementado como un hash MD5 de las tres primeras partes del mensaje, intenta detectar daño al mensaje, no libra de alteraciones.

Ningún carácter nulo (valores cero) o caracteres con el octavo bit son permitidos en un mensaje CyberCash.

Firmas y Funciones Hash

Los mensajes de solicitud CyberCash entrantes normalmente tienen una firma, de todos los campos de los mensajes fuera de la firma. Esta firma se transmite dentro de la parte oculta del mensaje. Permite al servidor autenticar la fuente del mensaje.

Los mensajes del vendedor a un cliente comienzan una secuencia de la compra que tenga campos firmados por el vendedor. Estos campos y esta firma son incluidos por el cliente en la parte oculta de su mensaje de compra con tarjeta para el vendedor, cuando se pasan al servidor, puede verificar que el cliente vio la información del vendedor.

a) Firmas digitales

Las firmas digitales son un medios de autenticar información. En mensajes CyberCash, son calculados tomando el hash de los datos a ser autenticados, y codificando el hash usando una llave privada RSA. Cualquiera que posea la llave pública correspondiente puede decriptar el hash y compararlo con el hash del mensaje. Si son iguales, entonces puede estar seguro que la firma fue generada por alguien que poseía la llave privada que correspondía a la llave pública que usó y que el mensaje no fu alterado.

En el sistema CyberCash, clientes, vendedores, y el servidor tiene pares de llaves pública/privada. Guardando la llave privada en secreto y registrando la llave pública con el servidor (para un vendedor o cliente) o publicando su llave pública o llaves (para el servidor), ellos puedan proporcionar alta calidad en autenticación firmando partes de mensajes. Una firma digital RSA es aproximadamente del tamaño del módulo usado.

b) Funciones Hash

Los hash usados en mensajes CyberCash son resúmenes del mensaje. Es decir, es una impresión no invertible de un mensaje tal que es computacionalmente infactible encontrar un mensaje alterno con el mismo hash. Si confía en la autenticidad del hash y se presenta un mensaje que iguale al hash, puede estar seguro de que es el mensaje original.

El hash es calculado usando el algoritmo MD5. El mensaje sintético está compuesto de etiquetas y valores especificados en una lista para un hash particular. El hash es una orden dependiente de la entrada, es esencial que los pares de los valores de la etiqueta se reúnan en el orden especificado. En algunos casos, un rango de etiquetas igualadas es especificado.

Si una etiqueta se especifica en una lista de firmas, pero no está presente en el dato del valor de la etiqueta en los que el hash se calculo, no es incluido en el hash. Es decir, incluso la etiqueta y el terminador de la etiqueta se omiten desde el mensaje sintético.

Antes de iniciar el hash, el texto del mensaje sintético se procesa para quitar todos los "espacios en blanco". Los espacios en blancos son definidos como cualquier valor ASCII de 32 (espacio) o menos de 127 o más grandes. Las nuevas líneas, los retornos de carro, los espacios, los tabuladores, etc. son ignorados por el hash. Los hash MD5 son de 16 bytes de longitud. Esto significa que la codificación base 64 de ese hash será de 24 caracteres.

Registro de la Persona y Recuperación de la Aplicación

El primer paso del cliente para usar CyberCash es registrar a una persona usando la aplicación del cliente. Esto se hace con el mensaje R1y el servidor CyberCash responde con el mensaje R2.

Cuando la aplicación del cliente aprende que está fuera de fecha, puede usar el mensaje de solicitud GA1 para el servidor y su respuesta GA2 baja una nueva versión firmada de sí mismo.

- Registro (R1): Mensaje inicial enviado para crear una nueva Persona CyberCash
- Registro Respuesta (R2): Mensaje de respuesta de éxito o fallo de R1.
- Obtener Aplicación (GA1): Usado por CyberApp para conseguir la actualización de una versión.
- Conseguir Aplicación Respuesta (GA2): Devuelve exitoso y la URL de la copia actualizada de CyberApp si falla.

Uniendo Tarjetas de Crédito

El sistema CyberCash está diseñado para dar el control a la organización emisora de la tarjeta, si una tarjeta puede usar el sistema CyberCash. El cliente, después de haber registrado a una persona con CyberCash, puede unir cada tarjeta de crédito deseando usar su persona CyberCash. Esto se hace vía el mensajes BC1 del cliente al servidor CyberCash y BC4 es la respuesta del servidor.

- Une Tarjeta Crédito (BC1): Éste es el mensaje inicial en el proceso de unión de una tarjeta de crédito a una personas CyberCash.
- Respuesta Unión Tarjeta Crédito (BC4): Indica que el proceso de unión de una tarjeta de crédito ha terminado. Regresa éxito o fracaso

Mensaje de Compras con la Tarjeta de Crédito del Cliente

CyberCash se introduce después de que el ciclo de compra inicia con tarjeta del crédito, cuando el usuario ha determinado lo que está comprando. Cuando pulsan el botón de pago en CyberCash, un mensaje PR1 se envía del vendedor al cliente como cuerpo de un mensaje de tipo MIME aplicación /cybercash.

Si el cliente desea proceder, responde al vendedor con un CH1. El vendedor responde con un CH2 pero entre el recibo de CH1 y la emisión de CH2, el vendedor normalmente se comunica con el servidor CyberCash vía los mensajes CM*.

- Solicitud de Pago (PR1): Este mensaje es inicialmente enviado del vendedor al tarjetahabiente para desplegar el software de la cartera de CyberCash. Contiene un sumario de la orden firmada por el vendedor. La firma es verificada después por el servidor CyberCash y no por el tarjetahabiente actual. La compra ha sido completada. Este es el punto de pagar por las compras.
- Pago de Tarjeta de Crédito (CH1): Este mensaje es del tarjetahabiente al vendedor. Incluye los datos de la tarjeta encriptados con la llave pública del servidor CyberCash (Kpu_{SC}) y firmado por el comprador. También contiene un hash de la orden para mostrar acuerdo contra el vendedor, sin revelar lo que la orden es y la firma inicial del vendedor es remitida.
- Respuesta Cargo Tarjeta (CH2): El vendedor reenvía los recibos sin firmar del gateway al tarjetahabiente. Envía un CH1 e indica éxito o fallo.

Mensaje de Compras con Tarjeta de Crédito del Vendedor

El vendedor presenta las compras con tarjeta de crédito, hace ajustes, y envía los mensajes CM*. En general, el ciclo de tarjeta de crédito es conseguir autorización para una compra, capturando la compra en un lote para aclaración, entonces ejecuta la aclaración. También es posible una captura nula (es decir, remover un artículo de un lote), y procesos de créditos (ingresos).

Las autorizaciones siempre vienen de un adquiriente en la respuesta a un mensaje CM1 o CM2. Si la captura es realizada por el adquirente o alguna entidad entre el servidor CyberCash y el adquirente, esto se hace vía un mensaje CM3 o CM2 que depende del arreglo entre el vendedor y la entidad que hace la captura. Los ingresos (créditos) son manejados en el mensaje CM5. El mensaje CM4 se mantiene vacío a una captura o retorno antes de que el lote sea aclarado. CM6 es el formato del mensaje usado para las respuestas de todos los mensajes CM *.

La actual disputa de la resolución de los sistema de tarjeta de crédito, asume que el vendedor sabe el número de la tarjeta. Por lo tanto, para trabajar con esos sistemas, el especial paso de mensajes ha sido colocado para permitir al vendedor obtenerlos, para una transacción particular, la información CyberCash se esconde del vendedor.

Muchos vendedores operan en un modo de captura de terminal donde las autorizaciones son capturadas por el vendedor, después envía el lote del pago

- Sólo Auto (CM1): Este mensaje es usado por el vendedor, para ejecutar una operación de autorización en la tarjeta de crédito enviada por el cliente.
- Auto Captura (CM2): El vendedor envía los datos de la tarjeta encriptada y la orden al gateway. El gateway verifica la firma del tarjetahabiente en los detalles de la tarjeta, y la firma del vendedor enviada en los detalles de la orden. El gateway verifica que ambos el cliente y el vendedor estén de acuerdo con la orden. Hace la autorización y actualmente ingresa los cargos para el aclaramiento. Es como CM1, pero de diferente tipo.
- Post Auto Captura (CM3): Captura un cargo autorizado previamente. El mensaje es igual que CM1 sólo que también tiene un campo Autorización-Código (qué es incluido en la firma) y el tipo es diferente.

- Nulo (CM4): Vacía un cargo/regresa si recibió antes del aclaramiento. El mensaje es igual que CM1 sólo que también tiene un campo de recuperación-referencia-número (que también es incluido en la firma) y el tipo es diferente.
- Regreso (CM5): Regresa un cargo previo. Realmente ordena un cargo negativo. Es similar a CM1 pero de diferente tipo.
- Respuesta Cargo Acción (CM6): Al haber autorizado y capturado la compra en la red bancaria, el gateway regresa los recibos sin firmar para el vendedor y del comprador al vendedor.

La Serie de Mensajes MM*

La serie de mensajes CM *, es sobre los primeros sistemas de compra CyberCash con tarjeta de crédito para asegurar el manejo de los cargos desde los clientes CyberCash. Sin embargo, los vendedores que son autorizados al banco del adquirente para aceptar tales cargos, quizá también reciban el teléfono, correo, y ventas fuera del mostrador. Para evitar alguna necesidad de que el vendedor tenga un segundo sistema en paralelo para manejar esos cargos, un MM1 a través de una serie de mensajes MM6 es definida y ha sido implementada para las transacciones menos seguras.

Los mensajes MM* son similares a la serie CM*, pero la sección "oculta del cliente" es actualmente firmada por el vendedor y separa el ID CyberCash del cliente o antes une a la tarjeta requerida.

- Solicitud de datos de la tarjeta (CD1): Usado por el vendedor para conseguir el número de la tarjeta, etc., si la información se necesita por el vendedor para resolverse una disputa.
- Respuesta de los Datos de la Tarjeta (CD2): Responde a un CD1 con fracaso o con éxito y los datos de la tarjeta.

Mensajes de Error y Utilidad

Varios mensajes de utilidad, consultas de estados, y el reporte especial de error ha sido necesario implementarlos en el sistema CyberCash.

Es deseable poder probar la conectividad, sincronizar relojes, y conseguir una determinación inicial de que el protocolo del cliente y las versiones de software son aceptadas. Esto es hecho vía el del cliente P1 para el mensaje del servidor y el P2 del servidor a la respuesta del cliente.

Los clientes necesitan poder determinar el estado antes de las transacciones, cuando el cliente o el vendedor ha chocado durante o ha sufrido pérdida de datos desde la transacción. Dos mensajes de consulta de la transacción son definidos, TQ1 y TQ2. Uno sólo pregunta y el otro también cancela la transacción, sino se ha completado todavía. La respuesta a estos mensajes es una respuesta TQ3 del servidor.

Puesto que el sistema opera en un modo de respuestas de consulta, hay dos casos donde se necesitan mensajes de error especiales. Si una consulta parece ser de un tipo indeterminado o no conocido, el mensaje de error UNK1 es enviado. Si una respuesta parece ser indeterminada o de tipo desconocido, u otras condiciones serias de error ocurren al cliente o al vendedor, el cual debería de firmarse en el servidor CyberCash, los mensajes del log DL1 o DL2 son enviados por el cliente o el vendedor en las preguntas respectivas.

- Ping (P1): Verificación ligera de que se tiene conectividad desde el cliente al servidor. No hace ningún crypto para minimizar la sobrecarga
- Respuesta Ping (P2): La respuesta de los pings P1 de peso ligero. No hace ningún crypto para minimizar la sobrecarga
- Consulta de la Transacción (TQ1): Pregunta del cliente al servidor por el estado de la Transacción
- Cancelación de la Transacción (TQ2): Pregunta del cliente al servidor por el estado de cancelación de la Transacción
- Respuesta de la Transacción (TQ3): Informes generados por un TQ1 o TQ2.

- Error Desconocido (UNK1): Ésta es la respuesta enviada cuando la solicitud es mala y no puede determinar qué tipo es o el tipo es desconocido. Enviado desde el vendedor al cliente o del servidor al vendedor o del servidor al cliente.
- Log de Diagnóstico (DL1): El log de diagnóstico del cliente de un mal mensaje desde el vendedor o el servidor.
- Log de Diagnóstico del Vendedor (DL2): El log de diagnóstico del vendedor de un mal mensaje desde el servidor.

Proceso de Autorización / Aclaramiento de la Tarjeta del Crédito

Hay seis pasos en el proceso de la tarjeta del crédito. Los primeros cuatro siempre toman que la transacción ya se completo. El quinto y sexto son optativos.

1. Autorización: el vendedor contacta al adquirente de regreso, el cual normalmente contacta al banco emisor de la tarjeta y regresa al vendedor una aprobación/garantía o una desaprobación. Esto temporalmente disminuye el crédito disponible en la tarjeta.
2. Captura: la información de cargo para una compra se ingresa por el vendedor en un lote.
3. Aclaramiento: un lote de artículos es procesado. Esto realmente causa que aparezcan los artículos en el lote de los estados de la tarjeta de crédito como enviados por el banco emisor a su tarjetahabientes.
4. Pago: las transferencia interbancaria de fondos netos.
5. Nulo: el vendedor deshace el paso 2 (ó 6) y causa un cargo (o crédito) para ser removido de un lote. Debe ser hecho antes de que el lote sea procesado.
6. Crédito: el vendedor causa un "cargo negativo" o lo acredita para ser ingresado en un lote. Esto aparecerá en los estados de los tarjetahabientes.

Ventajas

- Usa encripción robusta para transportar la información de pago.
- El vendedor no ve el número de tarjeta del comprador
- Los vendedores no tienen que esperar un período de tiempo para recibir el pago como FV. La cuenta bancaria del vendedor es acreditada dentro del tiempo de la estructura normal para una transacción con tarjeta de crédito.
- Conexiones persona a persona son posibles.

Desventajas

- Compradores potenciales y vendedores deben instalar un software para usar el sistema. Esto es difícil para personas que no tienen experiencia en el manejo de las computadoras.
- Los vendedores necesitan tener una cuenta con un banco adquirente que acepte los pagos seguros en Internet.
- Es costoso.
- No provee una privacidad real.

Procedimiento de Compra por Internet (CyberCash)

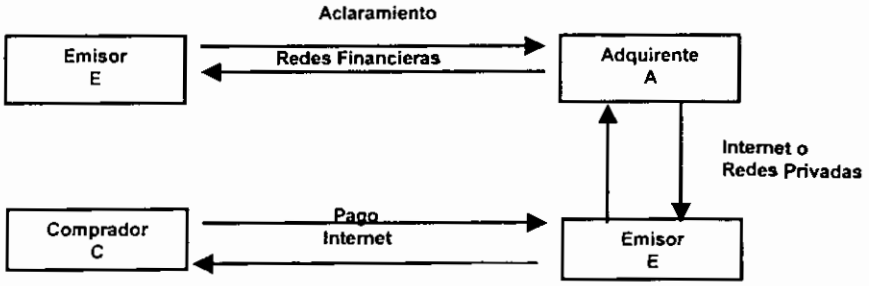
	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención del Software**	**comprador vendedor**									
.1	Obtienen el software Cybercash. Comprador (cartera) y vendedor (sw del vendedor)										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliento**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados.				5	*					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
9.	**Muestra datos del cliente y del artículo**	**vendedor**									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
.1	Asigna una cantidad de compra.				5	*				*	
11.	**Señalización de las formas de envío**	**vendedor**									
.1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional).				5	*		*			
12.	**Elección de forma de envío**	**comprador**									
.1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación				5	*					
.2	Menciona los procesos de pago					*		*			
14.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación.				30	*	*				

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
.2	Selecciona el método de pago.				5	*				*	
15.	**Corroboración de datos**	**vendedor**									
.1	Checa que los datos ingresados sean reales conforme al método de pago elegido.				15		*				
16.	**Muestra de la orden de compra**	**vendedor**									
.1	Envía una factura de los artículos adquiridos.				5	*			*		
.2	Despliegue de la factura en la cartera del comprador.										
17.	**Ingreso de Datos del Sistema de Pago**	**comprador**									
.1	Ingresa los datos de la tarjeta de crédito e información adicional.			5		*				*	
18.	**Aceptación de la orden**	**comprador**									
.1	Verifica que ésta de acuerdo con la orden.				5	*					
19.	**Envío de datos de pago**	**cartera**									
.1	Firma digitalmente los datos de la tarjeta y de la factura, los encripta y aplica funciones hash.										
.2	Envía los datos.										
20.	**Aceptación de la compra**	**SW vendedor**									
.1	Autorización y aclaramiento del pago.										
.2	Envía un recibo al servidor CyberCash, con información de la autorización, firmado y encriptado.				30	*			*	*	
21.	**Autorización del cargo**	**Servidor CyberCash**									
.1	Auténtica firmas del comprador y vendedor.										
.2	Envía la información pertinente al banco adquirente, junto con una solicitud en nombre del vendedor para la autorización de cargo.										
22.	**Proceso de Información**	**adquirente**									
.1	Decripta la información.										
.2	Procesa la transacción de tarjeta de crédito.										
.3	Regresa respuesta al Servidor CyberCash.										
23.	**Respuesta de la transacción.**	**Servidor CyberCash**									
.1	Envía un recibo electrónico al vendedor.										
24.	**Recepción del recibo**	**vendedor**									
.1	Recibe el recibo enviado por el Servidor CyberCash.										
.2	Lo envía al comprador.										
25.	**Envío del producto**	**vendedor**									
.1	Envía el producto.		25					*	*		
26.	**Recepción del producto**	**comprador**									
1	Recibe el producto.		700			*					

3.1.8 iKP (Protocolo de Pagos de Llaves en Internet / Internet Keyed Payments Protocol)

iKP[10] (donde i=1,2,3) es una familia de protocolos que definen una arquitectura para seguridad de pagos, involucrando tres o más participantes, desarrollados en los laboratorios de investigación de IBM en Zurich y el Centro de Investigación Watson en E.U. Se dice que iKP define una "Arquitectura" porque especifica un protocolo base que permite elegir entre varias opciones de diferentes negocios o requerimientos de seguridad. La "Seguridad de pagos" es provista por la criptografía de llave pública, y difiere de otros basados en el número de participantes que poseen sus propios pares de llave pública. Este número es indicado por el nombre de los protocolos: 1KP, 2KP, 3KP. Se provee mayor seguridad, si el mayor número de participantes tienen sus pares de llave pública. El protocolo 1KP está basado en infraestructura de seguridad que existe hoy. Los protocolos 2KP y 3KP pueden ser fasados gradualmente para lograr completa seguridad de pago multipartidario, como la más sofisticada infraestructura de certificación que pudiera estar en su lugar. Permite un despliegue del sistema gradual. Pueden ser "tres o más participantes", porque siempre se involucran compradores y vendedores que invocan a un tercer participante, tal como un sistema de tarjeta de crédito o bancos, que permiten transacciones de pago.

Involucra transferencias de pago entre bancos u otras organizaciones financieras, por medio del uso de tarjetas de crédito y débito, y también por cheques electrónicos, pero no permite el uso de dinero electrónico. Su principal objetivo es proporcionar a Internet una base para asegurar los pagos electrónicos, mientras se utiliza la infraestructura financiera para la autorización y aclaración de pagos.



Participantes en el protocolo

1) Comprador (C) Entidad que compra bienes, información o servicios, vía Internet.
2) Vendedor (V): Entidad que vende bienes, información o servicios y recibe un pago.
3) Adquirente (A). Banco del vendedor, adquiere tickets de cargo de los vendedores.
4) Emisor (E): Banco del comprador, emite cargos de tarjetas para los compradores.

En los protocolos iKP, el adquirente actúa como un gateway entre Internet y las redes financiera existentes que soportan transacciones entre bancos. Los protocolos iKP tratan sólo con las transacciones de pago, no son protocolos de compra (no proveen encripción de la información del pedido) Su función de ventas es permitir el pago de las transacciones entre varias partes involucradas. Por eso estos protocolos son compatibles con los diferentes browsers

Administración de Certificados

iKP se basa en la criptografía de llave pública(RSA). Al realizar un pago electrónico puede ser que se involucren una, dos o tres llaves públicas, por lo general el adquirente tiene un par de llaves, pública y privada, para recibir información confidencial como el número de cuenta del comprador y para firmar la autorización del mensaje, el vendedor quizá tenga su par de llaves para firmar las solicitudes de pago y las confirmaciones de compra y el comprador también puede tener un par de llaves para firmar la autorización del pago.

El vendedor y el comprador deben tener la llave pública del adquirente en el pedido para validar su firma del método de autorización. Específicamente el comprador requiere la copia para poder encriptar su número de cuenta y su información. Si el vendedor firma la factura, el comprador y el adquirente necesitaran la llave pública del vendedor. Si el comprador firma el pago, el adquirente y algunas veces el vendedor necesitaran la llave pública del comprador.

Las llaves públicas son distribuidas como certificados firmados por alguna autoridad, y pueden ser distribuidos:

1. Antes de ejecutar iKP (en el browser o fuera de línea)
2. Al momento de ejecutar iKP.

El establecimiento de una autoridad certificadora (AC), y la comunicación de la raíz de la autoridad de la llave pública son establecidas fuera de este protocolo. Cada sistema de tarjeta de crédito debería tener su propia autoridad certificadora con su raíz de llave pública, y esta firmaría los certificados para los adquirentes, vendedores y compradores que utilicen ese sistema de tarjeta de crédito. También otras organizaciones confiables pueden emitir certificados para alguno o todos los participantes de iKP.

Negociación contra Pago

Las transacciones de compra se dan en tres fases:

1. Negociación de los términos de compra y otros detalles,
2. Pago actual, y
3. El pedido realizado/entregado.

La negociación es una comunicación bilateral entre comprador y vendedor que puede darse de varias formas (vía HTTP usando un browser WWW y un servidor, e-mail, catalogo de ofertas del vendedor y e-mail para el pedido del comprador). El proceso de negociación, no se dirige sólo a lo que se pidió (x unidades de tal artículo y de otros más) pero si a los términos del pedido (precios, dirección de entrega, horarios, crédito, tipo de la tarjeta), y el método de pago (efectivo, cheque, dinero digital, iKP, si un recibo se requiere, etc.). En cualquier punto de la negociación siempre el comprador comenzará el pago, aquí es cuando la negociación acaba e iKP inicia.

iKP requiere los siguientes datos en el sistema del comprador: llave pública del adquirente, llave pública del vendedor (si se implemento), número de cuenta del comprador (CAN), llaves pública/privada del comprador (si se implemento), PIN del comprador (si se implemento), cantidad del pago y moneda ($$), y descripción del pedido (DESC).

iKP requiere los siguientes datos en el sistema del vendedor: llave pública del adquirente, ID del vendedor, llaves pública/privada del vendedor (si se implemento), llave pública del vendedor (si se implemento), cantidad del pago y moneda ($$), y descripción del pedido (DESC)

La descripción del pedido (DESC) es una cadena oculta que es incorporada por medio de un hash dentro del protocolo unido a la descripción de pago. iKP, no tratara de conocer el contenido de la descripción lo único que le interesa es que tenga los detalles relevantes de la transacción y, que vendedor y comprador tengan la misma cadena oculta.

Se dice que iKP es una arquitectura general porque:

- Interacciona con una gran variedad de métodos de pago por medio de seleccionar algunos flujos de mensajes o campos opcionales.
- Se puede usar en varios canales de comunicación entre los participantes (HTTP, S-HTTP, e-mail)
- Hay una sintaxis para cada canal de comunicación a pesar del estilo de compra (tarjeta de crédito contra tarjeta de débito)

Requisitos de Seguridad

a) Requisitos del Emisor/Adquirente

Asumen emisor y adquirente disfrutar un acuerdo de confianza mutua. Son más, las infraestructuras que habilitan la comunicación segura entre las partes que ya están acordadas. Por consiguiente, los requisitos del emisor y adquirente, son:

- [REQ A1] Prueba de Autorización de la Transacción por el Comprador. Al cargar una cuenta, el adquirente debe tener prueba que el dueño de la cuenta ha autorizado el pago.
- [REQ A2] Prueba de Autorización de la Transacción por el Vendedor. Cuando el adquirente autoriza el pago al vendedor, el adquirente debe tener prueba de que el vendedor está deseoso de aceptar el pago.

Ambos deben cumplir con este tipo de pruebas:

- Prueba Débil: autentica comprador a adquirente pero no proporciona no repudiación.
- Prueba Fuerte: proporciona no repudiación, es decir, pueden usarse para resolver disputas entre el comprador y proveedor del sistema de pago.

Nota: Si en los requisitos que se muestran a continuación, se hace referencia a pruebas débiles y fuertes, nos estaremos refiriendo al mismo tipo de pruebas mencionas anteriormente

b) Requisitos del Vendedor

- [REQ V1] Prueba de Autorización de la Transacción por el Adquirente. El vendedor necesita una prueba de que el adquirente autorizó el pago.
  - Prueba Débil.
  - Prueba Fuerte.
- [REQ V2] Prueba de Autorización de la Transacción por el Comprador. El vendedor requiere una prueba de que el comprador autorizó la transacción.
  - Prueba Débil.
  - Prueba Fuerte.
- [REQ V3] Imposibilidad de un Pago Desautorizado. No debe ser posible el pago sin que el vendedor dé su autorización
  - Imposibilidad los pagos desautorizados son imposibles con tal de que el adquirente no se comprometa.
  - Disputabilidad aún cuando el adquirente se comprometa, el vendedor puede demostrar no haber autorizado el pago.

c) Requisitos del Comprador

- [REQ C1] Imposibilidad de un Pago Desautorizado. No debe ser posible cargar a la cuenta del comprador sin posesión del número de cuenta, (optativo) el PIN, y (si aplica) la llave secreta de firma del comprador.
  - Imposibilidad. los pagos desautonzados son imposibles con tal de que el adquirente no se comprometa.
  - Disputabilidad. aún cuando el adquirente se comprometa, el vendedor puede demostrar el no haber autorizado el pago.

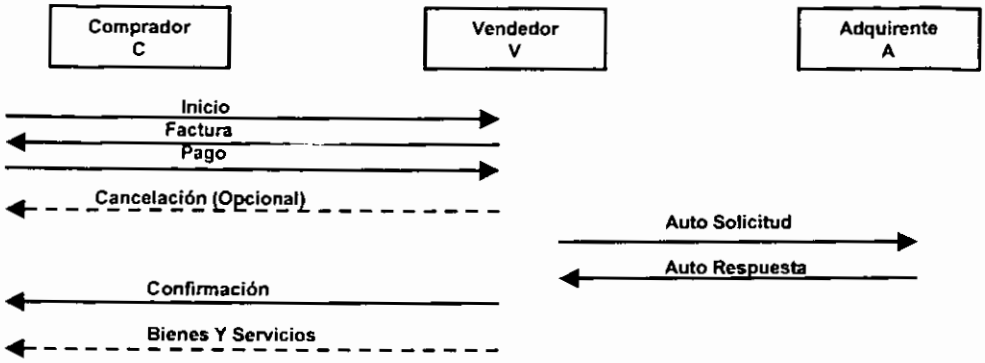
- [REQ C2] Prueba de Autorización de la Transacción por el Adquirente. El comprador exige una prueba de que el adquirente autorizó la transacción.
- [REQ C3] Certificación y Autenticación del Vendedor. El comprador necesita una prueba de que el vendedor es acreditado por algunos adquirentes (garantía para la fidelidad del vendedor.)
- [REQ C4] Recibo del Vendedor. El comprador necesita una prueba de que el vendedor recibió un pago y, así, promete entregar los bienes.
  - Prueba Débil.
  - Prueba Fuerte.
- [REQ C5] Retiro de Transacción/Pedido.
  - Comprador y vendedor quieren mantener la privacidad de la información del pedido, del intruso en el canal $C \leftrightarrow V$.
  - Comprador y vendedor quieren esconder la descripción de los bienes/servicios del adquirente y del intruso en el canal del $V \leftrightarrow A$.
- [REQ C6] Anonimato. El comprador quiere proteger su identidad de los intrusos y de los vendedores. Esto incluye la incapacidad del vendedor para poner en correlación múltiples transacciones de pago por el mismo comprador.
- [REQ C7] Compromiso en beneficio del Vendedor. El comprador solicita varias ofertas de múltiples vendedores (browsing) antes de escoger hacer el pago.

e) No Requisitos

Lo siguiente es considerado fuera de alcance de los protocolos iKP:

- [NREQ 1] Sin rastro de pago con respecto al sistema del pago (Un adquirente iKP puede identificar al comprador y vendedor.)
- [NREQ 2] Capacidad en Tiempo-Real (pago pequeño). iKP no pueden garantizar un cierto rendimiento Esto significa que no hay apoyo para los pagos pequeños en tiempo real.
- [NREQ 3] Entrega Segura de bienes/servicios. iKP no se preocupa por entregar bienes/servicios.
- [NREQ 4] Negociaciones de monto del pago (precio) y otros detalles.
- [NREQ 5] Protección del análisis de tráfico y cobertura de canales. iKP no es una "Gran" solución de seguridad; no proporciona confidencialidad para la información que no es considerada importante en una transacción de pago

Funcionamiento de iKP



1. Inicio: El comprador inicia el flujo del protocolo.
2. Factura: El vendedor responde regresando una factura.
3. Pago: El comprador genera una instrucción de pago y la envía al vendedor.
4. Cancelación: El vendedor puede rehusarse a continuar con la transacción.
5. Auto Solicitud: El vendedor envía una solicitud autorizada al adquirente.
6. Auto Respuesta: El adquirente usa los existentes sistemas de aclaración en la red para obtener la autorización y regresar una respuesta autorizada.
7. Confirmación: El vendedor envía la respuesta firmada del adquirente y otro parámetro adicional al comprador.

Datos intercambiados en una transacción iKP y símbolos:

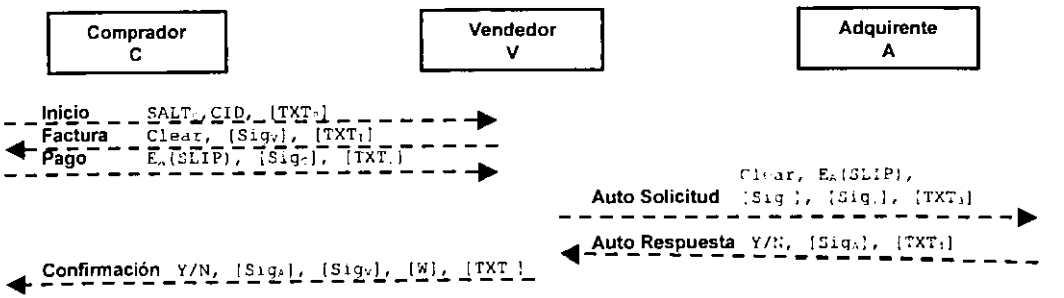
Dato	Descripción
A, V, C	Participantes en el Protocolo
[...]	Campos opcionales
Kpu_Z/Kpr_Z	Llave pública y privada de Z, donde $Z=\{A,V,C\}$
E	Encripción (con integridad) con Kpu_A. Toma un mensaje M para ser encriptado y un número aleatorio SALT y produce un texto cifrado $E_{Kpu_A}(M, SALT)$.
S-{TXT}	Firma con Kpr_C
$$	Monto y Moneda.
H(.)	Función hash one-way robusta.
CAN	Número de cuenta del comprador
ID	ID del vendedor. Identifica al vendedor al adquirente .
TID	ID de la transacción. Único identificador de la transacción.
DESC	Descripción de los bienes o servicios de compra, como una cadena oculta. Incluye información del pago tal como el nombre del tarjetahabiente y un número de identificación del banco.
SALT	Número aleatorio generado por C, usado para asegurar la privacidad de la información del pedido en el canal V ↔ A.
NONCE	Número aleatorio generado por el vendedor para proteger de la repetición. Puede ser implementado con un contador
DATE	Fecha/Hora actual del vendedor
PIN	PIN del comprador, si se presenta puede ser usado opcionalmente en 1KP para reforzar la seguridad.
Y/N	Respuesta desde la tarjeta del emisor. Sí/No o un código de autorización.

Dato	Descripción
R_C	Número aleatorio escogido por C para formar CID. Debe servir como prueba para el comprador de que el vendedor acordó el pago.
CID	Un pseudo-ID del comprador el cual únicamente identifica a C. Computado como $CID=H(R_C, CAN)$.
W	Número aleatorio generado en 2KP y 3KP por el vendedor. Usado para unir la confirmación a los mensajes de factura y pago.
TXT_i $J \{0,1...\}$	Información opcional que puede acompañar el flujo. Puede ser usada para llevar al contexto identificadores.

Datos formados con la combinación de los datos mencionados anteriormente

Dato	Descripción
Common	Información común por todas las partes: $SS, ID_C, TID_V, DATE, NONCE_V, CID, H(DESC, SALT_C), [H(W)]$
Clear	Información transmitida en la aclaración: $ID_C, TID_V, DATE, NONCE_V, H(Common), H(DESC, SALT_C)$
SLIP	Instrucciones de pago: $SS, H(Common), CAN, R_C, [PIN]$
$E_A(Slip)$	Instrucciones de pago encriptadas con la llave pública del adquirente: $Kpu_A(SLIP)$
$CERT_X$	Certificado de llave pública de X, emitida por un AC
Sig_A	Firma del adquirente: $Sig_A[H(Y/N, H(Common))]$
Sig_V	Firma del vendedor en Auto Solicitud: $Sig_V[H(H(Common), [H(W)])]$
Sig_C	Firma del tarjetahabiente: $Sig_C[H(E_A(Slip), H[Common])]$

Contenido del flujo



Notas:

- Si Sig_V está presente en la Factura, entonces debe ser incluido en la Auto Solicitud y Confirmación.
- Si Sig_C está presente en el Pago, entonces debe ser incluido en la Auto Solicitud.
- H(W) debe ser incluido en COMMON, si y sólo si Sig_V está presente en la Factura.
- Si H(W) es incluido en COMMON, entonces W debe proporcionarse en la Confirmación.

Los aspectos siguientes del protocolo son optativos.

- [OPT1] Firma del comprador Sig_C en el Pago
- [OPT2] Firma de vendedores Sig_V en la Factura (mutuamente exclusivo con OPT8)
- [OPT3] Comprobación del vendedor de Sig_C en el Pago(sólo si OPT1)
- [OPT4] El sexto procedimiento entero Confirmación
- [OPT5] Comprobación del comprador de Sig_A en la Confirmación (sólo si OPT4)

- [OPT6] Comprobación del comprador de Sig_V en la Factura
- [OPT7] Comprobación del comprador de V (sólo si OPT4, OPT2 y OPT6; o OPT4, OPT8 y OPT9)
- [OPT8] Firma de vendedores Sig_V en Auto Solicitud (mutuamente exclusivo con OPT2)
- [OPT9] Comprobación del comprador de Sig_V en Confirmación (sólo si OPT4 y OPT8)

Relación entre requisitos y opciones. (el 0 significa ninguna opción.)

REQUISITOS	OPCIONES NECESARIAS
A1 a	0
A1 b	1
A2 a+b	2 ó 8
S1 a+b	0
S2 a	0 *
S2 b	1, 3
S3 a+b	2 ó 8
B1 a	0
B1 b	1
B2	4, 5
B3	2 ****
B4 a+b	2, 6, 7 ó 7, 8, 9
B5 a	0 ***
B5 b	0
B6	0 **
B7	6

Notas:

* La prueba de autorización del comprador siempre es indirecta, es decir, el vendedor toma el Y/N del adquirente para demostrar que la autorización del comprador fue verificada.

** El anonimato es sin sentido si se usa OPT1, a menos que el comprador comunique directamente al adquirente o el certificado del comprador no se transmite en público.

*** Un intruso que captura $SALT_C$ en el canal C ↔ V puede montar un ataque contra $H(DESC,SALT_C)$ y obtener DESC

**** Un certificado del vendedor que certifica ID_V y su dirección electrónica ya podría servir como una prueba débil.

1KP

En este protocolo solo el adquirente necesita poseer y distribuir su certificado de llave pública $CERT_A$. Encripción de llave pública es requerida sólo desde el comprador, mientras la decripción es requerida sólo por el adquirente. Ambos compradores y vendedores son requeridos para verificar la firma generada por el adquirente. Cada entidad participante en el protocolo se asume que posee alguna información inicial. Información de cada entidad del sistema:

Actor	Datos de Información
Comprador	DESC, CAN, Kpu[illegible], [PIN], CERT
Vendedor	DESC, Kpu[illegible], CERT
Adquirente	Kpr[illegible], CERT

Asume que comprador y vendedor han acordado la descripción de los bienes (DESC) antes de comenzar el protocolo. También asume que tarjetahabiente y vendedor poseen la llave pública de la AC y el certificado del adquirente desde el cual ellos pueden extraer su llave pública.

a) Iniciación

1. El comprador forma una sola vez un ID del tarjetahabiente (CID) que lo identifica. Es computado como el hash del número de cuenta del comprador (CAN), y un valor aleatorio R_c CID=H(R_c,CAN).
2. Genera otro número aleatorio $SALT_c$, que será usado por el vendedor como Sal para elegir la información de la descripción de los bienes (DESC), para evitar revelarlo al adquirente.
3. El comprador transfiere las dos cantidades al vendedor como parte Inicial del mensaje.
4. Pone TXT_0 para incluir las opciones protocolares deseadas y/o DESC.
5. Envía Inicio.

b) Iniciando Proceso y Composición de la Factura

1. El vendedor recupera $SALT_c$ y CID de Inicio.
2. El vendedor genera $NONCE_v$ y DATE. Este permite al adquirente identificar únicamente un pedido. También escoge un ID de la Transacción (TID_v) para identificar el contexto.
3. Computa H(DESC,$SALT_c$) y está ahora en una posición para formar Common. El vendedor entonces computa H(Common).
4. Envía Clear en el flujo de la factura al comprador

Factura: (ID_v,TID_v,DATE, $NONCE_v$,H(Common))

c) Procesando la Factura

1. El comprador ya tiene DESC y $SALT_c$ como parte de su información de inicio y computa H(DESC,$SALT_c$). Esta cantidad es incluida en Common por el vendedor y es usada por el comprador para formar Common en el siguiente paso.
2. Computa H(Common) y verifica que esté el valor de H(Common) en el Clear generado por el vendedor. Este confirma que comprador y vendedor están de acuerdo sobre el contenido de Clear.
3. Genera una instrucción de pago (SLIP). El también incluye el número aleatorio R, el cual fue usado para crear CID. Este permite al adquirente checar que el CID dado al vendedor corresponde al CAN en el mensaje de pago, pero el vendedor no recobra el número de cuenta del comprador. El entonces encripta el SLIP usando la llave pública del adquirente.
4. Transfiere el SLIP encriptado(EncSlip) al vendedor como parte del flujo de pago.

Pago: (K_{pub} (Slip))

d) Procesando el Pago

1. Si por alguna razón el vendedor decide no llevar a cabo más procesos de mensajes, envía un mensaje de Cancelación al comprador.
2. El vendedor ahora ejecuta una autonzación. Forma un mensaje de Auto Solicitud. El vendedor incluye Clear y H(DESC,$SALT_c$) junto con EncSlip, el cual es recibido como parte de la instrucción de pago. Este permite al adquirente formar Common y verificar H(Common) generado por el vendedor y el comprador

Auto Solicitud: (EncSlip, Clear, H(Desc,SALTc))

e) Procesando Auto Solicitud

1. El adquirente extrae de Clear el valor H(Common) computado por el vendedor. Este es referido como h1. Este también checa para repeticiones que usan los valores ID_v,TID_v,DATE y $NONCE_v$

2. Decripta EncSlip y extrae H(Common) de SLIP como computado por el comprador. Este es referido como un h2.
3. Checa que h1=h2. Asegura que ambos comprador y vendedor esten de acuerdo en la información del pedido.
4. Reforma Common desde varios campos que se reciben en la Auto Solicitud y asegura que H(Common) = h1 = h2. Para abreviar Common consiste de un número de campos y H(Common) permite a los participantes del protocolo verificar que todos ellos están de acuerdo en los detalles (ej., precio y descripción de los bienes) de la transacción. Sin embargo, cantidades como la descripción de información (DESC) y número de cuenta del tarjetahabiente (CAN), son disfrazados de manera semejante que sólo las partes que necesitan saber que información está dando acceso a ésta.
5. El adquirente entonces contacta al emisor de la tarjeta y obtiene liquidación para la transacción.
   Al recibir una contestación del emisor, el adquirente computa una firma digital en la contestación (Y/N) y H(Common) y envía la Auto Respuesta al vendedor.

$$\text{Auto Respuesta: } (Y \ / \ Y, \ Sig_A)$$

f) Procesando la Auto Respuesta

1. El vendedor verifica la firma (Sig_A).
2. El vendedor remite la respuesta y la firma del adquirente al comprador como parte del flujo de confirmación del mensaje. El comprador en turno verifica la firma del adquirente y que la transacción esté completa.

El 1KP es simple y eficiente para efectuar pagos electrónicos con los mínimos requerimientos para agregar infraestructura de certificación. Sus debilidades son:

- Un comprador se auténtica para un vendedor usando solo un número de tarjeta de crédito y un PIN opcional opuesto al uso de firmas digitales.
- El vendedor no se auténtica para el comprador o el adquirente.
- Ni el vendedor ni el comprador mantienen recibos innegables para la transacción.

2KP

En adición al adquirente, cada vendedor necesita poseer una par de llave pública y es requerido para distribuir la llave pública contenida en su certificado CERT para comprador y adquirente. Este permite al comprador y al adquirente verificar la autenticidad del vendedor. Hay tres elementos en la factura:

1. El vendedor genera un número aleatorio W y crea un compendio del mensaje H(W). El agrega H(W) al Clear (Common también contiene H(W)). La inclusión de W en Confirmación más tarde actúa como un recibo de prueba para el comprador de que el vendedor ha aceptado la respuesta de autorización.
2. El vendedor usa su llave secreta(Kpr_V) para firmar H(Common) y H(W) para producir Sig_V.
3. El vendedor también incluye su certificado de llave pública $CERT_V$ así que el comprador puede verificar la firma Sig_V.

Actor	Datos de Información
Comprador	DESC, CAN, Kpu[illegible], $CERT_A$
Vendedor	DESC, Kpu[illegible], [illegible], Kpr[illegible], $CERT_V$
Adquirente	Kpu[illegible], Kpr[illegible], [illegible]

Al recibir la Factura el Comprador verifica la firma del vendedor Sig_V y genera un flujo de mensaje de pago como antes. El vendedor añade la misma firma Sig_V que él envía al comprador como también su certificado de llave pública $CERT_V$ para la Auto Solicitud. El adquirente verifica la firma del vendedor antes de autorizar la

transacción. Finalmente, el valor de W es enviado en Confirmación al comprador, quién en turno computa H(W) y verifica que éste se parezca al valor la factura.

- El comprador y el adquirente pueden verificar la autenticidad del vendedor debido a la inclusión de la firma del vendedor SIG_V y $CERT_V$
- El vendedor genera un número aleatorio W e incluye un resumen del mensaje del número H(W) en Common. El también firma el par H(W) y H (Common) para formar SIG_V. La firma y H(Common) son verificados por comprador y adquirente. El adquirente también firma H(Common) en SIG_A. Cuando el comprador recibe W como parte del flujo del mensaje de confirmación, el es capaz de verificar que H(W) contiene en SIG_V y SIG_A comparándolo con el H(W) que ha sido computado. También, ninguna otra parte es capaz de encontrar W, ya que esto involucraría invertir una fuerte función one way.

3KP

En suma al 2KP, en 3KP, todas las partes poseen pares de llave pública y sus certificados correspondientes. Permite la no repudiación de todos los protocolos de intercambio. El protocolo es modificado para que el comprador envíe un certificado al vendedor, quien lo dirigirá al adquirente.

El comprador ahora envía su certificado de llave pública al vendedor como parte del mensaje inicial. Como parte del pago, el comprador envía su firma Sig_C al vendedor, donde Sig_C es computada encriptando EncSlip y H(Common) El vendedor es capaz de verificar la firma del comprador, como el ya posee el certificado del comprador $CERT_C$. El vendedor dirige Sig_C como parte de la Auto Solicitud al adquirente, quien verifica la firma en turno.

La firma del comprador provee innegable prueba de la autorización de la transacción para el comprador. Puede ser verificado por el vendedor y el adquirente

La seguridad de este protocolo depende del número de entidades que posean su par de llaves públicas.

Actor	Datos de Información
Comprador	DESC, CAN, Kpu_{AC}, Kpr_C, $CERT_C$
Vendedor	DESC, Kpu_{AC}, $CERT_A$, Kpr_V, $CERT_V$
Adquirente	Kpu_{AC}, Kpr_A, $CERT_A$

Estas son algunas de las características del diseño protocolar:

Verificación de Confirmación

El propósito de H(W) en el campo Clear de Factura, y de W en Confirmación es unir los mensajes a cada uno. W asegura al comprador (y a cualquier tercera parte) que el vendedor es consciente de la autorización del adquirente y se compromete a la transacción. La combinación de SIG_V y W le dan prueba innegable al comprador del acuerdo con el vendedor para la transacción.

SALT

El propósito de $SALT_C$ es formar una llave para el hash de DESC. El resultado cuantitativo H(DESC, $SALT_C$) se transfiere sobre el canal A ↔ V Si el hash no fuera "sal", un intruso que curiosea en el canal A ↔ V puede montar un ataque de diccionario en H(DESC) desde que DESC es escogido de un intervalo pequeño de bienes/servicios. Sin el conocimiento de $SALT_C$, los ataques de diccionario son computacionalmente duros

$SALT_C$ debe, ser guardado en secreto. Sin embargo, se envía en el clear del flujo Inicio, para que V pueda incluirlo en Common. Así, si el canal C ↔ V no es protegido para confidencialidad, un intruso puede obtener $SALT_C$ de allí y entonces montar un ataque de diccionario en la sal de los hash. No obstante, éste es un ataque

más duro, y se espera que el canal C ↔ V sea protegido, ej., a través del uso de SSL, SHTTP, o una IP segura.

Tolerancia de la falta y Manejo de la Excepción

En cualquier ambiente de comunicación (Internet, etc.) la fiabilidad absoluta es imposible. Por consiguiente, para diseñar, asegurar, robustecer, protocolos de pago, debemos considerar las posibles anomalías.

Es supuesto que todas las partes en iKP (excepto el adquirente) implementan interrupciones y retransmisiones siempre que un mensaje no saque ninguna contestación.

Todos los mensajes inesperados, es decir, aquellos que no corresponden a un pendiente o registro de transacción, se ignoran. Todos los mensajes inválidos (ej., adquirente que recibe Inicio) son semejantes a ignorados.

El término "duplicado" se usa debajo para decir que el mensaje es por otra parte válido. También, el término "no solicitado" se usa para decir que el mensaje es por otra parte válido, es decir, todos contienen firmas comprobables.

Se asume que todas las partes tienen acceso al almacenamiento no-volátil. El término "grabando" se usa para significar compromiso al almacenamiento estable.

Excepciones del Comprador

Nota: El comprador no firma sus mensajes de error.

1) Ninguna contestación para Inicio. El comprador se rinde y persigue después de la contestación.

2) Mensaje de error del vendedor (Los mensajes de error del vendedor opcionalmente son firmados.)

   a. Mensaje de Error firmado: El comprador verifica la firma. Si es inválida, el mensaje se desecha. Por otra parte la transacción se detiene y se registra.
   b. Mensaje de Error sin firmar: Grabe el mensaje y acuda a medios fuera de línea.

3) Mensaje de error del adquirente (Se firman todos los mensajes de error del adquirente.) Primero, el comprador checa la firma del adquirente. Si es inválida, el mensaje se desecha. Por otra parte, la transacción se detiene y el mensaje de error se graba con otro estado de transacción. Nota que el usuario actual quizá necesita ser notificado en este punto.

4) Ninguna contestación al Pago. El comprador renuncia después al registro de Pago, Inicio, Factura y R_C.

5) Confirmación Inválida. Esto puede pasar si cualquiera de Y/N, SIG_A, o SIG_V (si se llevó a cabo) son inválidos, o W(se usó) no es igual H(W) de la Factura. El comprador puede retransmitir cualquier Pago inmediatamente o esperar la pausa antes de hacerlo. Es más, puede ser una idea buena para generar un mensaje de error.

6) Factura duplicada. Descartada.

7) Confirmación duplicada. Descartada.

8) Factura inválida. Si la firma del vendedor (optativa) es inválida, Inicio se retransmite. Si H(DESC,$SALT_C$) no es igual a su contraparte dentro de Common, error, el mensaje se envía e Inicio se retransmite. Si CID es inválido dentro de Common, el mensaje de error se envía e Inicio se retransmite.

Excepciones del vendedor

(Es supuesto que el vendedor es quien siempre tienen capacidad de firma, firma mensajes de error.)

1) Inicio Inválido (Ésta probablemente no es una condición de error real.)

2) Pago inválido. Esto puede ocurrir si la Factura es inválida o expirada. En cualquier caso, el mensaje de error se envía de regreso. (el vendedor puede contestar incluso con una nueva Factura.)

3) Ninguna contestación para Auto Solicitud. El vendedor notifica al comprador (vía el mensaje de error especial) que el adquirente es actualmente inalcanzable. IMPORTANTE: vendedor y comprador deben retener este mensaje de error; puede usarse más tarde en disputas para mostrar que era del vendedor, en ese momento, es incapaz de procesar el pago.

4) Auto Respuesta inválida. Si la firma del adquirente es inválida, se desecha.

5) Mensaje de error del adquirente. La firma del adquirente se verifica y el mensaje de error se remite al comprador.

6) Mensaje de error del comprador. TBA

7) Inicio Duplicado. Retransmite Factura.

8) Pago Duplicado. Si la Auto Solicitud correspondiente esta pendiente, ignórala. Alternativamente, un mensaje de error especial puede ser regresado con un mensaje de que "la transacción esta pendiente." Si la Auto Respuesta es recibida, reenvía la Confirmación

9) Auto Respuesta duplicada. Descartada/ignorada.

Excepciones del Adquirente

Nota: El adquirente firma todos sus mensajes de error y descarta/ignora todos los mensajes de error que recibe. También, si el PIN del comprador o CAN son incorrectos, el adquirente recibirá una respuesta negativa de la red de aclaramiento. Esto es considerado "el negocio usual", es decir, no una condición de excepción/error. (El Adquirente simplemente contesta al vendedor con un código negativo auto en Confirmación)

1) Auto Solicitud inválida. Nota "intersección" entre (e) y (c).

   a La firma del Vendedor (si se presenta) inválida
   b La firma del Comprador (si se presenta) inválida
   c El hash de Common dentro del SLIP su colega no es igual a su contraparte en Auto Solicitud
   d Expirado Common (pero no duplicado)
   e El inválido SLIP, es decir, la desencripción falla (ej., por razones de integridad)
   f CID de Common no es igual a CAN,R_C de SLIP
   g Repetir Common (esto es diferente de la Auto Solicitud duplicada; quizá pase si el comprador intenta reusar un Common ya procesado; el adquirente descubre esto verificando [DATE,ID_v,TID_v])

   En todos estos casos, un mensaje de error con un código apropiado se envía al vendedor El estado de la transacción se graba entonces para la posteridad.

2) Auto Solicitud duplicada. Si la transacción todavía está pendiente, ignora o envía un mensaje de error al vendedor. Por otra parte, reenvía la apropiada Auto Respuesta (o mensaje de error si la Auto Solicitud original resultara con la condición de error.)

3) Ninguna contestación de la red de aclaramiento (interrupción). Una posibilidad es enviarle un mensaje de error especial al vendedor. TBA

Mensajes de error

Todos los mensajes de error tienen el formato siguiente:

```
V= (error_code, in_msg, other_info)
```

donde: Z es $\{_A, v, c\}$, el error_code es auto explicativo, in_msg es el mensaje entrante que producirá el error, other_info es la información optativa que lo acompaña

Encripción en iKP

El uso de encripción en iKP se limita a proteger el PIN del comprador y su número de cuenta (CAN). Todos los protocolos requieren que el comprador encripte el SLIP como parte del flujo del mensaje de Pago.

E_A denota encripción RSA con integridad bajo Kpu_A la llave pública del adquirente. El tamaño del módulo de Kpu_A se asume que es por lo menos de 1024 bits. El formato de TXT para ser encriptado es:

```
TXT = [V .., $$, H(COMMON), CAN, R , PIN, SALT]
       \_ _ _ _ _ SLIP _ _ _ _ _ /
```

Dato	Descripción
V_{NO}	Versión Protocolar, 32 bits, (Nota que V_{NO} puede moverse fácilmente fuera de la parte encriptada; no hay ninguna razón particular debe estar aquí.)
$$	64 bits
CAN	0-128 bits; (pueden usarse 128 bits para poner en código a 38 dígitos decimales; las tarjetas de crédito actuales son sólo de 12 dígitos
PIN	0-64 bits (19 dígitos decimales)
H(COMMON)	128 bits
R:	Por lo menos 128 bits
SALT	Al azar, por lo menos 64 bits, su longitud máxima es la diferencia entre 896 bits y la suma (en bits) de todos los campos anteriores.

Todos los componentes anteriores se ponen en código de una cadena TXT de longitud de 896 bits.

Se encripta:

```
1) Agrega 64 bits de ceros a TXT para formar x [0^(64),TXT]      [x es de 960 bits de
   longitud.]
2) Genera aleatoriamente la cadena de 64-bit E .:
3) Computa a = x XOR H: (E.:) y entonces pone b = E.: XOR H '.'  H 1 () es una salida de
   función de hash de 960 bits y H .: .: una salida de una función hash de 64 bits.
4) Computa E.: (a,b, la longitud de a,b e 1.24 bits.
```

Se desencripta:

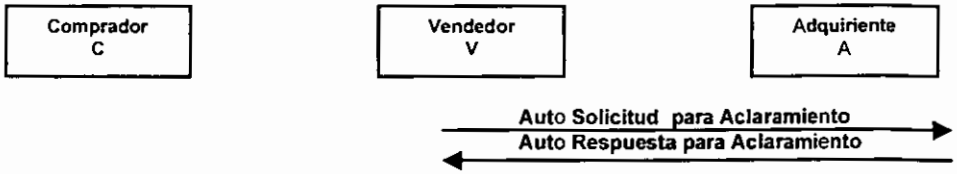
```
1)  Computa ..  E  .,b,  .,b
2)  Computa E.:     E X'R H ..:
3)  Computa x    a XOR H:(E.:)
4)  Verifica la existencia de 64 que llevan 0 s en x y obtiene TXT.

➢   H (DATA     primero 64 bits de salida de H(DATA)
➢   H:(DATA,    primero 960 bits de la secuencia H(Inicio,0,DATA),
     H(Inicio,1,DATA),H(Inicio,2,DATA) donde Inicio es una constante.
```

Autorización contra Aclaramiento

Los sistemas de pago con tarjeta difieren entre "autorización" y "aclaramiento" de pagos.

- Autorización: confirma que un pago dado no eleve la deuda del poseedor de la cuenta sobre su límite de crédito, y reserva la cantidad especificada de crédito.
- Aclaramiento: carga la cantidad a la cuenta de crédito. Puede pasar simultáneamente con autorización, o como un paso después de la autorización.

iKP provee la autorización y si queremos cubrir el aclaramiento se va a involucrar un intercambio de mensajes entre el vendedor y adquirente.



Se necesitan los siguientes cambios al protocolo básico:

- El mensaje de Auto Solicitud debe incluir un campo que indica si el vendedor sólo pide autorización, o autorización y aclaramiento del pago.
- El campo de Y/N en Auto Respuesta y Confirmación debe indicar si el pago sólo es autorizado, o ambos autorizado y aclarado.
- Para aclarar un (autorización previa) pago, Auto Solicitud original, el mensaje es retransmitido por el vendedor al adquirente con el nuevo campo para pedir la solicitud de aclaramiento. El adquirente envía Auto Respuesta al vendedor que indica si el pago fue aclarado con éxito. No hay Confirmación del mensaje desde que el comprador no participa en las transacciones de aclaramiento.

Reembolsos: Los sistemas de tarjeta de crédito soportan el concepto de reembolsos. El comprador le devuelve mercancía al vendedor junto con el ticket original de la tarjeta de crédito. El vendedor emite un ticket del reembolso completo o de una parte de la cantidad de pago original, para ser acreditada a la cuenta de tarjeta de crédito del comprador. Si el vendedor puede firmar, para procesar un reembolso, comprador y vendedor corren iKP usando una cantidad negativa, acreditando eficazmente en lugar del cargo del dinero a la cuenta del comprador. Esto puede repetirse muchas veces si el comprador regresa partes de una orden en múltiples transacciones de reembolso.

Como una opción, el vendedor y adquirente quizá requieran el mensaje Confirmación de una compra asociada al reembolso. Esto permite al vendedor y al adquirente validar el reembolso contra la cantidad original de la compra. Permite al vendedor verificar la transacción de la compra original y descubre que el total de varios reembolsos son más que la compra original.

Consulta del Estado de la Orden: Dada la distinción entre la autorización y el aclaramiento, los compradores quizá quieran un método para averiguar si un pago se ha aclarado. Existen muchos tipos de consultas de estados de la orden.

Aclaración de Pagos en Internet: Uno de los requerimientos fundamentales de iKP, es la necesidad de interactuar con una red financiera de aclaramiento separada a través de entidades llamadas adquirentes o gateways del adquirente. Mientras esta asunción puede permanecer válida por algunos años, el aclaramiento de pagos, sólo se requiere en algún momento. En este caso, iKP necesitaría ser capaz de permitir comunicación directa con el banco emisor (comprador) o la institución financiera

Consideraciones de seguridad: iKP intenta direccionar la seguridad involucrando a una tercera parte en el mecanismo de pago en Internet. iKP no direcciona la seguridad relativa a las negociaciones que pueden ocurrir antes de iKP. Dependiendo del método usado en las comunicaciones, los protocolos de seguridad como SSL, SHTTP, PEM, o MOSS deben utilizarse si la privacidad, autenticación, firmas, u otros atributos de seguridad son requeridos para las transacciones. Los mecanismos de firma con llave pública son extremadamente dependientes de la seguridad de las llaves privadas correspondientes. iKP requiere llaves privada y pública del adquirente, opcionalmente de vendedores y compradores. Los implantadores deben prestar atención particular en los métodos usados para almacenar las llaves privadas de estos participantes. La encripción del almacenamiento de las llaves privadas, hardware a prueba de trampas, mecanismos de revocación de certificados, y fechas de expiración de certificados deben ser considerados. iKP espera que las llaves públicas sean distribuidas vía certificados firmados por una autoridad de certificación reconocida (ACs). La definición de las AC, y el mecanismo de la distribución de las llaves públicas raíz, esta fuera del alcance de iKP. La seguridad de iKP confía finalmente en la seguridad de la raíz de llaves utilizada por el comprador, vendedor, y el software del adquirente.

Procedimiento de Compra por Internet (iKP)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
1.	**Obtención de un certificado**	**adquirente**									
.1	Obtiene un certificado.										
.2	Pública el certificado.										
2.	**Obtención de llaves y certificados**	**comprador vendedor**									
.1	Obtención de la llave pública de la AC.										
.2	Obtención del certificado del Adquirente										
3.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
4.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
5.	**Alta de dirección e-mail de un comprador**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
6.	**Ingreso de dirección e-mail del comprador**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
7.	**Ingresa sus datos el comprador**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
8.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados.				5	*					
9.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envie el producto.				5	*					
10.	**Muestra datos del comprador y del artículo**	**vendedor**									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envio.				5	*			*		
11.	**Asignación de una cantidad del artículo**	**comprador**									
.1	Asigna una cantidad de compra.				5	*				*	
12.	**Señalización de las formas de envío**	**vendedor**									
.1	Da las diferentes formas de envio y una breve descripción (Nacional/Internacional)				5	*		*			
13.	**Elección de forma de envío**	**comprador**									
.1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
14.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación.				5	*					
.2	Menciona los procesos de pago.					*		*			
15.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación.				30	*	*				
.2	Selecciona el método de pago.				5	*				*	
16.	**Envía datos de identificación, de pago y de la orden de compra**	**comprador**									
.1	Envía su identificación, los datos del pago y de la orden de compra al vendedor.										
17.	**Compone Factura**	**vendedor**									
.1	Recupera los datos.										
.2	Asigna un número a la transacción.										
.3	Envía la factura al comprador.										
18.	**Procesando la Factura**	**comprador**									
.1	Obtiene datos de la factura.										
.2	Genera un Slip.										
.3	Envía el Slip encriptado al vendedor.										
19.	**Proceso de Pago**	**vendedor**									
.1	Genera la autorización y la auto solicitud.										
.2	Envía la auto solicitud al adquirente.										
20.	**Proceso de Auto solicitud**	**adquirente**									
.1	Extrae datos de la auto solicitud.										
.2	Verifica que comprador y vendedor estén de acuerdo con la información del pedido.										
.3	Contacta al emisor.										
21.	**Autorización del pago**	**emisor**									
.1	Liquidación de la transacción.										
.2	Envía respuesta al adquirente de transacción completa.										
22.	**Envía respuesta de éxito de la transacción**	**adquirente**									
.1	Envía respuesta al vendedor firmada.										
.2	Al recibir respuesta del adquirente la envía al comprador	**vendedor**									
23.	**Envío del producto**	**vendedor**									
.1	Envía el producto.		25					*	*		
24.	**Recepción del producto**	**comprador**									
.1	Recibe el producto.		700			*					

3.1.9 SEPP (Secure Electronic Payment Transaction Protocol / Protocolo de Transacciones de Pago Electrónico Seguras)

Desarrollado por MasterCard en Octubre de 1995, para asegurar el procesamiento de pago usado para las transacciones de tarjeta del banco sobre redes públicas y basado en 3KP. Los vendedores están capacitados para verificar que el tarjetahabiente éste usando un número de cuenta válido. Provee mecanismos para prevenir fraudes desde un vendedor legítimo y para obtener datos de las tarjetas de crédito. Define un sistema de administración de certificados para controlar los servicios de seguridad soportados por los certificados.

SEPP es equivalente al ticket de cargo, firma y proceso de envío. Asume que comprador y vendedor ya han negociado el precio de los bienes de compra. Toma la entrada del proceso de negociación (cantidad a pagar, descripción del pedido, método de pago, etc.) y las causas de pago para pasar por las tres vías de comunicación entre el tarjetahabiente, el comerciante y el adquirente.

Arquitectura del sistema:

Entidades

- Tarjetahabiente: Un autorizado tenedor de una tarjeta de banco, emitida por un emisor quien es registrado para llevar a cabo el comercio electrónico.
- Vendedor: Un vendedor de bienes o servicios, quien acepta pagos de manera electrónica.
- Adquirente: Una institución financiera registrada que soporta vendedores y proveedores de servicio para procesar transacciones con tarjetas de crédito. El adquirente consiste en un gateway del adquirente y una autoridad de registro del vendedor. El gateway del adquirente sirve como interfaz para que el sistema del vendedor soporte autorizaciones y capturas de servicio para vendedores. La autoridad de registro del vendedor (MRA), capacita al adquirente para asegurar la recepción, validar, y enviar la solicitud de certificado del vendedor, es el sistema administrador de certificados y recibe de regreso los certificados.
- Sistema Administrador de Certificados (CMS): Un agente de una o más asociaciones de tarjetas bancarias que proveen la creación y distribución de certificados electrónicos para vendedores, adquirentes y tarjetahabientes. El CMS consiste de una o más autoridades certificadoras para proveer confianza, un servicio que te garantice, un servicio confiable para los tarjetahabientes, vendedores y adquirentes. También contiene la solicitud de certificados de los servidores que emiten certificados para tarjetahabientes a través de WWW e interfaces MRA del adquirente para proveer certificados a los vendedores.

Sistema Administrador de Certificados

El CMS es implementado como una jerarquía de servidores, con soportes criptográficos. Un certificado es usado para firmar la llave pública de un usuario para informar su identificación.

1. Un certificado del tarjetahabiente, firma la llave pública de un certificado de un tenedor, para especificar un número de cuenta y asegurar que el vendedor tiene un número de cuenta legítimo que se provee en la transacción. Para proteger la privacidad del tarjetahabiente, se aplica una función hash al número de cuenta especificado en el certificado de llave pública del tarjetahabiente. El tarjetahabiente pasa su número de cuenta y una variable secreta llamada código de certificado para un adquirente, así que el adquirente puede verificar el valor del hash contenido dentro del certificado del tarjetahabiente.
2. El certificado del vendedor asegura al tarjetahabiente que él es un legítimo vendedor MasterCard.
3. La llave pública dentro del certificado del adquirente es usada por el tarjetahabiente para encriptar la instrucción de pago, la cual incluye el número de cuenta.

Existen los siguientes pares de llaves

- Llaves del tarjetahabiente: Un tarjetahabiente requiere dos pares de llaves para crear su firma digital durante la transacción de pago. La llave privada es almacenada localmente en el disco y encriptada usando un password conocido sólo por el tarjetahabiente. Las llaves pública y privada son generadas localmente por un dispositivo o software criptográfico.
- Llaves del vendedor: También tiene de uno a dos pares de llaves. Un par es requerido para crear firmas digitales y el otro es opcional usado para encriptar los datos del pago enviados del vendedor al adquirente.
- Las llaves del adquirente: Tres pares de llaves son requeridos por el gateway del adquirente. El primer par es usado para la firma digital de recepción provista para el tarjetahabiente y vendedor, el segundo es usado para la encripción y decripción de los datos de pago recibidos desde el tarjetahabiente, y el último es para firmar solicitudes de renovación de certificados para ser enviados al CMS.

Las partes públicas deben certificar sus llaves por la CMS.

Proceso de Pago

SEPP asume que tarjetahabiente y vendedor se han comunicado para negociar los términos de la compra y generar un pedido. Este protocolo puede ser usado en modo interactivo (WWW) y no interactivo (catálogo en CD). En modo no interactivo, los detalles de la transacción pueden ser enviados vía correo electrónico.

a) Orden de compra con autorización en línea.

1. En mensajes de modo interactivo, una transacción SEPP inicia cuando el tarjetahabiente envía un mensaje de Inicio al vendedor. Se usa para solicitar al vendedor que prepare una factura como el primer paso en el proceso de pago.

2. El vendedor responde un mensaje Factura, que contiene la cantidad de la transacción, información de identificación del vendedor, y datos usados para validar las transacciones subsecuentes en el proceso.

3. El tarjetahabiente responde enviando una Solicitud de Orden de Compra. Contiene la instrucción de pago (PI) del tarjetahabiente. El PI es encriptado de manera que sólo pueda ser leído por el adquirente.

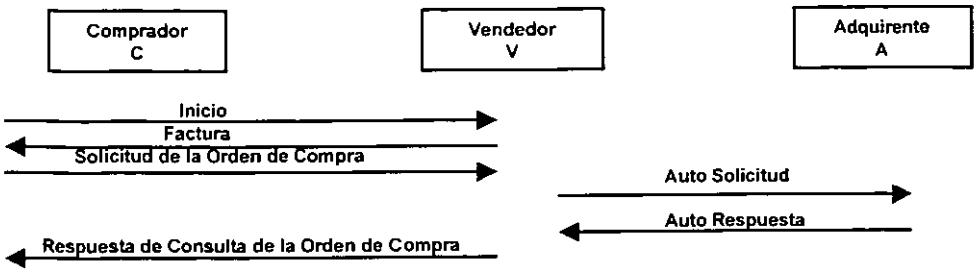
4. El vendedor entonces envía la Auto Solicitud al adquirente.

5 El adquirente lleva a cabo lo siguiente:

   - Auténtica al vendedor;
   - Decripta el PI desde el tarjetahabiente;
   - Válida que el certificado del tarjetahabiente contenga el número de cuenta usado en la compra;
   - Válida la consistencia entre la autorización de la solicitud del vendedor y los datos de pago del tarjetahabiente;
   - Formatea una solicitud de autorización estándar al emisor y recibe una respuesta;
   - Responde al vendedor con una válida Auto Respuesta

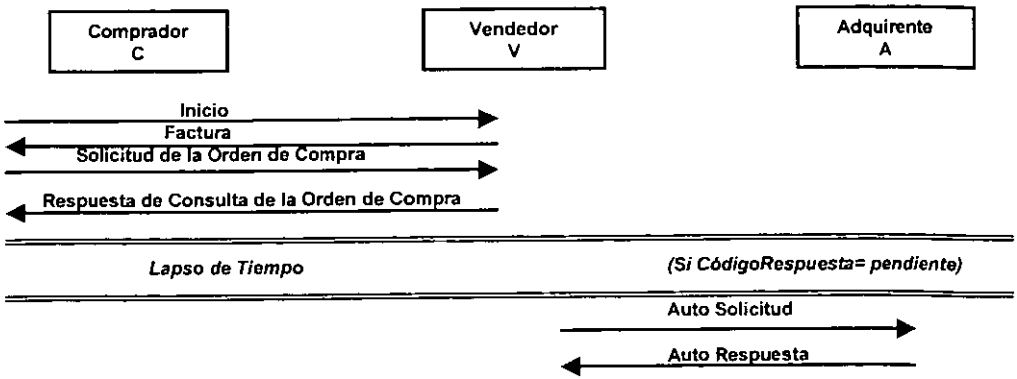
6 El vendedor responde con una Respuesta de la orden de compra indicando que también el vendedor ha recibido la solicitud de la orden de compra y la autonzación de la solicitud será procesada más tarde, o la autorización de la respuesta ha sido procesada por el adquirente.

El tarjetahabiente puede entonces solicitar el estado de la orden de compra usando un mensaje Consulta de la orden de compra. El vendedor responde con un mensaje Respuesta de consulta de la orden de compra.



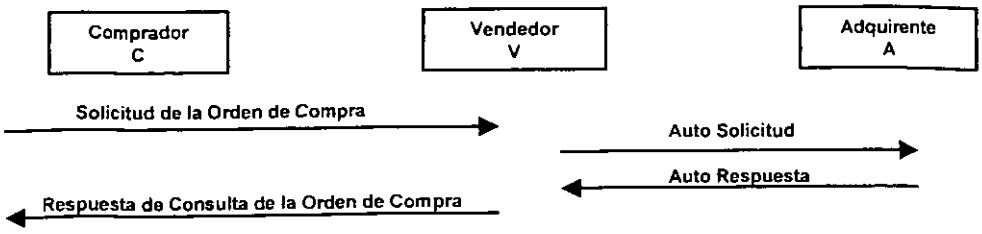
b) Orden de compra con autorización de retraso.

El vendedor escoge un autorización de retraso hasta después de enviar una respuesta al tarjetahabiente. El mensaje final para el comprador es una Respuesta de consulta de la orden de compra, en vez de una Respuesta de la orden de compra, porque el vendedor no ha completado la autorización. La Auto Respuesta y la Auto Solicitud siguen el mismo flujo que el paso previo.



c) Orden de compra fuera de linea

En el caso de transacciones de correo electrónico, el primer mensaje desde el tarjetahabiente, es una Respuesta de la orden de compra. La Respuesta de la orden de compra del vendedor la envía de regreso vía e-mail al tarjetahabiente. Los mensajes Inicio y Factura son omitidos

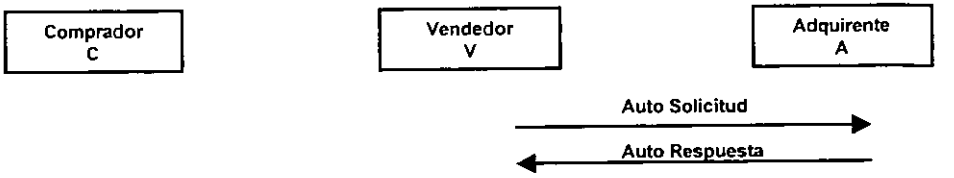


d) Captura

El vendedor usa este flujo para solicitar al sistema de aclaración de tarjeta de crédito la transferencia de fondos del tarjetahabiente al vendedor. Este puede ocurrir después de que el flujo de autonzación ha sido completado y si la orden de compra no fue capturada en el flujo de autorización. El vendedor debe enviar la Solicitud de Captura al mismo adquirente al cual se le envío el mensaje de Auto Solicitud.

Existen 3 modos de captura:

1) Captura en línea combinada con autorización. El vendedor quizá solicite que el pago sea capturado por el adquirente en el tiempo en el que la autorización es obtenida.
2) Captura en línea diferida. El vendedor quizá solicite la captura de pago de manera separada desde y subsecuente a la autorización.
3) Captura fuera de línea. El vendedor quizá obtenga el pago a través de mecanismos que no involucra SEPP.



e) Solicitud de orden de compra.

f) Error.

Requerimientos de seguridad

Tajetahabiente:

- Los pagos no autorizados son imposibles y no pueden ser cargados a una cuenta de un tarjetahabiente, sin tener un número de cuenta del tarjetahabiente y una llave privada.
- Un tarjetahabiente puede verificar la autenticidad/confiabilidad de un vendedor.
- Recibe una prueba irrefutable de una autorización de la transacción desde el adquirente.
- Obtiene un recibo desde el vendedor que da pruebas de no repudio, de que él recibió la autorización de pago

Vendedor

- Recibe una prueba innegable de que el adquirente ha autorizado la transacción.
- Recibe una prueba innegable de que el tarjetahabiente ha autorizado la transacción.

Adquirente

- Recibe una prueba innegable de autorización de la transacción por el tarjetahabiente, antes de que su cuenta haya sido debitada.
- Recibe una prueba innegable de autorización de la transacción por el vendedor. Es imposible autorizar la transacción de pago sin la autorización del vendedor

Procedimiento de Compra por Internet (SEPP)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
1.	**Obtención de Certificados y de llaves**	**comprador vendedor adquirente**									
.1	Obtienen sus certificados.										
.2	Obtienen sus pares de llaves para firmar y encriptar.										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un comprador**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del comprador**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el comprador**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados				5	*					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
9.	**Muestra datos del comprador y del artículo**	**vendedor**									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
.1	Asigna una cantidad de compra.				5	*				*	
11.	**Señalización de las formas de envío**	**vendedor**									
.1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)				5	*		*			
12.	**Elección de forma de envío**	**comprador**									
.1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación.				5	*					
.2	Menciona los procesos de pago.					*		*			

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
14.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación.				30	*	*				
.2	Selecciona el método de pago.				5	*				*	
.3	Ingresa los datos que se requieren de la forma de pago elegida			5		*				*	
15.	**Envía datos de pago**	**comprador**									
.1	Envia información del pago e información referente al comprador.										
16.	**Envío de Factura**	**vendedor**									
.1	Envía una factura con datos referentes al importe de la compra, información de identificación del vendedor, entre otros datos.										
17.	**Solicitud de la orden de compra**	**comprador**									
.1	Envío de la solicitud de la orden de compra donde contiene la instrucción de pago, éste es encriptado.					*			*		
18.	**Envía la solicitud al adquirente**	**vendedor**									
.1	Envia los datos que le envio el comprador.										
19.	**Proceso de autorización**	**adquirente**									
.1	Auténtica al vendedor.										
.2	Decripta la información del comprador.										
.3	Válida el certificado del comprador, los datos de pago y la autorización del vendedor de la solicitud										
.4	Realiza una solicitud de autorización hacia el emisor.										
19.	**Contestación de la autorización**										
.1	Envía la respuesta de la autorización de la solicitud al adquirente.	**emisor**									
.2	Envia la respuesta anterior al vendedor	**adquirente**									
.3	Envía la respuesta de autorización de la orden al comprador.	**vendedor**									
20.	**Corroboración de la solicitud de la orden de compra**	**comprador**									
.1	Solicita una consulta de la orden de compra										
21.	**Envío de la consulta de la orden de compra**	**vendedor**									
.1	Envia la consulta al comprador.										
22.	**Envío del producto**	**vendedor**									
.1	Envía el producto.		25					*	*		
23.	**Recepción del producto**	**comprador**									
.1	Recibe el producto.		700			*					

3.1.10 OpenMarket

OpenMarket, Inc , fue fundado en 1994. Maneja transacciones de tarjeta de crédito vía servidores Web, pero estaba planeándose el soporte para tarjetas de débito, cuentas de cheques y ordenes de compra corporativas. Usa passwords y, opcionalmente, dos tipos de dispositivos para generación de respuestas: NetKey segura y criptografía ID Shared-key. Ofrecerá servidores seguros a los vendedores que soporten S-HTTP y SSL.

Es un sistema administrador de transacciones pero vende lo que se le llama Proveedor de Servicios de Comercio (CSPs / Commerce Service Providers, pueden ser los bancos en Internet), es un servicio en línea, como CyberCash. Es completamente independiente del browser y del contenido del servidor.

Como servidor el comprador navega y elige el artículo a adquirir y elige el botón "Buy One Now (Comprar uno ahora)", pero para un vendedor que usa un equipo OMI el botón "Buy One Now" es una liga que une una oferta digital (OD) con la porción de consulta del URL, el resto de la URL es direccionado al CSP favorito del vendedor, éste es el operador del servicio de transacción OMI. Cuando el browser ejecuta la redirección a ese servicio, un programa CGI está esperando a cuidar la transacción de pago tal como lo hace Cybercash (con tarjeta de crédito e incrementa una variedad de otros mecanismos de pago). Mientras que el vendedor se conecta al CSP en un estado de espera, el CSP tratará de hacer que el pago sea enviado con la solicitud apropiada en la red financiera convencional y maneje los valores de regreso en la red.

Asumiendo que el dinero está disponible, la transferencia de dinero entre el pago del comprador y la aceptación del vendedor se llevan a cabo. El CSP redirecciona al comprador al vendedor original, pero con un nuevo cargo de pago en el componente de la consulta de la URL. Este componente es un recibo digital (RD) indicando al vendedor que el comprador ha pagado y ahora el vendedor puede entregar los bienes.

3.1.9 SET (Secure Electronic Transactions/Transacciones Electrónicas Seguras)

Fue lanzado por la alianza de MasterCard, Netscape Corporation, IBM, y otras compañías, en enero de 1996 SET usa un sistema de pago que es análogo al pago tradicional de tarjetas

SET ofrece a los compradores la mayor seguridad disponible en el mercado comercial. En vez de proveer a los vendedores con acceso a los números de tarjetas de crédito, SET codifica los numeros, así sólo el consumidor y la institución bancaria pueden retener certificados SET que los identifican y llaves públicas asociadas con sus identidades digitales. Al tiempo de la compra, cada parte del software SET válida a ambos, comprador (tarjetahabiente) y vendedor antes de que la información sea intercambiada. La validación tiene lugar verificando los certificados digitales que fueron emitidos por la autorización de la tercera parte.

Es una combinación de un protocolo a nivel de aplicación y procedimientos recomendados para manejo de transacciones con tarjeta de crédito sobre Internet. Diseñado para tarjetahabientes, vendedores y bancos (y otros procesadores de tarjetas), SET cubre la certificación de todas las partes involucradas en una compra, como la encripción y los procedimientos de autenticación.

La siguiente lista describe las funciones de la especificación.

- Proveer información de pago confidencial, y hacer posible la confidencialidad de ordenar la información que es transmitida con la información de pagos.
- Asegurar la integridad para todos los datos transmitidos.
- Proveer autenticación de que un comprador es un usuario legítimo de una marca de tarjeta bancaria (ej Visa, MasterCard, American Express.)
- Proveer la autenticación de que un vendedor puede aceptar un pago con tarjeta bancaria, a través de su relación con una institución financiera apropiada
- Asegurar el uso de las mejores prácticas de seguridad y técnicas de diseño, para proteger a todas las partes legítimas en una transacción de comercio electrónico.
- Asegurar la creación de un protocolo que ni es independiente de los mecanismos de seguridad de transporte ni previene su uso
- Facilitar y alentar la interoperabilidad a través del software y proveedores de redes

Los participantes en una transacción de SET son

- Tarjatahabiente Es la persona que usa la tarjeta de crédito para pagar por compra de bienes o servicios
- Vendedor Es el negocio o la organización que vende bienes o servicios al tarjetahabiente.
- Emisor: Es una institución financiera que provee al tarjetahabiente una tarjeta de crédito Su responsabilidad es garantizar el pago en nombre del tarjetahabiente. El proceso del emisor es fuera de banda desde la perspectiva de SET, aunque es todavía parte de la transacción
- Adquirente Es la institución bancaria que procesa la autorización del pago con tarjeta de crédito y el pago al vendedor La responsabilidad del adquirente es obtener autorización del pago desde el emisor del tarjetahabiente
- Gateway de Pago. Es una institución que trabaja en nombre del adquirente para procesar los mensajes de pago del vendedor, incluye instrucciones de pago desde los tarjetahabientes El gateway puentea la comunicación entre SET y las redes de tarjeta de crédito existentes.
- La Autoridad Certificadora (AC) Provee certificación para el vendedor, el tarjetahabiente, y el gateway de pago La certificación significa asegurar que las partes involucradas en una transacción son quienes dicen ser

Transacción de Compra: Obtención de un certificado Antes de que inicie una transacción, cada parte involucrada debe obtener certificados, éstos se basan en el formato de los certificados X 509 Los certificados se usan en el proceso de autenticación

1. El gateway obtiene los certificados que necesite desde la AC
2 El vendedor obtiene su certificado desde la AC.
3 El tarjetahabiente obtiene su certificado desde la AC.

Compra:

4 El tarjetahabiente va de compras a una tienda virtual y decide que bienes y servicios desea comprar
5 El vendedor envía el certificado del tarjetahabiente.
6 El tarjetahabiente envía una solicitud para la compra de los artículos que ha seleccionado. Este mensaje contiene información acerca de la orden del tarjetahabiente e información del pago. El vendedor obtiene la información de la orden, y envía la información del pago con la tarjeta del tarjetahabiente dentro del gateway de pago. El vendedor nunca es privado de la información de pago del tarjetahabiente y por lo tanto no tiene manera de obtener la información del pago. Las medidas de seguridad están diseñadas para proteger al tarjetahabiente
7. El vendedor y el gateway de pago comparten la información de la autorización. Esto consiste en que el vendedor envíe la información al gateway de pago, tal como la información del pago del tarjetahabiente y la cantidad de la transacción. El gateway de pago también puede autorizar o rechazar la transacción basado en la información recibida desde el vendedor. La cantidad autorizada debe ser capturada después por el vendedor, y no hay intercambio de dinero durante la fase de autorización.
8 El vendedor envía un mensaje al tarjetahabiente finalizando la transacción (fin de la transacción para el tarjetahabiente)
9 Este paso es opcional, pero permite al vendedor cambiar o eliminar el dinero autorizado en el paso 7

Captura: Esta fase se da cuando la captura de dinero se ha autorizado en el paso 7. Usualmente la autorización del dinero es capturada por el vendedor

10 El vendedor y el gateway de pago comparten la información de captura. Una solicitud es enviada del vendedor al gateway para capturar el dinero que ha sido autorizado, esta solicitud de captura puede ser para una autorización de una sola cantidad o múltiples cantidades. El gateway procesa la solicitud de captura a través de la red financiera de pago con tarjeta.
11 Si un error ha ocurrido al capturar los fondos del tarjetahabiente, un mensaje entre el vendedor y el gateway toma lugar para dar marcha atrás a la captura. Este paso es opcional y sólo pasa si ha ocurrido un error de captura

Acreditar: Algunas veces un vendedor necesita acreditar la cuenta de un tarjetahabiente.

12 El vendedor y el gateway intercambian mensajes para acreditar la cuenta del tarjetahabiente
13 Si un crédito ha sido garantizado por error, el vendedor y el gateway pueden intercambiar mensajes para dar marcha atrás al crédito otorgado

Procesamiento de Errores SET

SET define una serie de mensajes de error que son usados cuando ocurre un error procesando alguno de los mensajes de SET. El receptor de un mensaje SET genera un error cuando el formato del mensaje es erróneo o el contenido de su verificación. Cuando el mensaje falla, un error es enviado desde el receptor del mensaje al emisor

Este mensaje de error no intenta indicar una falla de un proceso, pero es más bien para indicar una falla en el contenido o la verificación

Existen cuatro categorías de error en SET

- Mensaje de duplicación. Suficiente información aparece en el mensaje envuelto que el receptor puede detectar si un mensaje es una retransmisión o no. Si el mensaje está siendo retransmitido, no está diseñado para ser transmitido más que una vez, el receptor puede genera un error
- Mensajes corruptos. Estos no pueden ser analizados correctamente por el receptor.
- Mensajes mal formados. Pasa cuando el mensaje puede ser analizado, pero es otra manera ilegal debido al hecho de que los valores están fuera del rango esperado.
- Falla en la criptografía. Si en el mensaje recibido falla la prueba de autenticación, un mensaje de error es regresado al emisor

SET Software

Cada uno de los participantes en una transacción SET usa un software que trabaja en su nombre para ejecutar una transacción. Estos son

a) La cartera

Es la aplicación SET del tarjetahabiente. Si un tarjetahabiente desea comprar bienes o servicios desde un vendedor SET, necesita tener una cartera. Esta permite al tarjetahabiente hacer una transacción de pago segura con tarjeta sobre Internet usando SET. El tarjetahabiente recibe un equivalente digital de una tarjeta de pago desde una AC, almacena ésta en su cartera, y la usa para comprar bienes o servicios de los vendedores

La cartera puede trabajar de varias formas, pero la más común es cuando es una aplicación plug-in del browser. El plug-in es un programa que se separa del browser, pero trabaja en conjunto con éste para ejecutar ciertas tareas. La tarjeta ejecuta la tarea de manejar la compra SET del tarjetahabiente.

Esto se empieza a ejecutar una vez que el comprador ha elegido los artículos que desea comprar y apreta el botón de pago, se inicia la cartera.

El corazón de la funcionalidad de la cartera está fuera de las especificaciones de SET, el vendedor es el que decide agregar funcionalidad. Todas las carteras deben ser mínimamente capaces de ejecutar las siguientes funciones:

- Iniciar el proceso de pago con el vendedor.
- Informarse acerca y recibir la información de pago desde el vendedor.
- Informarse acerca y recibir el estado del pago desde el vendedor
- Informarse acerca del estado de una orden
- Aceptar mensajes desde el adquirente de un tarjetahabiente.
- Iniciar una solicitud para los certificados del tarjetahabiente
- Solicitar una forma de registro a una AC y regresarle la forma completada
- Recibir los certificados para el tarjetahabiente
- Informarse acerca del estado de los certificados solicitados

Existen diferentes carteras, que se pueden elegir para el uso de SET, y son

- X-PAY™ Java Credit Wallet
- CyberCash® Internet Wallet
- CommerceSTAGE™ Secure Credit Cardholder
- GlobeSetR Wallet™
- IBM Consumer Wallet
- MicrosoftR Wallet
- WebWallet™
- PayPurse™
- vWALLET™
- NetPay™ Wallet

b) El servidor del vendedor (POS)

El servidor del vendedor, o punto de ventas (POS/ point of sale), es el software SET del vendedor Este no maneja ninguna de la páginas Web que el vendedor usa para ofrecer bienes y servicios. El servidor trabaja junto con las páginas Web existentes; estas páginas deberán ser alteradas para proveer ganchos que trabajen con el servidor del vendedor.

Se dará un ejemplo simplificado de cómo trabajan la suite de software del vendedor y del tarjetahabiente entre sí:

1 El tarjetahabiente navega en la tienda del vendedor En las páginas Web se presenta un catálogo virtual de bienes y servicios que el vendedor ofrece. El tarjetahabiente selecciona los artículos que desea adquirir
2 El tarjetahabiente selecciona el medio de pago de la compra.
3. Al haber obtenido los datos de la compra se le informa al servidor del vendedor los detalles de la transacción.
4. El servidor del vendedor envía un mensaje al tarjetahabiente vía la tienda y el browser Este mensaje es responsabilidad para iniciar la cartera
5 La cartera y el servidor del vendedor procesan la transacción de acuerdo a las reglas de SET, aquí otra entidad se involucra (gateway, el banco del adquirente, etc.), pero éste es el que inicia la actual transacción de SET.

El servidor del vendedor es responsable sólo de manejar los mensajes de SET

El corazón de la funcionalidad del servidor del vendedor está fuera de las especificaciones SET. Todos los servidores deben ser capaces por lo menos de ejecutar las siguientes funciones:

- Responder al mensaje de inicio de la cartera
- Recibir una solicitud de compra desde la cartera del tarjetahabiente, y envía un mensaje de respuesta basada en el resultado de la compra.
- Recibir una consulta desde el tarjetahabiente acerca del estado de una transacción, y regresar un mensaje con la información del estado.
- Recibir una solicitud de registro del tarjetahabiente, y proveer al tarjetahabiente una forma de registro, o una dirección donde puede encontrar tal forma
- Generar una solicitud de certificado para ser enviada a la AC y procesar el mensaje de respuesta
- Enviar un mensaje consulta acerca del estado de un certificado y procesar un mensaje de respuesta
- Generar y enviar un mensaje del adquirente para autorizar la solicitud de compra de un tarjetahabiente y procesar el mensaje de respuesta.
- Generar y enviar un mensaje del adquirente para revocar una previa solicitud de compra autorizada y procesar el mensaje de respuesta
- Generar y enviar un mensaje que maneje procesamiento por lotes con el adquirente, y procese el mensaje de respuesta del adquirente
- Solicita la captura de fondos desde el adquirente y maneja la respuesta del adquirente
- Generar mensajes que soliciten la revocación de fondos previamente capturados, y que maneje el mensaje de respuesta
- Solicitar que el adquirente emita un crédito para el tarjetahabiente y que maneje el mensaje de respuesta del emisor
- Generar un mensaje de solicitud de revocación de un crédito garantizado previamente y maneje el mensaje de respuesta
- Obtener formas de registro desde una AC
- Manejar todos los errores generados por el protocolo SET

Existen diferentes servidores para los vendedores, que se pueden elegir para el uso de SET, y son:

- X-PAY™ Server
- CyberCash® CashRegister
- CommerceSTAGE™ Secure Credit Payment
- GlobeSetR POS™
- IBM Payment Server
- PayWare™
- vPOS™
- NetPay™ Merchant

c) La autoridad certificadora (AC)

Una AC es responsable de emitir certificados digitales, que sirven para identificar y autenticar a los participantes en una transacción SET; por lo tanto las AC son responsables de garantizar que individuos y organizaciones tengan certificados en donde se demuestra, que ellos son quienes dicen ser Las especificaciones SET previenen la intercepción de números de cuenta del tarjetahabiente, fechas de expiración, e información de pago por individuos autorizados a través del uso de métodos de encripción provistos.

La AC garantiza certificados para el tarjetahabiente (cartera), el vendedor (servidor del vendedor), y el banco emisor del vendedor (gateway)

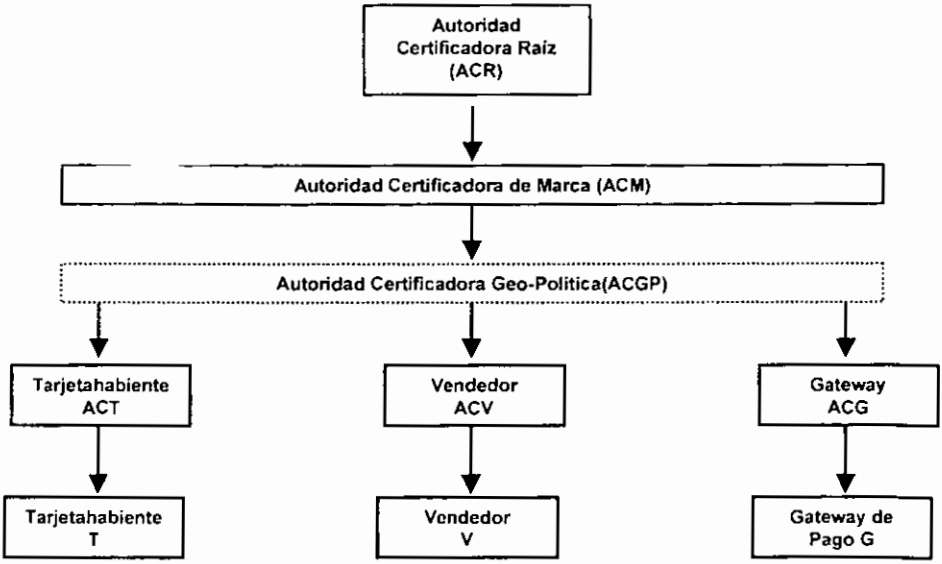
El corazón de la funcionalidad de la AC está fuera de las especificaciones SET Todas las AC deben ser capaces por lo menos de ejecutar las siguientes funciones:

- Recibir, procesar, y responder al mensaje de inicio del certificado del tarjetahabiente
- Recibir, procesar, y responder al mensaje de inicio del certificado de todos los vendedores
- Recibir, procesar, y responder al mensaje de forma de registro de todos los tarjetahabientes.
- Recibir, procesar, y responder a las solicitudes de certificados de los tarjetahabientes y vendedores.
- Recibir, procesar, y responder a las solicitudes de estado de los certificados de los tarjetahabientes y vendedores

Existen diferentes AC, que se pueden elegir para el uso de SET, y son

- Entrust/CommerceCA™
- CyberTrust Certificate Management Systems
- CommerceSTAGE™ Secure Certificate Authority
- GlobeSet CA
- IBM Payment Registry

El protocolo SET define nueve entidades en su arquitectura de administración de certificados



- Autoridad Certificadora Raiz (ACR): Es manejada bajo condiciones físicas de seguridad extrema y es usada solo para crear certificados de nuevas Autoridades Certificadoras de Marcas y de nuevas Autoridades Certificadoras Raiz. Es responsable de distribuir las Listas de Revocación de Certificados (LRC), si un certificado de una AC de Marca ha sido comprometido.

- Autoridad Certificadora de Marca (ACM): Sirven para permitir la marca de una tarjeta de pago para tener el control sobre la creación y distribución de sus certificados. La ACM es similar a la ACR en que se manejan bajo extremas condiciones de seguridad física y son usadas sólo para emitir certificados, Identificadores de LRC de marca (ILM), y LRCs para sus AC subordinadas.

- Autoridad Certificadora Geo-Politica (ACGP): Permite otro nivel de control entre las ACB y sus autoridades certificadoras suboordinadas. Su propósito es permitir el control regional de distribución de certificados por las marcas de tarjeta de crédito. Esta es opcional, sino es usada, los certificados normalmente emitidos por la ACGP serán emitidos por la ACB.

- Autoridad Certificadora del Tarjetahabiente (ACT): Es responsable para generar y distribuir todos los certificados de los tarjetahabientes.

- Autoridad Certificadora del Vendedor (ACV): Es responsable para generar y distribuir todos los certificados de los vendedores.

- Autoridad Certificadora del Gateway (ACG): Emite certificados de lo gateways de SET.

- Certificados del Tarjetahabiente: Son equivalentes digitales de una tarjeta de pago, y son emitidos por la ACT del tarjetahabiente.

- Certificados del Vendedor: Son equivalentes digitales a la marca de una tarjeta de pago, que aparece en la ventana de la tienda del vendedor. Esto significa que el adquirente del vendedor en nombre del vendedor, procesa la transacción del tarjetahabiente cuando una marca de tarjeta es usada.

Diferentes tipos de entidades necesitan diferentes tipos de certificados, éstos son

- Certificados con firmas digitales, contienen la llave de firma pública de la entidad.
- Certificados de encripción de llaves, contienen una copia de un certificado de encripción pública de la entidad
- Certificados de Firmas de Listas de Revocación de Certificados, contienen copias de los certificados públicos de las entidades y las llaves de firmas de LRC.

d) El gateway

El gateway provee una liga entre el servidor del vendedor y el adquirente del vendedor. Esencialmente sirve como puente entre la transacción SET y las redes financieras. Este componente permite a SET trabajar dentro de la infraestructura existente sin hacerle drásticos cambios.

El corazón de la funcionalidad del gateway está fuera de las especificaciones SET. Todos los gateways deben ser capaces por lo menos de ejecutar las siguientes funciones:

- Recibir y procesar mensajes de solicitud de autorización de pago del vendedor, y regresa una respuesta al vendedor
- Recibir y procesar mensajes de solicitud para revocar una cantidad previamente autorizada, y regresa una respuesta
- Recibir y procesar mensajes desde que el vendedor solicita la captura de fondos, y envía un mensaje al vendedor.
- Recibir y procesar mensajes de solicitud para revocar la captura. Un mensaje debe ser regresado cuando el vendedor termine.
- Recibir y procesar mensajes desde el vendedor que solicite un crédito al tarjetahabiente, y regresa un mensaje al vendedor.
- Procesar mensajes de revocación del crédito del vendedor, y regresa un mensaje al vendedor acerca del crédito revocado
- El vendedor quizá asigne un identificador al lote de los artículos de captura, el gateway debe ser capaz de procesar los mensajes pertenecientes a esos lotes, así como regresar un mensaje al vendedor
- Da una lista actualizada de revocación de certificados al vendedor, cuando el vendedor la solicita.
- Obtiene formas de registro desde una AC
- Pregunta por y obtiene certificados desde una AC
- Consulta a una AC acerca del estado de los certificados del gateway, así como acepta un mensaje de regreso de la AC

Existen diferentes gateways, que se pueden elegir para el uso de SET, y son:

- X-PAY™ Server
- CommerceSTAGE™ Secure Payment Gateway
- GlobeSet Gateway™
- IBM Payment Gateway

La estructura de mensajes SET

Este protocolo consiste en pares de mensajes solicitud/respuesta. Para permitir interoperabilidad, los mensajes son definidos en una máquina independientes del formato de la especificación.

La encripción es ejecutada en partes de ciertos mensajes. Es una solución fin a fin que permite que la información contenida con los mensajes sea selectivamente revelada a las partes conforme sea requerida.

Los mensajes necesitan ejecutar una transacción de compra, que usualmente incluye

1. Inicio (PinitReq/PInitRes)
2. Orden de Compra (Preq/PRes)
3. Autorización (AuthReq/AuthRes)
4. Captura de Pago (CapReq/CapRes)
5. Consulta de Tarjetahabiente (InqReq/InqRes), éste es opcional

Analizaremos cada uno de los mensajes, a continuación.

1. Inicio del Pago (PinitReq/PinitRes)

El pago SET inicia después de que el tarjetahabiente ha sido presentado con una forma de orden completada y aprobado su contenido.

El mensaje PinitReq es enviado al vendedor para indicar que el tarjetahabiente está listo para pagar los bienes. Este contiene

- MarcaID. Es la marca de la tarjeta que será usada en el pago, como VISA o MasterCard.
- LID. Un ID local para la transacción.
- Opcional lista de certificados (Thumbs) ya almacenadas en la cartera. Esta lista consiste de un resultado de una función hash SHA de cada certificado sostenido.
- $Chall_c$. Esta variable challenge, será usada en la respuesta del vendedor, para garantizar lo reciente de la comunicación

Al recibir PinitReq, el vendedor genera un ID único y global que es combinado con el LID para formar el ID de la transacción (TransID). Es usado para identificar una compra específica desde otro mensaje de compra recibido.

La respuesta del vendedor contiene el TransID junto con los certificados y la fecha actual. El challenge del tarjetahabiente es incluido junto con un nuevo challenge del vendedor ($Chall_v$). El certificado incluye las llaves que son necesitadas en el pago y que el tarjetahabiente no tiene, tal como las llaves públicas del vendedor y el adquirente.

Desde que el tarjetahabiente ha recibido una respuesta apropiada a su challenge, el puede confiar que el vendedor es acreditado.

2. Orden de Compra (Preq/PRes)

Los mensajes de la orden de compra cumplen con la compra actual por el tarjetahabiente desde el vendedor. El tarjetahabiente envía dos elementos, la información de la orden (OI) y las instrucciones del pago (PI), al vendedor.

- El OI contiene los datos que identifican la descripción del pedido al vendedor.
- El PI contiene los datos actuales de la tarjeta, la cantidad de la compra, y los identificadores de la transacción y de la orden. El PI es encriptado con la llave pública del adquirente así que el vendedor no puede ver su contenido. Este es enviado al adquirente después como parte de la autorización.

La Información de la Orden (OI)

Esta formada por el challenge del vendedor ($Chall_v$), el cual es regresado para demostrar al vendedor lo reciente del mensaje. Odsalt es un nonce usado cuando se aplica el hash de la descripción de la orden, incluyendo este nonce aleatorio dentro del hash, los ataques de diccionario son prevenidos. Esto es, el nonce detiene a un atacante de adivinar el valor hash, H(OIDatos), tratando todas las posibles combinaciones de palabras de diccionario en la descripción de la orden.

Una firma dual se crea usando el valor hash de OIDatosy PIDatos (Datos contenidos en PI). Las ligas de las firmas OIData y PIData, ligan la orden del tarjetahabiente a la autorización de las instrucciones de pago para mostrar que se firmaron juntas. Cualquiera que posea OIData o PIData y la firma dual puede verificar la firma sin necesidad de tener conocimiento de la otra. La firma dual es también una rápida optimización desde que sólo una firma es necesitada en vez de tener firmas separadas para OIData y PIData. La firma del certificado del tarjetahabiente es incluida con la firma para que el vendedor pueda verificarla

Firmas Duales SET

Con ayuda de la firma dual se puede verificar el valor del otro mensaje. El resultado de aplicar un XOR al hash del mensaje 1 con el hash del mensaje 2 es incluido en la firma. La firma puede ser verificada con este valor y también el mensaje 1 o el mensaje 2. Esto previene el tener que incluir H(M,) en una copia de la firma, y $H(M_2)$ en la segunda copia de la firma cuando se distribuyen a las dos partes involucradas. En lugar, de que los valores sean extraídos desde el valor del XOR y la versión de la firma dual verificada. Se muestra un caso a continuación:

- Se toman dos mensajes, M_1 y M
- Se crea la firma dual:
  H= H(H(M,) + H(M))
- Firma dual normal:
  (H), Sig., H(M) para el tenedor de M .
  (H), Sig., H(M,) para el tenedor de M .
- Pero ahora incluye en la firma:
  γ = H(M,) XOR H(M)
- La firma dual SET para todas las partes es:
  (H ,Sig., γ
- El tenedor de M_1 verifica la firma dual extrayendo $H(M_2)$ de γ.
  H(M, se obtiene aplicando el algoritmo hash a M .
  H(M,) = H(M,) XOR γ
- Habiendo obtenido $H(M_2)$ de γ, la firma dual es validada de manera normal
  H,M , y H(M) son concatenados, y al resultado se le aplica el algoritmo hash.
  H = H(H'M), H(M ')), el resultado del hash, H , debe ser igual al H en la firma.
  H = H firma válida.

La optimización de la firma dual SET permite que la misma firma sea enviada a ambas partes (H ,Sig., γ, en vez de reemplazar γ con diferentes valores para cada receptor

Instrucciones de pago (PI)

El contenido nunca es enviado al vendedor, pero si es enviado al adquirente. Los datos actuales de las tarjetas de crédito son incluidos con nonces para frustrar ataques de repetición y diccionario. Los datos de la tarjeta son protegidos usando una encripción muy robusta, la cual consiste en cifrar los datos de manera directa con RSA, en vez de cifrarlos con la llave simétrica DES y después encriptando la llave simétrica usando RSA. Este tipo de encripción es mucho más segura que un cifrado normal

Se aplica una función hash a la orden, H(Orden), es incluida, la cual identifica la orden única del tarjetahabiente con esa instrucción de pago

La firma dual ya creada para OI. Es usada como la firma en PI El PI es encriptado con la llave pública del intercambio de llaves del adquirente. Esto previene al vendedor, o a alguien, de ver su contenido.

La solicitud de pago incorpora el pago actual de tarjeta de crédito desde el punto de vista del tarjetahabiente. Este es el corazón del protocolo de pago SET y una vez enviado, el tarjetahabiente ha mostrado un acuerdo de pago que no puede ser fácilmente revocado.

Procesando PReq

Cuando el vendedor recibe una solicitud de compra del tarjetahabiente, las partes OI y PI son extraidas. El vendedor verifica la firma dual del tarjetahabiente en OI usando el certificado del tarjetahabiente recorriendo la cadena de confianza de certificados a la raiz.

Antes de enviar una respuesta de compra (PRes) al tarjetahabiente, el vendedor normalmente ejecuta la autorización y quizá los pasos de captura de pago. PRes quizá sea regresado antes de la captura o antes de autorización y captura. La opción escogida afectara el contenido del mensaje

Si la autorización es retrasada, el vendedor enviará una respuesta de compra indicando que el tarjetahabiente debe consultar el estado de la transacción más tarde.

Cuando el vendedor no envía la respuesta al tarjetahabiente, éste contendrá el estado de la transacción y algún código de resultado disponible El CompletadoCódigo indica si los pasos de autorización o captura han sido completados Los resultados contienen los códigos de autorización o captura para la transacción si esos pasos han sido ejecutados Esos códigos son generados en la red financiera de tarjetas bancarias para autorizar y aprobar la transacción, y quizá aparezcan en la factura mensual del tarjetahabiente

El mensaje de orden de compra forma la compra actual por el tarjetahabiente del vendedor. Cuando el tarjetahabiente recibe la respuesta del vendedor, sabe también que el pago se ha realizado o que la transacción está esperando a ser procesada por la red financiera de tarjetas de crédito

3. Autorización (AuthReq/AuthRes)

Permite al vendedor verificar sí el tarjetahabiente tiene crédito para la compra y obtiene el permiso para cargar la transacción a su tarjeta. En la solicitud de autorización, el vendedor envía datos acerca de la compra, firmados y encriptados al adquirente El PI del tarjetahabiente también es enviado en esta solicitud.

Los datos enviados incluyen el valor hash de los detalles de la orden Si son iguales que el H(Orden) presentado en el PI, el adquirente sabe que el vendedor y el tarjetahabiente están de acuerdo acerca de los bienes pedidos y la cantidad de compra. La firma dual en el PI provee que ésta venda desde el tarjetahabiente. El (OIDatos) en la solicitud del vendedor muestra el conocimiento de OIDatos que son firmados por la firma dual, mostrando un acuerdo de los datos de la orden sin revelarlos Los Thumbs son una lista opcional de certificados relevantes sostenidos por el vendedor para prevenir que el adquirente los envie en la respuesta. La dirección de facturación del tarjetahabiente (se obtiene fuera del protocolo SET) y otros detalles del vendedor como el tipo de negocio son esperados

Autorización y Captura pueden ser ejecutados desde una sola solicitud, conocida como transacción de ventas. VentasInd es usado para indicar si el vendedor desea hacer esto

Al recibir AuthReq, el adquirente decripta las partes del mensaje, verifica firmas, y checa la consistencia entre los detalles de compra enviados por el vendedor y los que están en PI Si la solicitud del vendedor (AuthReqAmt) no es la misma que la CompraAmt, ésta es checada con la diferencia que sea aceptada para la norma El adquirente obtiene autorización a través de la red financiera

Habiendo recibido una buena autorización desde el emisor de la tarjeta, una respuesta de autorización (AuthRes) es regresada al vendedor con el código de autorización desde el vendedor. Este contiene un token (señal) de captura, firmado y encriptado, el cual es usado más tarde por el vendedor para capturar el pago. Sólo el adquirente puede decriptar el token, guardando los datos de captura escondidos de alguien más.

Si la captura fue ejecutada con la autorización (transacción de ventas), entonces el código de captura y la cantidad son regresadas en vez del token de captura. Al recibir una autorización aprobada, un vendedor puede embarcar los bienes comprados. Una autorización aprobada indica que el emisor de la tarjeta ha verificado los detalles de la tarjeta y el límite de crédito, y aprueba la continuación de la compra.

4. Captura de Pago (CapReq/CapRes)

Después de procesar una orden, el vendedor necesita solicitar el pago previamente autorizado para ser transferido a su cuenta. El pago total para muchas autorizaciones pueden ser capturadas en un solo lote de solicitud.

Un vendedor quizá acumule muchos tokens de captura (desde la autorización) a través del día y entonces los reembolsos para ese al final del día.

Muchos tokens de captura de diferentes transacciones pueden ser incluidos en una sola solicitud por eficiencia. Para cada token, la cantidad autorizada correspondiente y el ID de la transacción son incluidos. Eso debería ser igual a la encripción de datos dentro del token de captura. CapID es el único valor usado para identificar esta captura de otras. Las solicitud es firmada y encriptada por el vendedor.

Después de la verificación de la solicitud de captura el adquirente acredita la cuenta del vendedor. Los intereses de la transacción quizá sean deducidos en este estado. La respuesta de captura (CapRes), firmada y encriptada, contiene una indicación de éxito, la cantidad acordada, y el código de captura desde la red financiera.

Después del éxito de la captura, el vendedor ha recibido el pago del dinero de la compra del tarjetahabiente. Si el vendedor no ha enviado ya la respuesta de la compra al tarjetahabiente, es hecho ahora.

5. Consulta de Tarjetahabiente (InqReq/InqRes)

El mensaje de consulta permite a un tarjetahabiente verificar el estado de una transacción. Una consulta puede ser enviada tiempo después de la solicitud de la compra, y un tarjetahabiente puede consultar sólo su propia compra. La consulta puede ser ejecutada muchas veces para una sola transacción.

La solicitud de consulta contiene el ID de la transacción e incluye un nuevo challenge. Debería ser único para cada invocación, desde la consulta quizá sea repetidamente. La consulta es firmada para probar que la solicitud viene desde el tarjetahabiente correcto.

La respuesta de consulta regresada por el vendedor es muy similar a PRes. Este contiene el estado de la transacción y algunos códigos de resultado (autorización y captura) disponible. Habiendo recibido una respuesta de consulta, el tarjetahabiente puede asegurar como una compra específica con un vendedor acreditado es procedente.

Registro del tarjetahabiente

Todas las partes involucradas de un pago necesitan certificados para enviar mensajes SET. Cuando los tarjetahabientes quieren iniciar usando SET para hacer redes de pago, deben obtener un certificado de llave pública desde una AC. Cada tarjetahabiente necesita un certificado de firma conteniendo su llave pública de firma, así que por eso los mensajes firmados pueden ser verificados. Un certificado de encripción, con el

intercambio de llave pública, es opcional desde que ninguno de los mensajes de pago SET enviados al tarjetahabiente son encriptados en la actual versión de SET

Los certificados tienen fecha de expiración, la cual usualmente es igual a la fecha de expiración de la tarjeta de crédito.

El proceso de registro inicia cuando el tarjetahabiente envía una solicitud (CInitReq) a AC preguntando por:

- El certificado de intercambio de llaves de la AC. Esta permitirá enviar los mensajes más tarde a la AC para ser encriptados con la llave pública intercambiada. Aclaramiento, para verificar este certificado, todos los usuarios deben tener una copia de la llave pública raiz
- Una forma de registro electrónico desde la institución financiera del tarjetahabiente.

El tipo de solicitud indica si el tarjetahabiente busca un certificado de firma, un certificado de encripción, o ambos. El BancoID (BIN) son los primeros seis números en la tarjeta y únicamente identifica al banco emisor. El campo Lenguaje es usado para solicitar el lenguaje en la forma de registro regresada. Un thumb de un certificado actual es enviado

La respuesta de la AC(CInitRes) tiene la apropiada forma de registro, los certificados de la AC y esas necesitan verificarlos, y la lista de los certificados relevantes revocados (LRC), todos firmados por la AC.

El tarjetahabiente ahora válida los certificados recorriendo la cadena de confianza y remueve algunos certificados en la lista de revocación. El tarjetahabiente puede estar confiado de que ha recibido una forma de registro válida desde una AC acreditada. La forma de registro es llenada e incluye el número de tarjeta de crédito y la fecha de expiración. Para enviar los datos sensitivos a la AC, es encriptada directamente con el intercambio de llaves de la llave pública RSA de la AC

El nonce del tarjetahabiente (NonceTarjeta) será combinado con un nonce generado por la AC (NonceAC) en la forma PANNONCE. Este nonce es usado en el protocolo de pago H(DatosTarjeta, PANNONCE) también aparece en los certificados de los tarjetahabientes

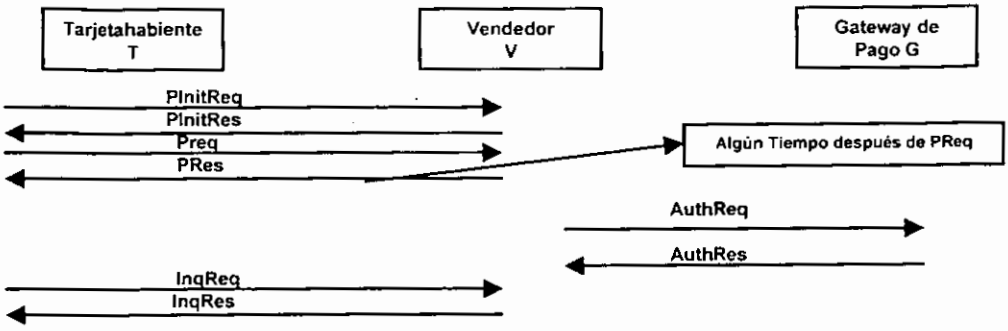
El tarjetahabiente firma las llaves pública que son certificados, e incluyen éstos con la forma de registro para construir el mensaje de solicitud de certificado (CertReq). La solicitud es encriptada antes de enviarla a la AC

Cuando la AC recibe la solicitud de certificado, esta autentica la tarjeta con el banco emisor usando una red financiera. Si los datos de la tarjeta son válidos esto firmará y generará los certificados para las llave públicas del tarjetahabiente.

La respuesta de certificado desde la AC (CertRes) contiene los nuevos certificados y el NonceAC encriptado. El tarjetahabiente verifica los certificados. También combina el NonceAC decriptado con el NonceTarjeta para formar un PANNONCE

Puede ser verificado que H(DatosTarjeta, PANNONCE), el cual forma el único ID del tarjetahabiente, y aparece en los nuevos certificados

El tarjetahabiente tiene la firma del certificado requerido para hacer una compra, y puede iniciar a realizar pagos con tarjeta de crédito a los vendedores.



Pasos en una Transacción SET

Procedimiento de Compra por Internet (SET)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de Certificados y de llaves**	**comprador vendedor adquirente, AC**									
1	Obtienen sus certificados	**emisor, gateway**									
2.	**Obtención del Software**	**comprador vendedor gateway, AC**									
1	Deben obtener su software respectivo cartera (comprador), servidor del vendedor (POS), la autoridad certificadora (AC), el gateway										
3.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
4.	**Selección del artículo a adquirir**	**comprador**									
1	Entra a la tienda virtual				5	*					
.2	Busca el articulo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
5.	**Alta de dirección e-mail de un comprador**	**comprador**									
1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
6.	**Ingreso de dirección e-mail del comprador**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
7.	**Ingresa sus datos el comprador**	**comprador**									
1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario			5		*				*	
8.	**Verificación del llenado de los datos**	**vendedor**									
1	Checa que los campos tengan datos				5		*				
2	Muestra los datos ingresados				5	*					
9.	**Elección de la dirección**	**comprador**									
1	Tiene que elegir la dirección a la cual quiere que se le envie el producto				5	*					
10.	**Muestra datos del comprador y del artículo**	**vendedor**									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envio				5	*			*		
11.	**Asignación de una cantidad del artículo**	**comprador**									
1	Asigna una cantidad de compra				5	*				*	
12.	**Señalización de las formas de envio**	**vendedor**									
1	Da las diferentes formas de envio y una breve descripción (Nacional/Internacional)				5	*		*			

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
13.	**Elección de forma de envío**	**comprador**									
.1	Elige la opción más adecuada conforme a sus necesidades.				5	•				•	
14.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación.				5	•					
.2	Menciona los procesos de pago.					•		•			
15.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación.				30	•	•				
.2	Selecciona el método de pago.				5	•				•	
.3	Ingresa los datos que se requieren de la forma de pago elegida.			5		•				•	
16.	**Envío de solicitud de compra**	**comprador**									
1	Envía la solicitud para la compra de los artículos seleccionados e información del pago, al vendedor.										
17.	**Envío de la solicitud al gateway de pago**	**vendedor**									
.1	Envía la solicitud de la compra enviada por el comprador al gateway.										
18.	**Proceso de autorización**	**gateway**									
1	Autorizan la solicitud.	**vendedor**									
2	Envía solicitud de captura al gateway.										
19.	**Proceso de captura.**	**gateway**									
.1	Procesa la solicitud de captura a través de la red financiera de pago con tarjeta de crédito.										
20.	**Acreditación del comprador**	**vendedor, gateway**									
.1	Acreditación de las cuentas del comprador.										
21.	**Contestación de la autorización**	**vendedor**									
.1	Envía la respuesta de autorización de la orden al comprador.										
22.	**Corroboración de la solicitud de la orden de compra**	**comprador**									
.1	Solicita una consulta de la orden de compra, donde le envían el número de transacción.										
23.	**Envío de la consulta de la orden de compra**	**vendedor**									
.1	Envía la consulta al comprador.										
24.	**Envío del producto**	**vendedor**									
1	Envía el producto		25					•	•		
25.	**Recepción del producto**	**comprador**									
1	Recibe el producto		700			•					

3.2 Cheques Electrónicos

Un cheque digital es un modelo de cheque de papel. No puede validar cheques digitales sin involucra al que lo emite. Asigna y endosa los cheques usando firmas digitales. Los certificados digitales establecen la identidad del pagador y la información del banco. La autenticación es lograda usando el criptosistema de llave pública. El pagador firma digitalmente una forma conteniendo la descripción de la transacción, información del pagador y del beneficiario, la cantidad y un sello con la hora. El beneficiario, que puede recibir la forma mediante correo electrónico público u otras formas variadas de comunicación electrónica, puede validar el cheque usando una llave pública y depositarla para recibir pago.

Hoy en día se está perdiendo el uso de este tipo de sistema de pago, esto radica en que los costos para procesar los cheques son caros, quizá involucren el transporte de los cheques firmados al banco, en el cual está girado antes de que sea posible determinar si el pago puede ser hecho, también incluye los llamados artículos regresados (cheques bounced) significa que el costo promedio por cheque es poco alto, y la segunda es el uso de tarjetas de débito, donde cada transacción incluye una verificación electrónica de la disponibilidad de fondos, tiene todas las propiedades de un pago basado en cheque sin las desventajas de una persona que verifique si tiene o no fondos.

Es claro pensar, que hay una necesidad de un sistema de pago como el cheque donde los fondos son transferidos desde la cuenta del pago del pagador a la cuenta de pago del tenedor, en el tiempo en el que la transacción toma lugar. Desde el punto de vista de los bancos sería deseable usar redes de transferencia de fondos interbancarios existentes, tanto como sea posible.

3.2.1 Ventajas de los Cheques Electrónicos

- Los cheques electrónicos trabajan de la misma manera que un cheque tradicional. Mantiene las características básicas y la flexibilidad de los cheques de papel, mientras mejora su funcionalidad, los cheques electrónicos pueden ser fáciles de entender y adoptar.
- Los cheques electrónicos son también usados en la aclaración de micropagos, la criptografía convencional de los cheques electrónicos hace más fácil su proceso que los sistemas basados en criptografía de llave pública. El pagador, el tenedor y el banco del pagador pueden autenticar los cheques a través del uso de certificados de llave pública. Las firmas digitales pueden ser validadas automáticamente.
- Pueden servir para mercados corporativos. Las firmas pueden usar cheques electrónicos para completar pagos sobre redes con un costo más efectivo que presenta alternativas. Además, desde que el contenido de un cheque puede ser unido a la información del remitente, el cheque electrónico fácilmente es integrado con las aplicaciones EDI, tal como un recibo de cuentas.

3.2.2 FSTC Proyecto de Cheques Electrónicos

El Consorcio de Tecnología de Servicios Financieros (FSTC), es un grupo de bancos americanos, agencias de investigación, y organizaciones gubernamentales, formado en 1993.

El FSTC es el proyecto de cheque electrónico desarrollado para hacer un reemplazo electrónico al cheque de papel. Se usarán cheques electrónicos como los cheques de papel, por negocios y consumidores, y usarán los sistemas existentes de aclaramiento interbancario. Como el cheque de papel, el cheque electrónico requiere la misma información que se necesita para completar un pago. Igualmente, las chequeras de cheques de papel son reemplazadas por chequeras de cheques Electrónicos portables; usan firmas digitales para firmar y endosar, y certificados digitales para autenticar al pagador, al banco del pagador y a la cuenta del banco. Sin embargo, a diferencia del cheque de papel, a través del uso de un emisor, el cheque electrónico puede parecerse a otros instrumentos de pagos financieros, tales como tickets de cargo electrónicos de tarjetas, cheques de viajero, o cheques certificados. Aunque el uso del cheque electrónico es hacer pagos electrónicos en redes públicas, el plan del proyecto permitirá usar el cheque electrónico en cualquier situación como las del cheque actual.

El cheque electrónico es entregado por transmisión directa o por sistemas públicos de correo electrónico. Los pagos (depósitos) consisten en cheques electrónicos que son recogidos por bancos vía e-mail y se aclaran a través de los canales de la banca existentes.

Un cheque electrónico contiene una instrucción para el banco del pagador, para hacer un pago de una cantidad específica para un identificado tenedor. En comparación con los cheques normales un cheque electrónico ofrece nuevos servicios: habilidad para que inmediatamente verifique los fondos disponibles. La seguridad puede incrementarse permitiendo validación de firmas digitales, y verificar los pagos puede ser más fácilmente integrándolos dentro de los procesos de ordenamiento y facturación. Un pagador emitirá un cheque con la misma información que un cheque de papel. Se asume que los usuarios tienen algún certificado basado en llave pública.

Los individuos capaces de emitir cheques tendrán en su poder un dispositivo de chequera basado en alguna forma segura de hardware. Su función es asegurar el almacenamiento de la llave secreta y la información del certificado, así como mantener un registro de que cheques han sido endosados o firmados recientemente. El cheque será enviado al tenedor por medio de un paquete seguro (un e-mail seguro o por medio de encripción entre las dos partes)

El tenedor endosa el cheque cuando es recibido, usa un dispositivo de hardware seguro para registrarlo antes de enviarlo al banco del tenedor. Al llegar a este punto, el FSTC prevé el procesamiento de manera idéntica al proceso de un cheque de papel. Significa que si se hace la aclaración del cheque usando la casa de aclaramiento automático normal (ACH) o los métodos de quejas de cheque electrónico.

Beneficios del Cheque Electrónico

- Cubre los elementos para ser un sistema de pagos en el comercio electrónico.
- Permite a los bancos recoger depósitos electrónicamente.
- Rápida adopción. Es fácil de entender y de manejar.
- Gran Flexibilidad. Soporta otros tipos de medios de pago.
- Alternativa eficiente para el consumidor y el vendedor.
- Integración abierta con los mecanismos de pago interbancario existentes.
- Direcciona los problemas de la recolección de depósitos electrónicamente en las redes públicas, desde que habilita a todos los clientes, para recoger, transmitir y depositar cheques electrónicos en sus cuentas sin ir físicamente al banco.
- Autenticación de Cheques Electrónicos. Los cheques electrónicos pueden ser autenticados por el uso de certificados de llave pública certificados por el tenedor, y los bancos del tenedor y pagador. Las firmas digitales pueden ser validadas automáticamente.

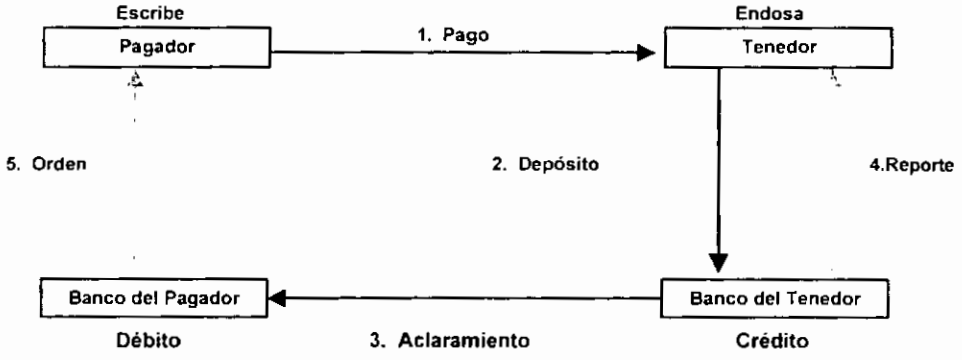
- Prevención del fraude y Confidencialidad: Los cheques electrónicos serán resistentes debido al uso de firmas criptográficas. Estas proveen gran seguridad y reducirán las pérdidas por fraude para todas las partes en el proceso de pagos eliminando en la mayoría de los casos malos cheques de papel. Proporcionan confidencialidad, los Cheques Electrónicos quizá se encripten, si se envían en redes públicas.

Flujo de la función de un cheque electrónico

Escenarios de pago

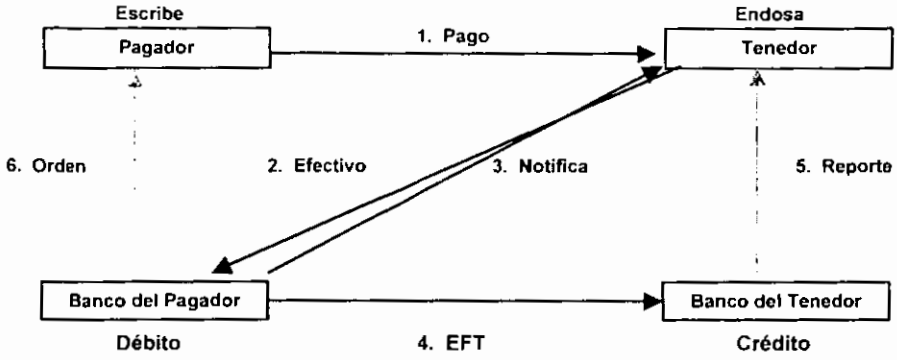
1. Depósito y aclaración.

El pagador emite un cheque electrónico firmado junto con su dispositivo chequera. Es enviado al tenedor quien lo endosa, también usando un dispositivo de hardware seguro antes de enviárselo a su banco. El banco entonces aclarará el cheque con el banco del pagador usando una transferencia ACH (Automatic clearing House / Casa Automática de Aclaramiento). Los bancos informan a sus clientes el progreso con los pasos de estado y reporte. No hay llave para el flujo del mensaje principal. Una de las desventajas de este escenario es que todas las partes deben tener capacidades para actualizar la red, y el procesamiento para negociar con cheques electrónicos, antes de que un solo pago pueda ser hecho.



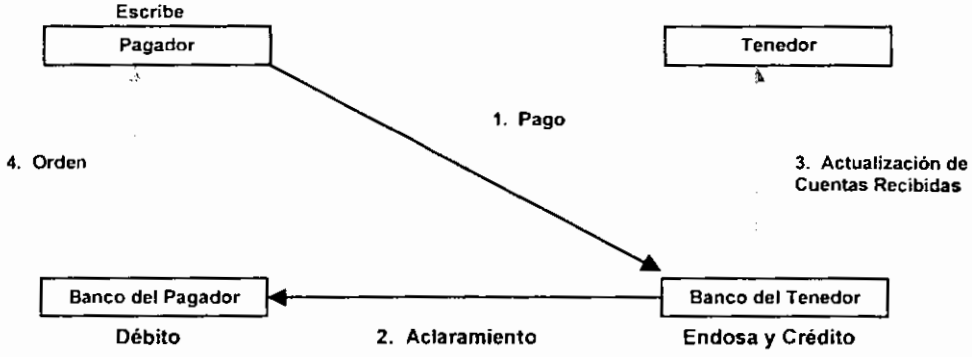
2. Efectivo y Transferencia

Mientras el tenedor puede aceptar cheques electrónicamente, si el banco no puede. El tenedor cobra el cheque presentándolo al banco del pagador especificando detalles de que su cuenta bancaria está en proceso. El banco del pagador responde con una notificación y entonces el crédito de la cuenta del banco del tenedor se realiza usando una convencional transferencia de fondos interbancarios (EFT)



3. Lockbox

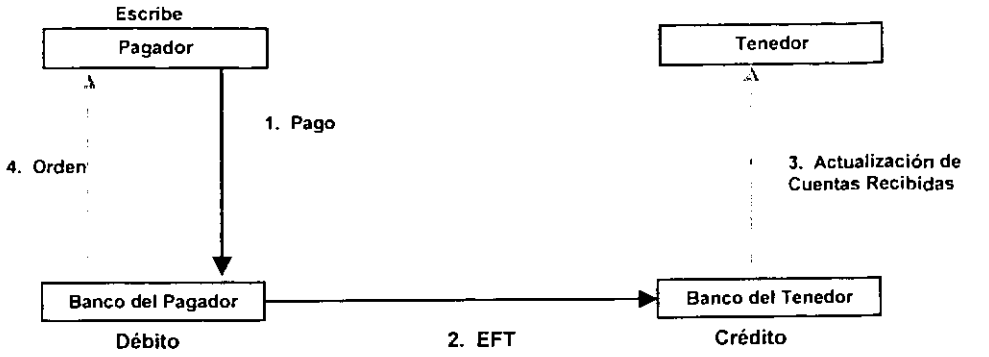
El cheque electrónico no es enviado al tenedor, pero si a su banco La cuenta de destino quizá sea una cuenta bancaria primaria del tenedor o una cuenta especial denominada lockbox, la cual es mantenida por el banco u otra tercera parte en nombre del tenedor



4. Transferencia de fondos

El pagador genera un cheque electrónico y lo envia directamente a su banco El banco transfiere el valor a la cuenta de banco del tenedor, y carga el monto al pagador usando un EFT interbancario convencional

En este caso, sólo el banco del pagador necesita estar equipado con el proceso de cheques electrónicos, y también todos los flujos son manejados por mensajes existentes del banco


Escribe
Pagador
Tenedor
1. Pago
4. Orden
3. Actualización de
Cuentas Recibidas
Banco del Pagador
Banco del Tenedor
Débito
2. EFT
Crédito

Procedimiento de Compra por Internet (FSTC/Depósito y Aclaración)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de la chequera**	comprador									
.1	Obtiene chequera electrónica.										
2.	**Ingreso a Internet**	comprador									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	comprador									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	comprador									
1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	comprador									
1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	comprador									
1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	vendedor									
1	Checa que los campos tengan datos.				5		*				
2	Muestra los datos ingresados				5	*					
8.	**Elección de la dirección**	comprador									
1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
9.	**Muestra datos del cliente y del artículo**	vendedor									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	*			*		
10.	**Asignación de una cantidad del artículo**	comprador									
1	Asigna una cantidad de compra.				5	*				*	
11.	**Señalización de las formas de envío**	vendedor									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional).				5	*		*			
12.	**Elección de forma de envío**	comprador									
1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	
13.	**Indica las formas de pago**	vendedor									
1	Pide password y su confirmación				5	*					
2	Menciona los procesos de pago					*		*			
14.	**Selección de un método de pago**	comprador									
1	Ingresa password y confirmación				30	*	*				
2	Selecciona el método de pago				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Emisión de un cheque**	**comprador**									
.1	Emite un cheque electrónico firmado.										
.2	Lo envia al tenedor para que lo endose.										
16.	**Endoso del cheque**	**vendedor**									
.1	Endosa el cheque enviado por el comprador.										
.2	Lo envia al adquirente.										
17.	**Aclaración del pago**	**adquirente**									
.1	El banco adquirente aclara el cheque con el banco emisor por medio de una transferencia ACH										
18.	**Progreso de la transacción**	**adquirente emisor**									
.1	Informan al comprador y al vendedor del progreso de la transacción.										
19.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	•			•		
20.	**Aceptación de la orden**	**vendedor**									
.1	Informa que la orden está lista.				5	•					
.2	Envia un mensaje, para informar el número de la orden.				30	•			•	•	
21.	**Envio del producto**	**Vendedor**									
.1	Checa el depósito del pago.		25			•					
.2	Envia el producto.		25					•	•		
22.	**Recepción del producto**	**Comprador**									
.1	Recibe el producto.		700			•					

3.2.3 NetBill

Sistema de pago desarrollado en Carneige Mellon University. El protocolo de transacciones NetBill inicia cuando un cliente solicita una cuota para seleccionar un artículo, y finaliza cuando una llave simétrica es recibida para desencriptar los bienes encriptados entregado durante la fase de entrega de bienes.

Los participantes en este sistema son clientes, vendedores y un servidor NetBill que mantiene cuentas para clientes y vendedores. Esas cuentas pueden ser ligadas a una cuenta convencional en instituciones financieras. Cuando un cliente compra un bien, su cuenta NetBill es cargada con la cantidad apropiada y la cuenta del vendedor es acreditada con el valor de los bienes. Una cuenta de un cliente NetBill puede ser usada para transferencias de fondos desde su banco. De manera similar los fondos en una cuenta NetBill del vendedor son depositados en su cuenta del banco. Garantiza que un cliente paga sólo por los bienes que son recibidos exitosamente. Una transacción NetBill es similar para verificar que inmediatamente transfiere desde una cuenta identificada a otra que toma lugar en el tiempo de la compra. El sistema sin embargo, carece de generalidad de una verificación en una de las partes, que debe tomar el rol del vendedor para que el pago se realice.

NetBill provee el soporte de transacciones a través de librerías integradas con diferentes pares de cliente/servidor. La librería del cliente es llamada la chequera (checkbook) y la del servidor es llamada caja (till); estas librerías se comunican con las aplicaciones respectivas del cliente y el servidor. Toda la comunicación de red entre los dos es encriptada para protección contra intrusos.

Antes de que el protocolo NetBill se ejecute, un usuario localizara la información requerida desde el servidor.

1 La transacción inicia cuando un cliente solicita una cotización formal a un vendedor. Hay cláusulas en el protocolo para permitir la negociación del precio estándar listado, para descuentos de volumen y de grupo, entre otros.

2 El vendedor, al recibir la solicitud de la cantidad, determina un precio para el usuario y regresa la cotización.

3 Si el cliente acepta el precio cotizado, da instrucciones a la chequera para enviar una solicitud de compra, a la caja del vendedor. Alternativamente el cliente quizá configure su chequera para enviar la solicitud de compra automáticamente si el precio es debajo de la cantidad especificada.

4 La caja al recibir la solicitud de compra, busca los bienes desde la aplicación del vendedor. Los encripta con una llave usada una sola vez y computa un checksum criptográfico al resultado. La caja entonces envía el resultado a la chequera del cliente.

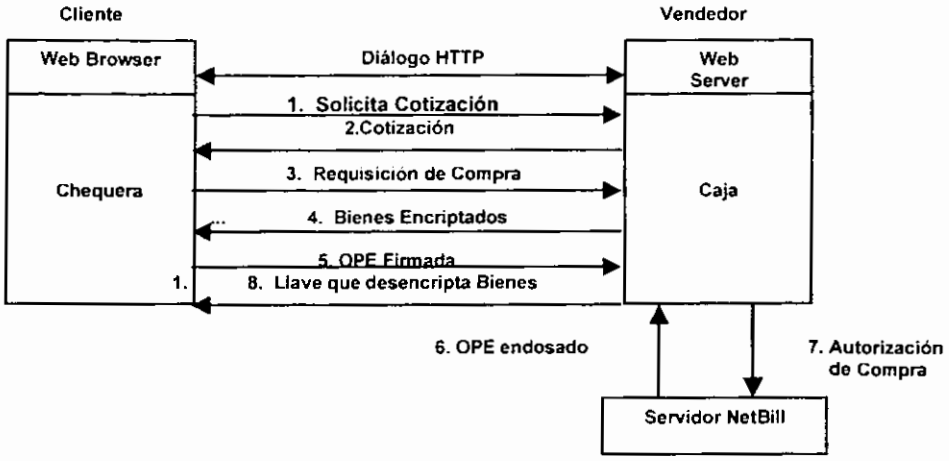
5 La chequera al recibir el mensaje encriptado, verifica el checksum. Este da la confianza a la chequera de que la solicitud de los bienes que recibió está intacta. Nota en este punto el cliente no pude desencriptar los bienes, sin que haya pagado por ellos. La chequera regresa una orden de pago electrónico (OPE) firmada a la caja del vendedor.

6 Una vez antes de que la OPE firmada sea enviada, un cliente quizá aborte la transacción sin daño de la transacción que está siendo completada contra la suya. El envío de una OPE firmada marca el punto de no regreso para el cliente. Al recibir la OPE la caja endosa la OPE al servidor NetBill.

7 El servidor NetBill verifica el precio, los checksums, y que, estén en orden y hace un cargo a la cuenta del cliente con la cantidad apropiada. Este carga la transacción y salva una copia de la llave de una sola vez. Regresa al vendedor un mensaje de aprobado o de falla, firmado digitalmente.

8 La aplicación del vendedor envía la respuesta del Servidor NetBill a la chequera del cliente junto con la llave que desencripta los bienes.

La transacción de compra involucra la información de los bienes, todas las transacciones son atómicas



Protocolo de Transacción

Procedimiento de Autenticación

La autenticación de NetBill se basa en un esquema modificado de Kerberos. La finalidad de las modificaciones es retener el uso de criptografía simétrica eficiente para el tráfico de cifrados, pero decrementar la dependencia de los servidores Kerberos permitiendo que las llaves públicas sean usadas en ciertas partes del protocolo de intercambios. El resultado es un sistema Kerberos de llave pública.

En Kerberos, si A desea comunicarse con B, un ticket debe ser primero conseguido (T_{AB}) desde un servidor con propósito especial, tan bien como una llave de encripción (K_{AB}) que se usará para asegurar el diálogo con B. Aunque contiene K_{AB}, el ticket no es un número secreto porque sólo puede ser decriptado por B. Cuando A desea enviar un mensaje a B, K_{AB} es aplicada a los datos, e incluye el ticket. A envía lo siguiente:

[illegible]

Cuando B recibe éste, él puede extraer K_{AB} desde el ticket y desencripta el mensaje, así sabemos que A es quien dice ser.

En NetBill, antes de que la comunicación tome lugar, A obtiene un ticket (T_{AB}) no desde un servidor especial sino desde B, de la siguiente manera. A inventa una llave simétrica de encripción ($K_{challenge}$), y la envía a B en el siguiente mensaje:

[illegible]

Se asume que A y B tienen acceso a sus llaves públicas de cada uno en forma de certificado. Así B puede validar la Sig_A, si él desea asegurarse de que la fuente del mensaje es en efecto el de A. B entonces usa su llave privada para obtener la llave K_{UnaVez}, y por lo tanto obtener acceso a la parte principal del mensaje que contiene la $K_{challenge}$. B ahora construye un ticket normal de Kerberos T_{AB}, y le asocia K_{AB} y regresa eso a A encriptandolo con $K_{challenge}$:

[illegible]

Un $K_{challenge}$ inventado en el primer lugar, fue compartido sólo con el tenedor de Kpr_B. Cuando este mensaje es exitosamente desencriptado, A recobra T_{AB} y K_{AB} en texto claro y conoce que ellos fueron generados por B.

Antes de que la transacción ocurra, el cliente contacta al vendedor de la manera antes mencionada y establece T_{CM} para ser usado en los diálogos subsecuentes. Similarmente el servidor del vendedor establece el ticket T_{MN} con el servidor NetBill y el cliente mantendrá a T_{CN} (via el vendedor) para comunicaciones con el servidor NetBill.

Protocolo de Transacción

Este protocolo puede ser dividido en tres fases:

1. El cliente solicita al vendedor una cuota para uno o más productos identificados. Requiere un mínimo de dos mensajes de intercambio o más, si el precio debe ser negociado.
2. Fase de entrega, donde el vendedor encripta los bienes al cliente.
3. Fase final, donde el cliente envía una autorización firmada al servidor NetBill, vía el vendedor, permitiendo que la compra sea completada.

Fase de solicitud de precio

Cuando el cliente desea hacer una compra, se envía el siguiente mensaje al vendedor:

T..., K... [Credenciales, PRD, Bid, RequestFlags, TID]

El vendedor extrae K_{CV} desde el ticket y lo usa para desempaquetar la solicitud de cotización. Los elementos más importantes son los datos de solicitud del producto (PRD), el cual describe los bienes solicitados, y el bid, el cual es el precio que el cliente está ofreciendo. Otros elementos incluyen las credenciales de los clientes, las cuales especifican algún grupo de miembros que quizás merezcan un descuento, RequestFlags, el cual da más información de la naturaleza de la compra y una transacción única ID (**TID**).

Al recibir este mensaje, el vendedor computará una cotización para los bienes y enviará el siguiente mensaje de regreso al cliente:

K... [ProductoID, Precio, RequestFlags, TID]

La inclusión del ID de la transacción (TID) une la cotización de regreso a la solicitud original hecha por el cliente. En respuesta, el Precio y las RequestFlags se refieren a los términos de que el vendedor está ofreciendo más de lo que fue solicitado por el cliente, y el ProductoID es una descripción textual que aparecerá en el estado de cuenta del cliente si la transacción es completada.

Fase de Entrega de Bienes

Cuando se concluye la negociación del precio, el cliente acepta la oferta del vendedor enviando oportunamente el ID de la transacción, éste es señal para el vendedor de que los bienes pueden ser ahora transferidos a través de la red a los clientes.

T..., F... [TID]

El vendedor genera una llave aleatoria, K_{Bienes}, que es usada para encriptar la información de la compra, y entonces enviada ligada a los productos para el cliente:

F_{Bienes} [Bienes], K... [SHA F_{Bienes} Bienes], ... [TID]

El cliente puede verificar la integridad de los bienes aplicando un algoritmo hash seguro (SHA / Secure Hash Algorithm), a los bienes, y verificando que sea igual a lo computado por el vendedor. Sin embargo, no será capaz de decriptar los bienes hasta que el pago este hecho. El ID de la orden del pago electrónico (OPEID) es una cantidad que será usada únicamente para identificar la transacción en la base de datos NetBill. Contiene campos que identifican al vendedor, tan bien como la información de un timestamp.

Fase de pago

El cliente firma un compromiso para hacer el pago y construir una orden de pago electrónico (OPE) OPE contiene detalles acerca de la transacción y es legible por el vendedor y el servidor NetBill Desde que el cliente está encriptando los datos para el servidor NetBill, asume que ya se autentico así mismo y tiene un ticket apropiado, T_{CN}, y su correspondiente llave de encripción K_{CN}

La parte de la transacción de OPE incluye los siguientes campos:

- Identidad del cliente
- El ID del producto y el precio especificado en la cotización del vendedor
- Identidad del vendedor
- Un checksum de los bienes encriptados

La parte de instrucción de pago de OPE incluye

- Un ticket que provee la identidad verdadera del cliente
- El número de cuenta del cliente
- Un campo memo del cliente.

Para iniciar la fase de pago, el cliente firma OPE y la envía al vendedor

$$T_{CN}, K_{CN}\{OPE, Sig_C\}$$

El vendedor verifica la firma del cliente, verifica que el ID del producto, el precio, y el checksum de los bienes estén en la orden antes de endosarla y regresarla al servidor NetBill, el proceso de endoso involucra la concatenación del número de cuenta del vendedor (Vacct), un campo memo (Vmemo), y la llave usada para encriptar los bienes (K_{Bienes}), y entonces firma el resultado, se firma con la llave privada del vendedor para producir Sig_V La cantidad que se envía al servidor NetBill es:

$$T_{CN}, K_{CN}\{\{OPE, Sig_C\}, Vacct, Vmemo, K_{Bienes}\}, Sig_V\}$$

Cuando el servidor NetBill incluye alguna información del estado de la cuenta en el recibo y envía lo siguiente al vendedor:

$$K_{CV}\{Recibo\}, K_{Bienes}, OPEID, Cacct, Balance, Flags\}$$

El vendedor desempaqueta el recibo, y guarda una copia, y la reencripta usando K_{CV} antes de enviar el mensaje al cliente:

$$K_{CV}\{Recibo\}, K_{Bienes}, OPEID, Cacct, Balance, Flags\}$$

El pago ya está hecho, y el cliente puede extraer K_{Bienes} desde el recipiente y así obtener los bienes Los campos Cacct, Balance, y Flags dan toda la información necesaria en el status de la post transacción en su cuenta NetBill.

Procedimiento de Compra por Internet (NetBill)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de la chequera**	**comprador**									
.1	Obtiene chequera electrónica										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	•					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	•					
3.	**Selección del articulo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	•					
.2	Busca el articulo a adquirir			5		•			•		
.3	Selecciona el articulo				5	•					
.4	Agrega el articulo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	•				•	
.5	Muestra el articulo seleccionado				15	•					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
1	Se va al botón de nuevo				5	•					
.2	Pide dirección e-mail						•				
5.	**Ingreso de dirección e-mail del cliente**	**comprador**									
1	Ingresa dirección e-mail				10	•				•	
6.	**Ingresa sus datos el cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		•				•	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos				5		•				
.2	Muestra los datos ingresados				5	•					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envie el producto.				5	•					
9.	**Muestra datos del cliente y del articulo**	**vendedor**									
.1	Despliega la información del articulo a adquirir y los datos de la dirección de envio.				5	•			•		
10.	**Asignación de una cantidad del artículo**	**comprador**									
1	Asigna una cantidad de compra				5	•				•	
11.	**Señalización de las formas de envío**	**vendedor**									
1	Da las diferentes formas de envio y una breve descripción (Nacional/Internacional)				5	•		•			
12.	**Elección de forma de envio**	**comprador**									
1	Elige la opción más adecuada conforme a sus necesidades.				5	•				•	
13.	**Indica las formas de pago**	**vendedor**									
1	Pide password y su confirmación				5	•					
2	Menciona los procesos de pago					•		•			
14.	**Selección de un método de pago**	**comprador**									
1	Ingresa password y confirmacion				30	•	•				
2	Selecciona el método de pago				5	•				•	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Envío de una solicitud de cotización**	**comprador**									
1	Envía al vendedor una solicitud de cotización de los artículos que se quieren adquirir.										
16.	**Recibe la solicitud de cotización**	**vendedor**									
.1	Al recibir la solicitud determina un precio para el comprador.										
2	Regresa la solicitud.										
17.	**Aceptación del precio**	**comprador**									
1	Comprador acepta el precio.										
.2	Da instrucciones a la chequera para enviar una solicitud de compra a la caja del vendedor.	**chequera**									
18.	**Recepción de la solicitud de compra**	**caja**									
.1	Busca los artículos a adquirir y los encripta.										
.2	Envía lo antes mencionado a la chequera.										
19.	**Verificación de datos**	**chequera**									
1	Verifica que los datos se hayan recibido integramente.										
.2	Regresa una orden de pago electrónico firmada a la caja del vendedor.										
20.	**Recepción de la orden de pago**	**caja**									
.1	Al recibir la orden de pago la endosa.										
2	La envía al servidor NetBill.										
21.	**Cargo de la transacción**	**Servidor NetBill**									
1	Verifica que los datos recibidos estén en orden.										
2	Realiza un cargo a la cuenta del comprador.										
.3	Regresa al vendedor un mensaje de la aprobación de la transacción, firmado.										
22.	**Envío de respuesta de la transacción**	**caja**									
1	Envía la respuesta del Servidor NetBill de la transacción a la chequera, y envía la llave que desencripta los bienes.										
23.	**Muestra de la orden de compra**	**vendedor**									
1	Despliega la información total de la compra.				5	*			*		
24.	**Envío del producto**	**vendedor**									
2	Envía el producto.		25					*	*		
25.	**Recepción del producto**	**comprador**									
1	Recibe el producto.		700			*					

3.2.4 NetCheque

Sistema desarrollado por el Instituto de la Universidad del Sur de California, basa su seguridad en el uso de Kerberos. Es un servicio de cuentas distribuidas y se basa en jerarquías de servidores NetCheque (bancos) que son usados para la aclaración de los cheques y establece cuentas interbancarias

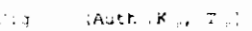
Una cuenta NetCheque es similar a las cuentas de un banco convencional contra la cuenta de los titulares que pueden escribir cheques electrónicos. Un cheque electrónico es como un cheque de papel el cual contiene la firma del cliente, te permite endosarlo para el vendedor antes de que el cheque sea pagado.

Usa tickets de Kerberos para crear las firmas digitales y endosar los cheques. Un NetCheque consiste de:

- Cantidad del cheque
- Unidad de moneda
- Fecha
- Número de cuenta
- Tenedor
- Firma del cliente
- Endosos para el vendedor y bancos

Los primeros 5 campos del cheque están en claro y son legibles por el portador del cheque. Los últimos dos campos son verificables por el banco contra el cheque que fue cobrado (girado)

Para escribir un cheque, un usuario genera la porción de texto claro del cheque. Él obtiene un ticket desde un servidor Kerberos que es usado para autenticarlo a él y a su banco (B), y permite compartir una llave de sesión (K_{CB}) con el banco. Entonces genera un checksum del contenido del cheque y lo coloca en un Autenticador ($Auth_C$). Encripta el autenticador con la llave de sesión que el comparte con su banco, agrega el ticket y el autenticador al servidor:



El ticket contiene una copia de la llave de sesión y es encriptada con la llave secreta del banco del cliente.

El cheque puede ser enviado al vendedor a través del correo electrónico sobre una red insegura, pero lo mejor para más seguridad es enviarlo por medio de un canal encriptado. Lo último que requiere el cliente es obtener un ticket de Kerberos adicional para el vendedor, el cual lo habilita para compartir la llave de sesión con el vendedor y encriptar la liga entre ellos.

Una vez recibido el pago un vendedor lee la parte de texto claro del cheque y obtiene un ticket Kerberos del banco del cliente desde un servidor Kerberos. El vendedor genera un autenticador ($Auth_V$) endosa el cheque en su nombre para el depósito en su cuenta. Agrega el endoso y el ticket al final del cheque. La firma del vendedor consiste de (Sig_V)

Entonces envía el cheque endosado a su banco (A) sobre un canal seguro. Esto lo hace obteniendo otro ticket Kerberos de su banco, y usándolo para compartir la llave de sesión para encriptar el canal.

Si el vendedor y el cliente usan diferentes bancos, entonces el banco del vendedor envía una indicación al vendedor de que el cheque ha sido depositado. Si el cheque tiene que ser aclarado a través de múltiples bancos, cada banco une su propio endoso al cheque, similar al del vendedor. Una vez que el cheque ha sido aclarado por el banco del cliente, los endosos agregados pueden ser usados para trazar la ruta de la cuenta del vendedor y eventualmente acreditar su cuenta

Procedimiento de Compra por Internet (NetCheque)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
1.	**Obtención de la chequera**	**comprador**									
.1	Obtiene chequera electrónica.										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
3	Selecciona el artículo				5	*					
4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra				5	*				*	
5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos				5		*				
.2	Muestra los datos ingresados				5	*					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
9.	**Muestra datos del cliente y del artículo**	**vendedor**									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envío				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
.1	Asigna una cantidad de compra				5	*				*	
11.	**Señalización de las formas de envío**	**vendedor**									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)				5	*		*			
12.	**Elección de forma de envío**	**comprador**									
1	Elige la opción más adecuada conforme a sus necesidades				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación.				5	*					
2	Menciona los procesos de pago					*		*			
14.	**Selección de un método de pago**	**comprador**									
1	Ingresa password y confirmación				30	*	*				
2	Selecciona el método de pago				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Generación del cheque**	comprador									
1	Genera un ticket de Kerberos y lo comparte con el banco.										
.2	Encripta el cheque, el ticket y el autenticador.										
3	El cheque se envia al vendedor.										
16.	**Recepción del pago**	vendedor									
.1	Al recibir el cheque, lo endosa y lo firma.										
.2	Envia el cheque al banco adquirente.										
17.	**Depósito del cheque**	adquirente									
.1	El banco adquirente envia un mensaje al vendedor de que el cheque ha sido depositado.										
.2	Endosa el cheque y lo envia al banco emisor.										
3	Aclara el cheque con el banco emisor.										
18.	**Aclaración del cheque**	emisor									
1	Aclara el cheque enviado por el adquirente.										
19.	**Envío de respuesta de la transacción**	vendedor									
1	Envia la respuesta al comprador de que la transacción se ha concretado.										
20.	**Muestra de la orden de compra**	vendedor									
1	Despliega la información total de la compra.				5	•			•		
21.	**Envío del producto**	vendedor									
.2	Envia el producto.		25					•	•		
22.	**Recepción del producto**	comprador									
1	Recibe el producto.		700			•					

3.3 Sistemas de Pago de Dinero Electrónico

El dinero físico que utilizamos hoy en día corre el riesgo de desaparecer, si ciertas dificultades que enfrenta el dinero electrónico son superadas. El advenimiento de tecnologías avanzadas, en el fotocopiado e impresión, hacen que el dinero físico sea un medio cada vez menos seguro y más caro de mantener.

La posibilidad que presenta el dinero electrónico, es la de sustituir al papel moneda, los cheques y hasta las operaciones vía tarjeta de crédito, que no es más que permitir la digitalización de todo el proceso de transacciones monetarias, para que no sólo los bancos y las grandes empresas utilicen un sistema electrónico de pago, sino también los individuos y los pequeños vendedores.

Es necesario entender que el dinero electrónico es radicalmente distinto a lo que hoy entendemos por dinero, concepto normalmente asociado con el del dinero físico o papel moneda. Otros medios de pago como el cheque o la tarjeta de crédito, no son más que sustitutos de ese dinero y tarde o temprano son canjeados por billetes por una de las partes involucradas en la transacción.

Un billete no es más que un trozo de papel, respaldado por el Estado y el sistema legal bancario. Es lo que hace posible obtener algo a cambio contra su entrega

El dinero electrónico debe mantener la característica de ser fungible, ser aceptado universalmente, tener un formato seguro y con respaldo, que pueda ser entregado de una parte a otra reiteradamente sin perder el valor original

Esta nueva forma de moneda no es más que un conjunto de bits. La información en bits transmitida en una transacción comercial, no es un intercambio de datos que crean el derecho de recibir cierta cantidad de dinero físico, sino que es en sí misma el dinero. Es esta característica del dinero electrónico, la que plantea las mayores dificultades para su implementación, ya que si esta información es copiada y no se cuenta con un sistema seguro que evite la duplicación del dinero, hará imposible su utilización

Básicamente, la idea del dinero electrónico es la siguiente: se almacena el dinero digital, previamente autorizado y firmado por un banco, en la computadora del usuario o en una tarjeta inteligente (con un chip integrado), el dueño puede gastar su dinero en cualquier establecimiento que acepte dinero electrónico, sin necesidad de abrir una cuenta o transmitir la información de su tarjeta de crédito. El establecimiento en cuestión debe aceptar el dinero y depositarlo en el banco. La seguridad en las transacciones se consigue mediante sistemas de criptografía virtualmente indescifrables

Para llevar a cabo este proceso se requiere de bancos que puedan cambiar dinero real por dinero electrónico, usuarios que tengan y gasten su dinero electrónico, establecimientos comerciales que lo acepten y bancos que puedan autorizar los pagos recibidos por los establecimientos. Por supuesto, la operación completa requiere de un sistema totalmente seguro como base

Hay dos tipos bien definidos de dinero electrónico:

- El identificable, que contiene la información que revela la identidad de la persona que originalmente extrajo el dinero del banco. De esta manera, permite a éste saber los movimientos del dinero en la economía, de la misma forma que lo haría una transacción con una tarjeta de crédito

- El anónimo (también conocido como cash digital o cash electrónico). El uso dado a este tipo de dinero es igual al papel moneda. Una vez que es retirado de la cuenta bancaria, se puede gastar o puede ser entregado sin dejar datos sobre quién lo utilizó

A su vez, existen dos variantes para cada tipo de dinero electrónico

- Online o en línea: para llevar a cabo una transacción con dinero electrónico online es necesario conectarse con el banco emisor, ya sea vía módem o vía red

- Offline o fuera de línea : no es necesario comunicarse con el banco emisor para realizar la transacción. Este tipo de dinero electrónico es uno de los más complejos porque presenta dificultad en su control y por lo tanto, se corre el nesgo de que sea copiado o gastado dos veces. Para evitar esto se utilizan métodos de claves criptográficas digitales de uso público y las llamadas firmas digitales que dan autenticidad al dinero electrónico.

Uno de los usos posibles del dinero electrónico, especialmente en reemplazo del dinero real o físico, es a través de una tarjeta acumuladora de valores o tarjeta inteligente (smart card), similar a la tarjeta telefónica, que contiene un chip recargable sobre el cual se pueda cargar o descargar la información necesaria. El usuario podría usar esta tarjeta para transacciones rutinarias de bajo valor ya que sólo permite cargar valores con un tope o límite.

Este sistema usa las tarjetas inteligentes que deben ser lo suficientemente confiables como para que el usuario no pueda repetir el proceso y recargarla indebidamente

Los bits de una tarjeta deben moverse de un lugar a otro, y una vez realizada la transacción, asegurarla, evitando que la transacción sea interceptada.

Con respecto a la seguridad, todo parece indicar que cada chip deberá tener la opción para que el usuario pueda usar un PIN, o número de identificación personal, para autorizar cada transacción. Esto sea tal vez incómodo para transacciones de bajo costo . sería algo así como si uno tuviera que ingresar su PIN cada vez que quisiera hablar por un teléfono público

El mismo chip podría usarse para guardar información personal, como tarjeta de crédito, como tarjeta de débito, llevar la información clínica del poseedor, etc.

Recientemente, Visa y Mastercard, dos precursores en el uso de esta tecnología, se pusieron de acuerdo en fijar un estándar que define los protocolos de comunicación entre las tarjetas y el lector. Cualquier emisor autorizado que cumpla con estas especificaciones de hardware y software, podrá cambiar cualquier tipo de información por este medio. Una consecuencia de este acuerdo permitirá el posible uso de una única tarjeta para realizar las compras, operar la cuenta bancaria desde un cajero o terminal, sumar los puntos de un programa de vuelo frecuente, y hasta permitir las compras vía Internet de una forma segura.

Propiedades del dinero

- **Aceptabilidad:** El dinero es casi universalmente aceptado como una forma de pago, independientemente de la cantidad de la transacción
- **Garantía de pago:** Una de las razones del porque es aceptable es que el manejo físico completa las transacciones y no hay riesgo de que el pago no sea aceptado posteriormente, ya que el valor de la transacción se cubre en el momento.
- **Transacciones sin cargos:** El dinero pasa de persona a persona, sin ningún cargo No se requiere autorización y, consecuentemente, no existen tráfico de comunicación o cargos.
- **Anonimato:** Muchas otras formas de pago involucran un papel de identificación
- **Independencia**. la seguridad del dinero digital no debe depender del lugar físico donde se encuentre, por ejemplo en el disco duro de una PC.
- **Seguridad**: el dinero digital no debe de ser usado en dos diferentes transacciones.
- **Privacidad**: el dinero electrónico debe de proteger la privacidad de su usuario, de esta forma cuando se haga una transacción debe de poder cambiarse el número a otro usuario sin que el banco sepa que dueños tuvo antes.
- **Pagos fuera de línea**: el dinero electrónico no debe de depender de la conexión de la red. así un usuario puede transferir dinero electrónico que tenga en una "smart card" a una computadora, el dinero digital debe ser independiente al medio de transporte que use
- **Transferibilidad**: el dinero electrónico debe de ser transferible, cuando un usuario transfiere dinero electrónico a otro usuario debe de borrarse la identidad del primero

- **Divisibilidad**: el dinero electrónico debe de poder dividirse en valores fraccionarios según sea el uso que se da, por ejemplo en valor de 100, 50 y 25

Pasos en una Transacción con Dinero Electrónico

La serie de pasos que puede seguir una transacción que se realiza con dinero electrónicc en un escenario simple es la siguiente:

Supóngase que el usuario A quiere mandar un cheque a B, usando ahora dinero electrónico

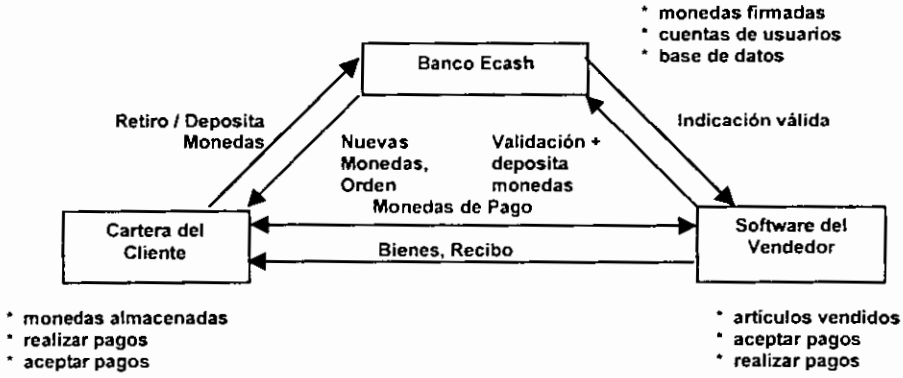
1 A genera un número aleatorio grande N de digamos 100 digitos y le da un valor digamos 1000 pesos
2 A encripta este número junto a su valor con su llave secreta asimétrica.
3 A firma este número y lo transmite a su banco.
4 El banco de A usa, la llave pública de A para desencripta el número y verificar la firma, así recibe la orden y sabe que es de A. El banco borra la firma de A del documento electrónico
5 El banco revisa que A tenga en sus cuentas la cantidad pedida 1000 pesos y la deduce de alguna de sus cuentas.
6 El banco firma el número que mando A, con el valor asignado de 1000 pesos
7 El banco regresa el número que ya es dinero a, A
8 A envia este dinero a B
9 B verifica la firma del banco de A, que está en N
10 B envia N a su banco
11 EL banco de B re-verifica la firma del banco de A en N
12 El banco de B verifica que N no esté en la lista de números "ya usados"
13 El banco de B acredita la cantidad de 1000 pesos a la cuenta de B
14 El banco de B pone a N en la lista de números "ya usados"
15 Finalmente el banco de B envia un recibo firmado donde establece que tiene 1000 pesos más en su cuenta

3.3.1 Ecash (Digicash)

Digicash es una compañía establecida en Holanda y en E.U., se especializa en sistemas de pago electrónico y dinero digital. Ecash fue desarrollado por DigiCash para proveer anonimato seguro al dinero electrónico para ser usado en Internet. Provee la privacidad de billetes y monedas con la seguridad adicional que requieren las redes abiertas. Es una solución de software en línea que permite pagar información, bienes, y servicios de pago externo (donde quizá el cliente reciba un pago como parte del servicio).

Los participantes en el sistema son los clientes, vendedores y bancos. Los clientes y vendedores tienen cuentas en el banco Ecash. Los clientes pueden retirar monedas contra su cuenta y almacenarlas en su software de monedero Ecash que reside en su computadora, este software es conocido como un cyberwallet (monedero cibernético). Este almacena y maneja monedas de los clientes, guarda los registros de todas las transacciones, y hace que los pasos del protocolo sean tan transparentes como sea posible para el cliente. El protocolo de retiro previene al banco desde que permite observar los números de serie de las monedas emitidas.

Un cliente puede usar las monedas para pagar mercancía. Al momento de la compra, el vendedor debe enviar las monedas a la casa de moneda del banco para asegurarse de que no han sido gastadas. Si las monedas son válidas, serán depositadas en la cuenta del cliente. Un vendedor también puede hacer pagos para un cliente usando el mismo procedimiento.



Participantes y sus funciones dentro de Ecash

Las monedas obtenidas desde un banco no deben ser aceptadas por otro. Como Ecash llega a ser más difundido, es como terceras partes quizá intercambien monedas de diferentes bancos o los bancos quizá provean ese intercambio. El aclaramiento interbancario quizá también llegue a ser posible, aunque las monedas todavía tendrán que ser enviadas a la casa de moneda del banco para su verificación.

Las monedas Ecash son únicas, emitidas particularmente por el cliente antes de ser firmadas por el banco, cada una tiene un número de serie que es generado por el software cyberwallet del cliente. Este número es escogido aleatoriamente, es lo suficientemente grande y es poco probable que alguien pueda generar el mismo número de serie.

El número de serie es unido y enviado al banco para ser firmado. Es donde se une el protocolo de unión de firma. El banco no es capaz de ver el número de serie de la moneda que está firmando. El método puede ser considerado similar a poner la moneda y una pieza de papel carbón dentro un sobre. El sobre es enviado al banco donde es firmado y regresado al cliente. El cliente abre el sobre y saca la moneda. La moneda ahora tiene firma. El papel carbón asegura que la firma del banco fue a través del sobre. La firma en la moneda sin

unir aparece con alguna firma digital normal No hay forma para decir que la moneda fue firmada usando el protocolo de unión de firma.

Llaves Moneda

Existe un problema, ya que el banco no puede ver lo que está firmando, como puede ver el valor de la moneda? Este problema puede ser resuelto por el banco usando una diferente llave de firma para cada denominación de moneda. El cliente informa al banco el valor de la moneda anónima para ser valuada. El banco entonces firma la moneda con la llave de firma representada para su denominación, y deduce la cantidad desde la cuenta del cliente

Una moneda consiste en un número de serie encriptado con la llave secreta apropiada del banco. Esta actúa como firma:

```
(# Serie) K-1 $1 Llave
```

Para permitir que la firma sea rápidamente verificada (decriptada), una indicación de que llave pública usar (VersionLlave) es incluida con una moneda Para conveniencia, el número de serie en texto plano es también incluido:

```
Moneda: #Serie,VersionLlave,(#Serie) K-1 $1 Llave
```

La VersionLlave puede ser usada para obtener otra información acerca de la moneda, incluyendo su valor, denominación y fecha de expiración. Esta información es intercambiada y almacenada durante la instalación de la cuenta inicial con un banco, o nuevamente durante el retiro. La llave pública se necesita para verificar cada firma de diferente valor, esta también es enviada al cliente.

Prevención del Doble Gasto

Las monedas Ecash son piezas de datos que pueden ser copiados. Para prevenir que las monedas copiadas sean gastadas nuevamente, el doble gasto debe ser prevenido.

Para asegurar que un número de serie no sea gastado dos veces, la casa de moneda del banco debe registrar cada moneda que es depositada de regreso en el banco Grandes base de datos de todos los números de serie son desarrolladas Una moneda válida sin gastar debe ser:

- Firmada, con una firma de denominación, por el banco,
- Tener una fecha de expiración asociada con ésta que debe ser después de la fecha presente,
- No aparecer en la base de datos de monedas gastadas

El tercer requerimiento puede ser sólo verificado por la casa de moneda del banco que mantiene la base de datos, y por lo tanto las monedas deben ser enviadas a éste para una verificación en línea durante la compra.

Cuando una moneda válida es aceptada, entonces puede ser gastada y su número de serie se ingresa a la base de datos. Un intento para gastar la moneda nuevamente debería de fallar

El tamaño de la base de datos Ecash podría llegar a ser tan grande e inmanejable. Pero usando las fechas de expiración con las monedas, los números de serie de esas monedas pueden ser removidos después de la fecha de expiración La máquina host del banco necesita tener una estructura escalable para hacer frente al crecimiento de la base de datos Además de que el manejo es un problema de escalabilidad, múltiples bancos, en la emisión y administración de su propia moneda con aclaramientos interbancarios, podría ser usado. También, si un gran número de gente comienza a usar regularmente Ecash, el sistema quizá empiece a mostrar retardos de inaceptabilidad y firmas de sobrecarga

Retiro de Monedas

Ecash usa el algoritmo de llave pública RSA. Para retirar una moneda ocurre lo siguiente:

1. El monedero del usuario escoge un factor anónimo r aleatoriamente.
2. El número de serie de la moneda, #serie, es oculto multiplicando el factor anónimo al exponente público (e2) para la denominación solicitada:

   #Serie * r^e2 (mod m)

   Aquí e2 es la llave pública para la denominación del par de llaves de 2 centavos.

3 El banco firma la moneda con la llave secreta de 2 centavos (d2):

   (#Serie * r^e2)^d2 (mod m) = #Serie^d2 * r^(e2*d2) (mod m)
   = #Serie^d2 * r (mod m)

El banco no puede ver el #Serie desde que no conoce r. La moneda anónima firmada es enviada de regreso al usuario.

4 El usuario divide el factor anónimo:

   (#Serie^d2 * r) / r (mod m) = #Serie^d2 (mod m)

La moneda firmada es la que permanece. Este aparece como una firma normal RSA (encriptada con la llave privada):

   (#Serie, {#Serie}Kpr_banco)

No puede ser ligada con el retiro. De esta forma, el anonimato completo quizá sea mantenido.

Muchas monedas de diferentes denominaciones, especificadas por el cliente, pueden ser obtenidas en una sola solicitud de retiro. La solicitud debe ser firmada con la llave privada del cliente, y la solicitud entera es protegida por la encripción con la llave pública del banco (Kpu_{Banco}). Esta llave es distinta de las llaves públicas de las monedas. La solicitud del retiro contiene las monedas anónimas sin firmar y una indicación de la denominación requerida. Una combinación de criptografía simétrica y asimétrica es usada en la implementación actual para eficiencia:

   {K, {Kpu_banco, {solicitud, {H(solicitud)}Kpr_cliente}}K}

Para eficiencia, la firma en un mensaje consiste de la solicitud y el hash de la solicitud encriptada con la llave privada del firmante:

   {solicitud, {H(solicitud)}Kpr}

El algoritmo simétrico usado es triple DES en modo CBC. El algoritmo hash (SHA) es usado para ejecutar una función hash.

Después de que el banco ha firmado las monedas anónimas, y es cargado el importe a la cuenta del usuario, son regresadas al usuario. La respuesta de retiro es firmada por el banco. El mensaje no es encriptado porque sólo el cliente conoce el factor anónimo y puede hacer no anónimas las monedas para después gastarlas.

Una Compra Ecash

El cliente almacena las monedas en el cyberwallet, el gasta esas monedas con un vendedor. El cliente decide que artículos comprar y coloca la orden con el vendedor. Este quizá envíe una forma al Web Site del vendedor.

Habiendo recibido una orden, el vendedor envía una solicitud de pago al cyberwallet del cliente. Este mensaje contiene detalles acerca de la cantidad de la orden, la moneda a ser usada, la hora actual, el banco del vendedor, el ID de la cuenta del vendedor en el banco, y la descripción de la orden

```
PagoReq = {moneda, cantidad, timestamp, BancoVendedorID, VendedorAcctId, descripción}
```

La solicitud es enviada en claro, la cual quizá permita a un intruso ver que está siendo ordenado y por cuanto

La cartera del cliente presenta al usuario esta información, preguntando si desea hacer el pago. El cyberwallet quizá también sea configurado para hacer pagos automáticamente para vendedores específicos o específicas cantidades. Si el usuario decide pagar, el valor de las monedas es solicitado y las cantidades son juntadas desde la cartera. La cantidad exacta debe ser enviada al vendedor porque aceptando el cambio podría comprometerse la anonimidad del usuario (el vendedor podría registrar los números de serie del cambio y coludir con el banco para revelar la identidad del usuario). El cyberwallet automáticamente reúne las cantidades correctas y puede retirar nuevas monedas del banco y más denominaciones son requeridas.

Haciendo el Pago

Las monedas usadas en el pago son encriptadas con la llave pública del banco (Kpu_{Banco}) antes de ser enviadas al vendedor. Este los previene de que sean robadas en el tránsito y que el vendedor sea capaz de examinarlas o entrometerse. El vendedor envía las monedas al banco para depositarlas en su cuenta. El mensaje de pago, es enviado al vendedor y después es enviado al banco, consiste de información acerca del pago y las monedas encriptadas:

```
Pago = {PagoInfo, {monedas} Kpu_Banco }
```

La información del banco incluye detalles acerca del banco, la cantidad, moneda, número de monedas, hora actual, y los IDs del vendedor entre otras cosas

```
PagoInfo = {BancoID, cantidad, moneda, nmonedas, timestamp, VendedorIDs, H(descripción),
           H(CódigoPagador)}
```

La información del pago es enviada al banco junto con las monedas encriptadas, durante el depósito del vendedor. Un hash de la descripción de la orden es incluido con la información de pago. Desde que el vendedor ya conoce la orden, puede comparar este valor con un hash o su copia de la orden, para verificar que el cliente está de acuerdo exactamente con lo que está siendo comprado. Cuando la información de pago es enviada al banco, no puede saber que está siendo comprado, sólo un hash de la orden es incluido

CódigoPagador es un secreto generado por el cliente. Un hash de éste, H(CódigoPagador) es incluido en la información de pago así que el cliente puede comprobarlo después al banco, después de que el vendedor ha depositado las monedas, él hace el pago. El banco registrará que el vendedor depósito un pago que contiene el H(CódigoPagador). Si el cliente revela el CódigoPagador, el banco puede estar seguro que el creador del CódigoPagador ha hecho el pago.

Sin embargo, para este trabajo, el banco necesita asegurarse que PagoInfo no fue comprometido entre la hora en que el cliente lo dejo y la hora en la que el vendedor lo depósito en el banco. Si esto pudo ser alterado, el valor del H(CódigoPagador) podría ser cambiado. Para prevenir esto, un hash del PagoInfo es incluido con las monedas antes de que sean encriptadas

```
{Monedas, H(PagoInfo)} Kpu_Banco
```

Cuando el banco recibe el pago, este genera su propio hash de PagoInfo. Si son iguales los valores encriptados con kpubanco, los cuáles sólo pueden ser decriptados, entonces nos aseguramos que el mensaje no fue alterado. El mensaje de pago es ahora:

$$Pago = \{PagoInfo, \{Monedas, H(PagoInfo)\}Kpu_{banco}\}$$

El pagador permanece anónimo, al menos de que él decida proveer el pago. El tenedor no es anónimo como debe depositar las monedas e identificar la información de pago construida por el cliente

Depósito de Pago

Al recibir el mensaje de pago, el vendedor lo envía al banco como parte de la solicitud de depósito.

$$Deposito = \{\{Pago\}Sig_V\}PK_{banco}$$

El depósito quizá opcionalmente sea firmado por el vendedor y encriptado con la llave pública del banco. El banco verifica que las monedas no hayan sido ya gastadas y acredita la cuenta del vendedor. Una indicación de éxito es regresada al vendedor

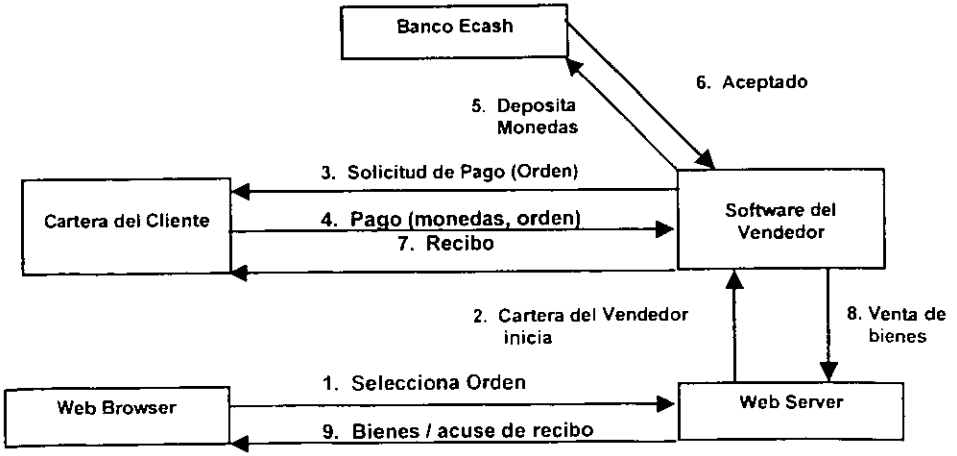
$$DepositoAck = \{resultado, cantidad\}Sig_{banco}$$

El formato del mensaje de depósito similar puede ser usado por un cliente para regresar las monedas sin gastar al banco.

Habiendo recibido el pago de un bien, el vendedor quizá regrese el artículo de compra o recibo al cliente. Si el vendedor falla, el cliente puede probar que el pago fue hecho y aceptado para revelar el CódigoPagador.

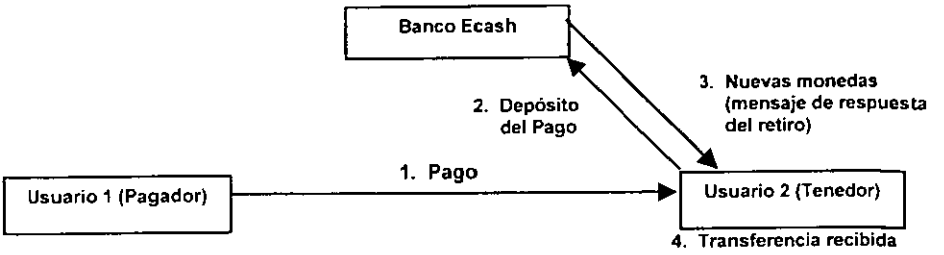
Usos de Ecash

a) Ecash en el Web: El cliente corre el cyberwallet y navega en el Web. Cuando una orden es seleccionada desde una página Web del vendedor, el software Ecash del vendedor es automáticamente iniciado por un CGI (Common Gateway Interface / Interfaz de Entrada Común). El CGI simplemente provee un medio para correr programas de un Servidor Web y permite pasar los resultados a través del servidor. El software del vendedor procede con la compra Ecash. Si el pago fue exitoso, el artículo o la indicación de la compra quizá sean regresados a través del Web al browser del cliente. Este método tiene la ventaja de que puede ser fácilmente integrado con la mayoría de los Web browser y los servidores.



b) Ecash en el Mail: El vendedor contacta al banco a través de un e-mail, para depositar las monedas y prevenir el doble gasto antes de entregar los bienes.

c) Transfiriendo Ecash: La transferencia Ecash de usuario a usuario es posible, aunque la cantidad transferida todavia tiene que ser enviada al banco para verificación. Utiliza el mismo protocolo de intercambio que en una compra. Las monedas son enviadas a través del banco del tenedor donde son depositadas. Nuevos valores de monedas con la misma cantidad son regresadas al tenedor. Esto se hace de manera transparente así que aparece que las nuevas monedas son recibidas directamente desde el pagador. Ambos usuarios deben tener cuenta en el mismo banco Ecash.



Monedas Perdidas

Para recobrar las monedas, el cliente que ha perdido las monedas notifica a la casa de moneda del banco su pérdida. El banco envía mensajes exactos desde el último retiro n al cliente. Actualmente n=16, así que las monedas anónimas firmadas desde los últimos 16 retiros son enviadas.

El cliente debe tener todavía el factor de anonimato usado para esos retiros, de otra manera las monedas no pueden dejar de ser anónimas. La cartera del cliente obtendrá las monedas y las depositará en la cuenta del banco del cliente. Es necesario depositar las monedas porque no se sabe cuales monedas de los últimos 16 retiros han sido gastadas ya o no. Esta es la verificación normal para prevenir el doble gasto. La cuenta del cliente acreditará la cantidad no gastada. El valor de algunas monedas perdidas habrá sido recobrado y el cliente podrá retirar las nuevas para gastar.

Como cometer el crimen perfecto y obtener monedas anónimas:

- Secuestrador anónimo toma un rehén
- El secuestrador prepara un gran número de monedas anónimas. Son enviadas anónimamente al banco como una demanda de rescate
- El banco firma las monedas debido a la situación del rehén.
- El secuestrador demanda que las monedas anónimas firmadas sean publicadas en un lugar público tal como el periódico o la televisión. Este previene recoger las huellas. Nadie más puede recuperar las monedas.
- El secuestrador puede seguramente tomar las monedas anónimas desde el periódico o la televisión y guardarlas en la computadora. Las monedas son recuperadas y el secuestrador tiene una fortuna en dinero digital.

Procedimiento de Compra por Internet (Ecash)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
1.	**Obtención de CyberWallet o monedero electrónico**	comprador									
1	Obtiene CyberWallet.										
.2	Almacena monedas retiradas desde su cuenta con el banco Ecash.										
2.	**Ingreso a Internet**	comprador									
1	Ingresa a Internet.				20	*					
2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	comprador									
1	Entra a la tienda virtual				5	*					
2	Busca el artículo a adquirir			5		*			*		
3	Selecciona el artículo				5	*					
4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	comprador									
1	Se va al botón de nuevo				5	*					
2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	comprador									
1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	comprador									
1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	vendedor									
1	Checa que los campos tengan datos.				5		*				
2	Muestra los datos ingresados.				5	*					
8.	**Elección de la dirección**	comprador									
1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
9.	**Muestra datos del cliente y del artículo**	vendedor									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	*			*		
10.	**Asignación de una cantidad del artículo**	comprador									
1	Asigna una cantidad de compra.				5	*				*	
11.	**Señalización de las formas de envío**	vendedor									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)				5	*		*			
12.	**Elección de forma de envío**	comprador									
1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	
13.	**Indica las formas de pago**	vendedor									
1	Pide password y su confirmación.				5	*					
2	Menciona los procesos de pago.					*		*			
14.	**Selección de un método de pago**	comprador									
1	Ingresa password y confirmación.				30	*	*				
2	Selecciona el método de pago				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Envío de una solicitud de pago**	**vendedor**									
1	Envía una solicitud de pago al monedero del cliente, contiene la descripción de la orden, identificadores, etc										
16.	**Realización del pago**	**comprador**									
1	Al pagar el comprador debe solicitar el valor de las monedas										
2	Envía la cantidad exacta encriptada al vendedor, e información del pago y de la orden de compra										
17.	**Depósito de las monedas**	**vendedor**									
1	El vendedor envía las monedas, información del pago y de la orden de compra al banco										
2	El banco deposita las monedas en la cuenta del vendedor	**Banco Ecash**									
18.	**Registro del pago**	**Banco Ecash**									
1	Registra el depósito realizado										
2	Envía una respuesta de aprobada la transacción										
19.	**Envío de respuesta de la transacción**	**vendedor**									
1	Envía la respuesta al comprador de que la transacción se ha concretado.										
20.	**Muestra de la orden de compra**	**vendedor**									
1	Despliega la información total de la compra.				5	*			*		
21.	**Envío del producto**	**vendedor**									
2	Envía el producto		25					*	*		
22.	**Recepción del producto**	**comprador**									
1	Recibe el producto		700			*					

3.3.2 Proyecto CAFE

CAFE (Acceso Condicional para Europa / Conditional Acces For Europe) fue un proyecto fundado por el programa ESPRIT de la Comunidad Europea. Inicio en 1992, programado para una duración de tres años. El objetivo del proyecto fue desarrollar un sistema general para administrar derechos a los usuarios

Los protocolos CAFE están basados en la idea de dinero electrónico, propuesta por David Chaum y el concepto de cheques con contadores. CAFE es un esquema híbrido que ofrece todos los beneficios del dinero electrónico anónimo, pero al mismo tiempo permite al usuario firmar cheques por una especifica cantidad.

El objetivo de CAFE es que fue diseñado para ser universal, prepagos, sistema de pagos fuera de línea con seguridad multipartes

Las caracteristicas del sistema son:

- Segundad multiparte: La mayoria de los sistemas proveen la seguridad de un solo lado La seguridad de cada entidad en el sistema es garantizada sin la necesidad de confiar en una tercera parte. Esto implica que cada parte debe ser capaz para confiar en el dispositivo que están usando También, los procedimientos y algoritmos usados en el protocolo deben ser abiertos y disponibles para inspección de todos.

- Pagos fuera de línea: No hay necesidad para un tenedor (vendedor) contactar una base de datos central, usualmente mantenida por monedas electrónicas emitidas, en el tiempo de la compra Este reduce el costo de mantener/ establecer una canal de comunicación entre dos

- Detección de doble gasto: Son confiables dispositivos para prevenir las intromisiones proveen la seguridad básica del sistema. Sin embargo si está bajo circunstancias extremas la resistencia a las intromisiones de un dispositivo es rota, el doble gasto puede tomar lugar. Los protocolos criptográficos diseñados para tal doble gasto serán detectados con muy alta probabilidad. Esta detección es lograr que el costo de mantener una base de datos de recientes pagos por instituciones financieras.

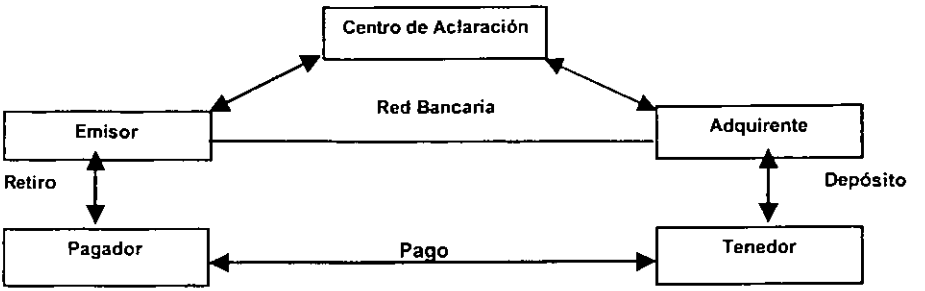
- Pagos sin intromisión: Bajo circunstancias normales, los pagos no pueden ser ligados al usuario si hay colaboración entre vendedores y bancos. La identidad de un usuario es, sin embargo, revelada si se hace el doble gasto de un pago. Como con un procedimiento de banco actual, la identidad del tenedor no es protegida

La arquitectura del sistema es

- Pagador (cliente): es equipado con un dispositivo resistente a los intrusos tal como una smart card o una cartera electrónica, la cual es usada para almacenar las monedas electrónicas y hacer los pagos.

- Tenedor (vendedor): recibirá pagos electrónicos desde los clientes en intercambio de bienes o servicios. Depositará los pagos en su banco para aclaramientos

- Banco El rol de un banco puede ser dividido en emisor/adquirente de moneda electrónica El emisor carga las monedas electrónicas dentro de la cuenta del cliente, y se asegura que la cantidad correcta sea cargada desde la cuenta del cliente. El adquirente acepta el depósito desde el vendedor y los aclara a través de canales de aclaración interbancaria



En CAFE usamos dispositivos para almacenar monedas electrónicas por el usuario, ejecutar operaciones criptográficas y hacer el pago a los vendedores

- Smart Card (Tarjeta Inteligente): Similar a una tarjeta de crédito y tiene un microprocesador empotrado con energía de un dispositivo externo. Toda la información es almacenada en un chip, el cual ejecuta computaciones criptográficas. Se refieren como el sistema alfa α
- Carteras: Consiste de dos partes: un observador y protege los intereses del banco y el otro es conocido como el monedero y protege los intereses del usuario. El monedero incluye un teclado. Este además protege al usuario como puede entrar su PIN en el monedero y no tener que confiar en un dispositivo de una tercera parte. Además, todas las comunicaciones entre la cartera y el mundo exterior son hechas exclusivamente a través del monedero, garantizando que un observador no puede divulgar ninguna información secreta al banco sin el conocimiento del usuario.
- Dos botones cartera (+): Consiste en dos botones del teclado y una pantalla digital. El módulo observador es implementado como una smart card que también ejecuta transacciones. El monitor del monedero, verifica, y confía toda la comunicación desde la smart card vía una interfaz de infrarrojos para la terminal del pago. El sistema alfa + es completamente compatible con el sistema alfa.
- Cartera completa: La cartera completa tiene un teclado numérico completo y una pantalla más grande que es usada en el dispositivo. El teclado completo también permite ingresar cantidades y PINs. El observador es implementado como un microprocesador construido en una smart card. No como en la smart card del sistema, el observador exclusivamente protege los intereses del banco. La cartera usa una versión adaptada de protocolos en el sistema y asegura mejor su privacidad para el usuario. El sistema de cartera completa es llamada el sistema (gamma) y es compatible con los sistemas y. En adición, éste tiene un slot (ranura) dentro del cual una smart card puede ser insertada y el dinero puede ser transferido

Los observadores son implantados dentro de una smart card para proteger los intereses de instituciones financieras. Un usuario no es capaz de completar una transacción de pago exitosamente sin la cooperación de un observador. Los vendedores no aceptaran los pagos que no sean autonzados por observadores certificados. Un observador aprueba cada pago en una manera similar creando una firma digital, la cual no muestre la identidad del observador o el usuario.

Seguridad

1. Usa dispositivos resistentes a intrusos para almacenar llaves criptográficas y para ejecutar transacciones criptográficas
2. Protege contra el doble gasto por medio de un mecanismo criptográfico fallback que permite a las instituciones financieras detectarlos, y también por medio de una lista negra de usuarios sospechosos. Los bancos distribuyen esas listas para todos los vendedores en el sistema

Monedas Fuera de Línea

Las monedas fuera de línea son donde la identidad del pagador es codificada dentro del número de la moneda, que es construido desde dos partes. Cuando la moneda es usada en una transacción de pago, el pagador debe revelar una parte de la moneda. Si la misma moneda es usada nuevamente, el usuario tendrá que revelar la segunda parte de la moneda. La moneda es construida de tal manera que revelando una sola parte de la moneda no identificará al pagador, pero si la moneda es gastada nuevamente, la identidad del pagador es revelada.

I Identidad del usuario, puede ser encriptada con un número aleatorio P
P Número aleatorio

La moneda consiste de dos partes:

1. Contiene la identidad encriptada I ⊕ P
2. La otra parte contiene la llave P

Cada parte es además encriptada con un esquema de encripción para producir C(I⊕P) y C(P). En una transacción de pago

En una transacción de pago, el pagador tendrá que adquirir un compromiso, el cual será también I ⊕ P o P, el cual no revela la identidad del pagador. Sin embargo, la otra parte es abierta, entonces la identidad del pagador será encontrada. Para detectar el doble gasto, un banco mantiene una base de datos de todas las monedas depositadas recientemente y busca su correspondiente par antes de aclarar la transacción de pago

Protocolo Alfa

Conjunto de protocolos usados por una smart card. Hay un número de rangos de retiros de monedas electrónicas para recuperar valores de tarjetas perdidas

a) Retiro

Un pagador usualmente sólo necesita comunicarse con el banco a través de una sesión de retiro, la cual resulta de un número de tickets en blanco de los pagos electrónicos cargados en la smart card. El banco guarda la trayectoria del balance en la tarjeta por medio de un contador en la parte del observador en la smart card. El balance es actualizado durante una solicitud de retiro y la cantidad correspondiente deducida desde la cuenta del banco del usuario. Una sesión de retiro consiste de:

1 La smart card del usuario envía la identidad de su banco y la información acerca de su certificado de llave pública del banco a la terminal. Este permite a la terminal conectarse para correcciones bancarias y verificar/actualizar el certificado de llave pública del banco almacenado en la smart card

2. La tarjeta y el banco mutuamente se autentican el uno al otro a través de la terminal. La tarjeta genera un número aleatorio y lo envía al banco. El banco firma éste con su llave secreta y regresa la firma. La tarjeta verifica la firma usando la llave pública del banco. La tarjeta regresa la autenticación de sí misma firmando una cantidad aleatoria enviada por el banco. En adición, también envía un snapshot (impresión) de su tabla de monedas (Contadores). El banco verifica la firma

3 Para asegurar que el banco pueda identificar los pagos duplicados, una llave pública (Kpu_{ID}) derivada desde la llave secreta del usuario ($K_{Usuario}$) es incorporada dentro de los tickets de pago. Para proteger la identidad del usuario, la tarjeta oculta este valor

Un ticket de pago consiste de:

1 Kpu_{Blinds} la cual es la versión anónima de Kpu_{ID}. Este valor también sirve como un ticket identificador

2. Dos llaves públicas auxiliares de una vez Kpu_1 y Kpu_2 , las cuales no son conocidas en el banco.

El proceso de obtener un ticket de un pago en blanco desde un banco, inicia cuando el usuario genera un ticket de pago y envía el hash H(PagoSlip) de éste al banco. El banco crea una firma digital (Sig_{Banco}) en el hash que envío. La firma es unida al ticket de pago con la dos llaves públicas de una sola vez. El usuario necesita sólo almacenar la firma del banco en la tarjeta, como todos los otros valores pueden ser regenerados por él en el estado de pago. Esto permite el almacenamiento eficiente de los tickets de pago.

b) Pago

Consiste en que el usuario llene una cantidad dentro de un recibo de pago en blanco junto con el nombre del tenedor, firmado con la llave secreta del usuano. Actúa de la siguiente manera:

- Un cliente inserta su tarjeta dentro de la terminal (pago) del vendedor. La terminal le dice a la tarjeta la identidad del tenedor, la fecha, la cantidad a ser deducida desde la tabla de monedas, entre otros. Esta información es codificada por la tarjeta dentro del recibo de pago (M).
- La tarjeta regenera el siguiente recibo de pago a ser usado. Este consiste de la generación de cantidades secretas y las llaves públicas de un solo uso. Esto es lo que consume la mayor parte del protocolo, y usualmente hecho en el background, mientras que los parámetros de pago están siendo negociados por el usuario y el vendedor.
- La tarjeta envía el recibo de pago en blanco al vendedor, consistiendo de la firma del banco y las llaves públicas necesitadas para usar el recibo (Kpu_1 y Kpu_2 donde i= 1 ó 2 dependiendo si el recibo está siendo usado por primera o segunda vez). El recibo de pago es marcado como que está siendo gastado por la tarjeta, cuando pensamos que el pago aún no ha sido completado.
- La terminal verifica la firma del banco del recibo de pago en blanco.
- La tarjeta prepara un mensaje correspondiente al contenido del recibo de pago. Contiene los siguientes campos:
    1. Las llaves públicas del recibo de pago Kpu_{Blind}(identidad del recibo) y Kpu_i
    2. ID del vendedor
    3. Fecha
    4. Cantidad
    5. Cadena aleatoria para asegurar que el mensaje es único

  El mensaje está firmado con la llave secreta del usuario ($SK_{Usuario}$) y la cadena aleatoria usada para generar el recibo de pago. Este resulta en una firma digital $SK_{Usuario}$
- La terminal verifica que el pago tiene la forma apropiada. Esto se hace junto con el recibo de pago en blanco enviado previamente.

Cuando el pago ha sido finalizado, la terminal envía un conocimiento a la tarjeta. La tarjeta actualiza sus contadores.

c) Depósito

Una vez aceptado el recibo de pago, el tenedor lo envía al adquirente (con una fecha posterior) quien lo regresa aclarado a través del sistema financiero de aclaramiento. El adquirente:

- Verifica el contenido del recibo de pago y válida la firma del banco.
- Verifica que el recibo de pago no ha sido depositado previamente.
- Busca un par igual de Kpu, en su base de datos para verificar que la parte correspondiente del pago no ha sido gastada previamente.

Si las primeras dos condiciones son completas, el tenedor tiene derecho a ser acreditado por la cantidad del pago. Un tenedor es responsable para checar todos los recibos de pago recibidos, contra sus copias locales de lista negra durante el protocolo de pago. Si un recibo es detectado en la lista negra, el tenedor aborta la transacción. Si un tenedor falla para verificar los recibos de pago recibidos contra la lista negra, entonces él tendrá que aceptar la responsabilidad de ellos como un centro de aclaramiento para rechazarlas. Cuando el centro de aclaramiento detecta un doble gasto, el recibo de pago inmediatamente se agregará a la lista negra.

Protocolo Gamma

Son extensiones modulares del sistema Alfa. La cartera consiste de un monedero que es capaz de ejecutar criptografía de llave pública. Todas las comunicaciones entre el observador y el mundo externo toman lugar vía el monedero. Este provee seguridad adicional para el usuario, como el monedero, ocultará y neutralizará alguna comunicación que quizá revele información secreta acerca del usuario al mundo exterior. Es capaz de sostener más recibos de pago que una tarjeta inteligente. Un usuario es también capaz de transferir un valor desde su cartera Gamma a su smart card Alfa.

Características adicionales:

- Múltiples monedas: Permite utilizar diferentes monedas tal como el efectivo actual, el usuario quizá intercambie monedas al banco (baja la cantidad en el bolsillo e incrementa algún otro) o pago en moneda no local si el vendedor lo acepta.
- Fault y Loss Tolerance: Si un usuario pierde su cartera el banco puede recobrar el dinero desde el respaldo y depositar los transcripts. Es hecho por respaldos regulares dentro de las transacciones de retiro. Si un usuario quiere recobrar las monedas perdidas, revela la identidad del recibo de pago almacenado después del último retiro. Este habilita al banco para rastrear esos recibos de pago.

Procedimiento de Compra por Internet (CAFE)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de dispositivo de almacenamiento de monedas.**	comprador									
.1	Obtiene dispositivo (smart card).										
2.	**Retira dinero del banco**	comprador									
.1	Se comunica al banco mediante una sesión de retiro.										
.2	El banco guarda la trayectoria del balance de la tarjeta de crédito en un observador de la smart card.	banco									
.3	Actualiza el balance y deduce la cantidad solicitada desde la cuenta bancaria del comprador.										
3.	**Ingreso a Internet**	comprador									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
4.	**Selección del artículo a adquirir**	comprador									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
5.	**Alta de dirección e-mail de un cliente**	comprador									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
6.	**Ingreso de dirección e-mail del cliente**	comprador									
.1	Ingresa dirección e-mail				10	*				*	
7.	**Ingresa sus datos el cliente**	comprador									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
8.	**Verificación del llenado de los datos**	vendedor									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados.				5	*					
9	**Elección de la dirección**	comprador									
.1	Tiene que elegir la dirección a la cual quiere que se le envie el producto.				5	*					
10	**Muestra datos del cliente y del artículo**	vendedor									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envio.				5	*			*		
11	**Asignación de una cantidad del artículo**	comprador									
.1	Asigna una cantidad de compra.				5	*				*	
12	**Señalización de las formas de envio**	vendedor									
.1	Da las diferentes formas de envio y una breve descripción (Nacional/Internacional).				5	*		*			
13	**Elección de forma de envio**	comprador									
.1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
14	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación.				5	*					
.2	Menciona los procesos de pago.					*		*			
15	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación.				30	*	*				
.2	Selecciona el método de pago.				5	*				*	
16.	**Realización del pago**	**comprador**									
.1	El comprador inserta su smart card dentro de la terminal de pago del vendedor.										
.2	La terminal pide información a la tarjeta sobre la identidad del tenedor entre otros.	**tenedor**									
17.	**Emisión de un recibo**	**vendedor**									
.1	La smart card genera un recibo.	**smart card**									
.2	Envía el recibo de pago en blanco al vendedor, firmado.										
18.	**Registro del pago**	**tenedor**									
1	Marca el recibo de pago indicando como que está siendo gastado.										
2	Verifica las firmas del banco.										
3	La smart card genera un mensaje con el del recibo de pago.	**smart card**									
4	Lo envía a la terminal.										
5	La terminal verifica que el mensaje de pago tenga la forma apropiada.	**tenedor**									
.6	Envía el recibo de pago al adquirente.										
19.	**Aclaración del pago**	**adquirente**									
.1	Verifica el contenido del recibo y válida firmas.										
2	Verifica que el recibo no se ha depositado previamente.										
3	Lo envía al tenedor.										
20.	**Envío de respuesta de la transacción**	**tenedor**									
1	Envía la respuesta a la smart card de que la transacción se ha concretado.										
21.	**Actualización de los contadores de la Smart Card**	**smart card**									
.1	Actualiza sus contadores.										
22.	**Muestra de la orden de compra**	**vendedor**									
1	Despliega la información total de la compra.				5	*			*		
23	**Envío del producto**	**vendedor**									
.2	Envía el producto.		25					*	*		
24	**Recepción del producto**	**comprador**									
1	Recibe el producto.		700			*					

3.3.3 NetCash

Sistema de pago desarrollado por el Instituto de Ciencias de Información de la Universidad del Sur de California. Consiste en distribuir servidores de monedas que emitan monedas electrónicas, y las emitan a usuarios de este sistema, aceptando cheques electrónicos en pago por ellas. El sistema es online, cada moneda debe ser verificada si es válida, y sino se ha gastado para enviarla al servidor casa de moneda para la verificación durante la compra. Aunque el dinero digital es identificado, con cada moneda teniendo un número de serie único, hay un mecanismo de intercambio para proveer anonimato limitado. Alguien con monedas válidas puede intercambiarlas anónimamente de un servidor de monedas a otro.

Sistema de macropagos apropiado para la venta de bienes, información y otros servicios de red. Los usuarios pueden realizar y aceptar pagos. Esta es una solución de software que no requiere un hardware especial, usa criptografía simétrica y asimétrica para proveer seguridad en la red del sistema y prevenir los fraudes. Todas las partes deben tener su par de llaves pública y privada (Kpu_X, Kpr_X). El uso de múltiples servidores moneda permite al sistema ser escalable, esto es, para manejar usuarios adicionales y usarlo sin causar daños a la ejecución.

Modelo/Estructura

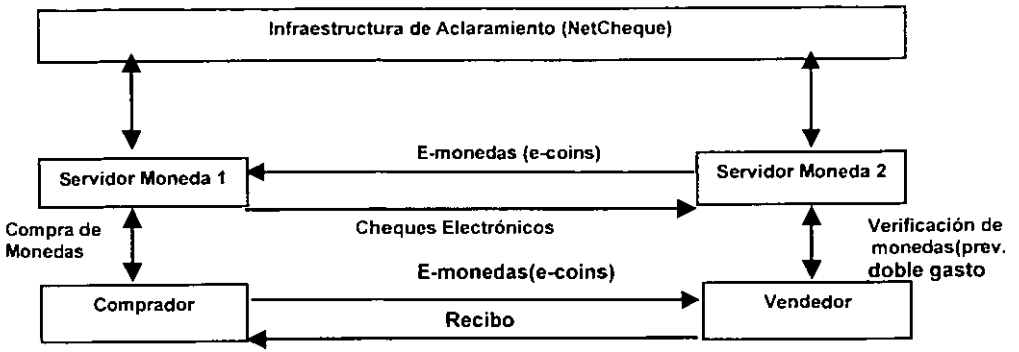
Las partes involucradas son compradores (clientes), vendedores y servidores moneda (SM). El SM provee los siguientes servicios (compradores, vendedores)

- Verificación de monedas, para prevenir el doble gasto
- Emisión de monedas para regresar pagos por cheque electrónico.
- Comprar monedas, dando un cheque electrónico de vuelta.
- Intercambio de monedas válidas por nuevas, las cuales proveen cierto anonimato.

NetCheque es el sistema propuesto para proveer una infraestructura de cheques electrónicos requerida para traer valores monetarios dentro y fuera del sistema NetCash. No solo los clientes pueden comprar y vender monedas NetCash en intercambio de cheques electrónicos, sino que los servidores NetCash pueden usar cheques electrónicos para poner deudas entre ellos mismos.

Cuando un comprador está haciendo una compra desde un negocio, ambas partes quizá usen diferentes servidores de moneda. El comprador quizá compre monedas desde el servidor de monedas (SM_1), pero el vendedor quizá quiera verificar las monedas a través de su servidor (SM_2). Las monedas pueden ser al final verificadas por el servidor de moneda que las emitió. SM_2 tendrá que enviar las monedas recibidas desde el vendedor a SM_1 para ser verificadas. Al regresar válidas monedas, SM_1 generará un cheque electrónico para SM_1. SM_2 puede emitir nuevas monedas para el vendedor o enviar un cheque electrónico en intercambio por las monedas válidas emitidas por SM_1. Todos los cheques pueden ser aclarados a través de una cuenta NetCheque y una infraestructura de aclaramiento. Mientras NetCheque propone el mecanismo de aclaramiento, es concebible que algún otro esquema de cheque electrónico o infraestructura de aclaramiento pueda ser usada.

Si SM_2 indica al vendedor que las monedas fueron válidas, un receptor y/o la compra de los bienes pueden ser regresados al comprador.



Una moneda electrónica NetCash es una pieza de datos que representa el valor monetario dentro de un sistema de dinero electrónico. Cada moneda es emitida por un servidor moneda y tiene un número de serie único para ese servidor, contiene

```
Moneda  {Csname, Csaddr, Expira, #Serie, Valor} SK
```

Cada moneda es encriptada con la llave secreta del servidor que las emitió (SK). Esta forma una firma digital que muestra que es auténtica. En las implementaciones actuales, para improvisar la eficiencia, la firma digital quizá esté formada para aplicar un hash de los campos de la moneda y encriptar el resultado con la llave secreta del servidor. Sería más eficiente que encriptar todos los campos sin aplicar la función hash. Los campos son:

Dato	Descripción
Csname	Nombre del servidor que emitió la moneda. Si Csaddr es inválido, esté podría ser usado para buscar la dirección actual de red del servidor en un directorio público.
Csaddr	Dirección de red del servidor emisor de moneda.
Expira	Fecha en la cual una moneda expira y ya no es aceptada como una moneda válida. El propósito de este campo es limitar la cantidad de números de serie, que deben ser recordados por un servidor de moneda para prevenir el doble gasto.
#Serie	Identificador único de la moneda para el servidor emisor de la moneda.
Valor	El valor de la moneda.

Prevención del doble gasto

Para la prevención del doble gasto un servidor de monedas debe tener una lista de números de serie de cada moneda emitida que se encuentre en actual circulación.

Durante la compra, el tenedor verificará que las monedas no hayan sido gastadas dos veces, regresándolas al servidor emisor. El SM checa que el número de serie de la moneda esté presente en la base de datos. Si es así, la moneda es válida. El número de serie debe ser removido desde una base de datos y la moneda será reemplazada con un número de serie (o un cheque electrónico). El nuevo número de serie será registrado en la base de datos y la moneda será regresada al pagador.

Una moneda puede ser válida sólo para una compra. Si fue abandonada en circulación, no hay manera de distinguir que realmente ya se gasto. Si un número de serie de la moneda no aparece en la base de datos, entonces tuvo que ser gastada anteriormente o removida o quizá expiro. Los números de serie que han

expirado quizá sean removidos de la base de datos para limitar su tamaño y permitir que los números sean reusados.

Transferencia de monedas

El valor monetario puede ser intercambiado entre individuos pero, con una compra básica, el servidor emisor necesita ser contactado para prevenir el doble gasto. Donde los individuos confían el uno en el otro no hay doble gasto de monedas, pueden ser transferidas directamente. Eventualmente, todas las monedas tendrán que ser regresadas al servidor que las emitió para verificarlas antes de que expiren.

Certificado de Seguridad

Sólo los servidores que emiten monedas pueden tener un certificado y tienen dos funciones:

1 Un medio de distribución de la llave pública del servidor (Kpa) de manera segura, firmada y verificada por una tercera parte confiable. Esta llave es usada para verificar la firma en una moneda y encriptar mensajes enviados al servidor.
2 Provee que una tercera parte llamada Corporación Federal Aseguradora (FIC/ Federal Insurance Corporation), provee seguridad para los SM para producir y manejar monedas NetCash. Esto indica que las monedas emitidas por este servidor pueden ser aceptadas como una oferta legal.

El certificado contiene

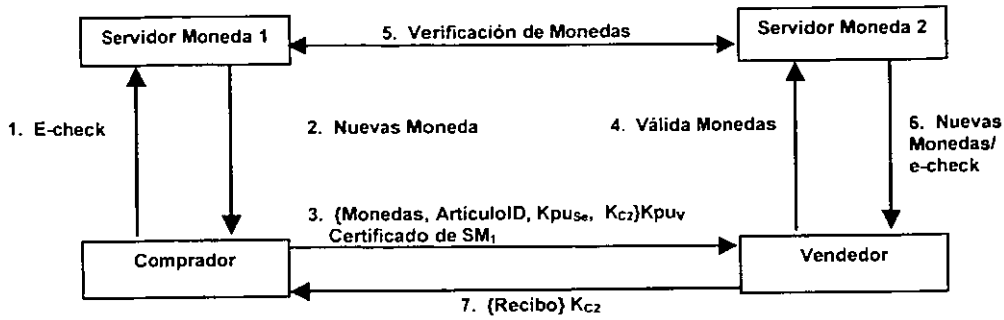
[illegible]

Dato	Descripción
CertID	Identificador único del certificado.
Cname	Nombre del servidor que emitió la moneda.
Kpa	Llave pública del SM.
FechaEmite	Fecha desde la cual el certificado es válido.
Expira	Fecha en la cual el certificado expira y no es válido.

El certificado es digitalmente firmado con la llave secreta de FIC, la cual actúa como una autoridad certificadora (AC). Algún comprador o vendedor que contacte un SM directamente necesitará obtener el certificado del servidor.

Compra básica

El comprador debe obtener monedas desde un SM, comprándolas con un cheque electrónico. Algunas de las monedas compradas son enviadas al vendedor en pago por un artículo. Para proteger contra el doble gasto, el vendedor verificará las monedas, directamente con el servidor emisor de monedas o indirectamente a través del servidor de su elección. En cambio para una moneda válida, el vendedor puede recibir nuevas monedas, emitidas por el servidor que él ha contactado o por un cheque electrónico. Un recibo firmado desde el vendedor, y posiblemente el artículo comprado, quizá entonces sean enviados al comprador.



Obteniendo Monedas

El usuario envía un cheque electrónico, junto con un número aleatorio generado una vez en la llave de sesión simétrica, encriptada con la llave pública del servidor para el servidor

{Echeque, R }KPs

El mensaje puede ser sólo decriptado y leído por SM_1. El cheque debería ser tal que sólo pueda ser gastado una vez, así que puede repetir el mensaje mientras no logre nada. El servidor regresará nuevas monedas al comprador, encriptadas con la llave de sesión K_C

{Nuevas monedas}K

El intercambio con el servidor puede ser generalizado, así que también un cheque o monedas pueden ser intercambiadas con el servidor por unas nuevas monedas o un cheque. Obviamente, un cheque no es intercambiado nunca por otro cheque. La solicitud generalizada es:

{Instrumento, K, Trans } Ps

donde Instrumento es un cheque electrónico o moneda, K, es una llave de sesión generada por el emisor X (comprador o vendedor), y Trans indica si se quiere intercambiar por nuevas monedas o por un cheque. Una respuesta exitosa es simplemente el Instrumento deseado (monedas o cheque), protegidos por la llave de sesión.

{Instrumento}K

Ese mensaje puede ser usado anónimamente para intercambiar monedas con un servidor

Pagando a un vendedor

El comprador envía una solicitud de compra al vendedor, encriptada con la llave pública del vendedor (Pv)

{Moneda, ArticuloID, Ppa , R }Pv , {Certificado de SM}

El comprador debe seguramente obtener Pv antes de que la compra tome lugar, se sugiere que esto sea hecho enviando la llave pública del comprador (Pc) al vendedor. El vendedor puede enviar seguramente su llave pública (Pv) al comprador, encriptada con la llave pública el comprador (Pc)

Pv = Pv

Este no es completamente seguro desde que un atacante pueda interceptar Kpu y regresar una llave pública falsa del vendedor:

Kpu, Kpu

Los pagos pueden ser interceptados desde que son encriptados con la llave pública del atacante. Más seguridad significa distribuir las llaves públicas, usando certificados, que podrían ser usados para frustrar el ataque. Los campos de solicitud de la compra son:

Dato	Descripción
Monedas	La cantidad de la compra en monedas NetCash.
ArtículoID	Identificador del artículo que el comprador desea comprar.
Kpu	Llave pública de una sesión generada recientemente. Después de una compra exitosa, quizá sea usada para encriptar los bienes de compra o el único identificador del comprador. Si el comprador no desea permanecer anónimo al vendedor, ésta podría ser la llave pública normal del comprador Kpu.
K	Una llave de sesión simétrica generada recientemente. Esta es usada para encriptar las respuestas y debe ser diferentes de K.

Verificación de Monedas

El vendedor verifica la firma usando el certificado del servidor, el cual se incluye en la solicitud. Para verificar que las monedas han sido gastadas doblemente el vendedor las envía, en este caso indirectamente, al servidor emisor SM_1 a través de su servidor preferido SM_2, una solicitud de intercambio es usada:

Monedas, K, Trans)Kpu

K es una llave de sesión simétrica generada por el vendedor. SM_2 envía las monedas a SM_1 para verificación, aceptando un cheque electrónico en el regreso (para validar las monedas). Nuevas monedas emitidas por SM_2 o un cheque, son enviadas al vendedor dependiendo de cual fue solicitada en la transacción:

Nuevas Monedas, Cheque

Finalmente un recibo encriptado firmado por el vendedor, es regresado por el comprador:

Recibo, K

donde

Recibo = E(Cantidad, Trans ID, Fecha, ...)

La firma en el recibo puede ser verificada usando la llave pública del vendedor. La entrega del artículo comprado o servicio está fuera del protocolo NetCash. Sin embargo, el Trans ID, el recibo y Kpu_{SE} pueden ser usados para autenticar y encriptar cuando los artículos son entregados.

Proveyendo anonimato limitado

Cuando un usuario compra monedas desde un SM, el servidor puede registrar el número de serie de las monedas que emite y a quien le fueron dadas. Si el servidor más tarde recibe monedas de un vendedor, un registro de los hábitos de gasto del usuario quizá sea construido. Desde que un usuario puede seleccionar con que servidor puede tratar, quizá escoja que no guarde registros.

El intercambio anónimo de monedas puede ser usado para proveer anonimato. Alguien puede intercambiar monedas válidas anónimamente con el servidor para emitir nuevas monedas. El SM conocerá las direcciones

de red de donde vino la solicitud. Sin embargo, si todas las personas tuvieran PC, la dirección de red quizá fuese buena indicación de donde fue originada la transacción. K_x es una llave de sesión temporal que no identifica al propietario.

Cuando las monedas son intercambiadas de esta manera, quizá el comprador o el vendedor (como parte de la verificación de monedas es quien ejecute el intercambio. Mejor el SM puede mantener registros iguales a los números de serie de las viejas monedas contra las nuevas. Cuando las monedas son eventualmente rescatadas de una verificación, el servidor conocerá quien inicialmente compra las monedas y quien eventualmente comercia con ellas, pero no quien tendrá algunas monedas intermedias. Esto previene al servidor de guardar exactos perfiles de gastos, provee al vendedor no coludir con el servidor. Sin embargo, gastar con un vendedor quien es conocido siempre intercambiando monedas para identificar un cheque, el anonimato quizá sea limitado.

Anonimato del Vendedor

Un vendedor quizá permanece anónimo a un SM usando el protocolo de intercambio anónimo obteniendo nuevas monedas desde las monedas presentadas por el comprador. El comprador permanece anónimo al vendedor, aunque el vendedor conocerá la dirección de red desde la cual se origino la solicitud del comprador. El vendedor puede ser anónimo al comprador con tal que genere y distribuya un par temporal de llaves públicas en vez de usar Kpu_V para cada compra. Esto es quizá no muy práctico desde que las llaves públicas fueron más grandes para generar las simétricas, y esto retrasa la compra. Un recibo desde un vendedor anónimo es también de valor limitado

Previendo Anonimato

Para revocar el intercambio de monedas por unas nuevas, y en lugar de emitir cheques con nombre, un SM puede prevenir estos usuarios anónimos. El servidor puede conocer quien emite las monedas y desde quien esas monedas son recibidas. Compradores y vendedores quizá permanezcan anónimos a cada orden usando el protocolo descrito anteriormente.

Aclaramiento

Cuando SM_1 verifica monedas con el servidor de monedas emisor SM_2 en nombre de un usuario, el SM siempre aceptara un cheque electrónico en intercambio por las monedas. Esto asegura que un servidor sólo emite sus propias monedas al usuario. Al final del dia, un SM puede presentar todos los cheques colectados de ese día desde otros servidores o compradores a su servidor de cuentas, el cual aclarará éstos a través de la infraestructura NetCheque.

Previniendo el fraude del vendedor.

Para prevenir el fraude del vendedor, una moneda es extendida para tener partes especificas del vendedor y el usuario, válidas sólo durante el tiempo específico de las ventanas

Moneda = $\{C_V, C_C, C_X\}$

La idea básica es que la primera parte de la moneda, C_V, pueda sólo ser gastada por el vendedor. Si el vendedor gasta ésta y no hace honor a la compra, el comprador puede obtener pruebas del banco que el vendedor fue pagado usando una segunda parte de la moneda, C_C. C_X, la tercera parte, es una precaución que permite a la moneda ser gastada por alguien si C_V y C_C nunca son usadas dentro de su tiempo válido de ventana

Cada una de esas tres partes contiene toda la información presente en una moneda regular NetCash, tal como el mismo número de serie y el valor de los campos. Esos campos son iguales en las tres partes. Sin embargo, el campo de expiración será modificado en cada una tal que C_V es válida durante el primer tiempo del marco, C_C durante el segundo, y C_X después de que

C_v = {Csname, Csaddr, #Serie, Valor, InfoVendedor, Tiempo + Kpr_v}
C_c = {Csname, Csaddr, #Serie, Valor, InfoComprador, Tiempo + Kpr_c}
C_r = {Csname, Csaddr, #Serie, Valor, Tiempo + Kpr_r}

C_v contendrá información de un vendedor en específico, incluyendo Kpu_v. C_v sólo será aceptada como una oferta legal por el SM, si el tenedor puede proveer el conocimiento de Kpr_v (la cual sólo el vendedor debería conocer) y el tiempo de moneda es dentro de la validación de la ventana especificada dentro de la moneda. El método exacto usado para proveer este conocimiento de Kpr es no dar una especificación NetCash.

C_c contendrá información específica del comprador, tal como Kpu_c, puede ser usada para autenticar al comprador si trata de gastar la moneda durante el segundo tiempo de la ventana, cuando es válida. La tercera parte de una nueva moneda, C_r, la cual es válida durante un tercer tiempo de ventana, no tendrá alguna información adicional o llaves empotradas en éste

Procedimiento de Compra por Internet (NetCash)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de Monedas**	comprador									
1	Debe comprar monedas al servidor de monedas con un cheque electrónico										
2.	**Ingreso a Internet**	comprador									
.1	Ingresa a Internet				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	comprador									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	comprador									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	comprador									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	comprador									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario			5		*				*	
7.	**Verificación del llenado de los datos**	vendedor									
.1	Checa que los campos tengan datos				5		*				
2	Muestra los datos ingresados				5	*					
8.	**Elección de la dirección**	comprador									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto				5	*					
9.	**Muestra datos del cliente y del artículo**	vendedor									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envío				5	*			*		
10.	**Asignación de una cantidad del artículo**	comprador									
1	Asigna una cantidad de compra				5	*				*	
11.	**Señalización de las formas de envío**	vendedor									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)				5	*		*			
12.	**Elección de forma de envío**	comprador									
1	Elige la opción más adecuada conforme a sus necesidades				5	*				*	
13.	**Indica las formas de pago**	vendedor									
1	Pide password y su confirmación				5	*					
2	Menciona los procesos de pago					*		*			
14.	**Selección de un método de pago**	comprador									
1	Ingresa password y confirmación				30	*	*				
2	Selecciona el método de pago				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Envio de una solicitud de compra**	**comprador**									
1	Envia una solicitud de compra, contiene la descripción de la orden, identificadores, las monedas, etc.										
16.	**Verificación de monedas**	**vendedor**									
1	Al obtener las monedas las envia a SM1, a través de SM2, y SM2 acepta un cheque de regreso.										
2	Al ser válidas las monedas le envia un cheque o nuevas monedas al vendedor.										
17.	**Recepción de las monedas**	**vendedor**									
1	Al recibir las monedas, envia un recibo al vendedor.										
18.	**Muestra de la orden de compra**	**vendedor**									
1	Despliega la información total de la compra.				5	*			*		
19.	**Envío del producto**	**vendedor**									
2	Envía el producto.		25					*	*		
20.	**Recepción del producto**	**comprador**									
1	Recibe el producto.		700			*					

3.3.4 CyberCoin

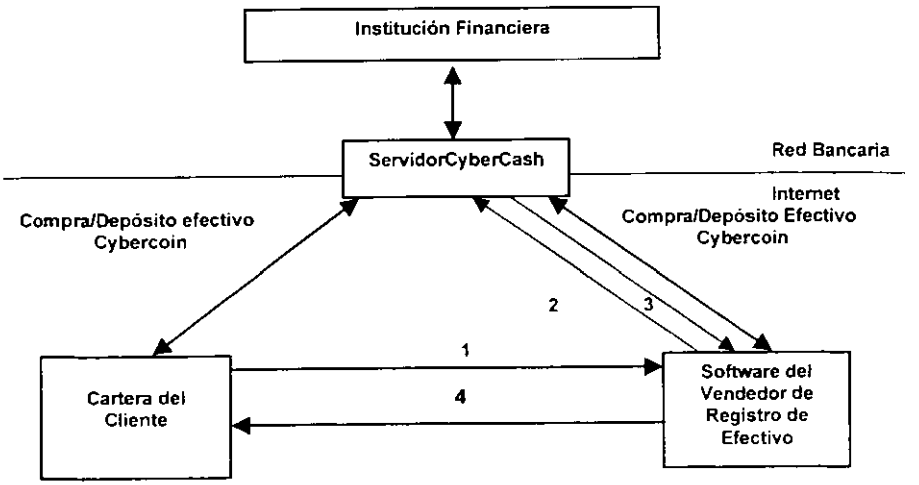
Ha estado en operación desde 1996 y lo desarrollo la misma compañía que desarrollo CyberCash. Este sistema es diseñado para ser usado donde el valor de una transacción es demasiado bajo para ser pagado con tarjeta de crédito.

Este sistema comparte similitudes con el esquema de dinero electrónico en línea. Los clientes compran dinero CyberCoin desde el servidor CyberCash, cargando la cantidad a su cuenta de tarjeta de crédito o banco. Puede ser almacenado en un área especial de la cartera CyberCash. Cuando un usuario decide pagar a un vendedor, él envía el mensaje de pago al vendedor quien verifica éste con el servidor CyberCash. Si la transacción es exitosa, el vendedor puede entregar los bienes al usuario. Una vez verificado el dinero, puede ser depositado dentro de la cuenta bancaria del vendedor vía el servidor CyberCash. La cartera mantiene un log de las transacciones hechas. Mientras el vendedor no conocerá la identidad del consumidor, este sistema no es anónimo como el servidor CyberCash tendrá que registrar cada transacción del usuario.

Cuando un cliente compra dinero CyberCoin, una cuenta es establecida con el servidor CyberCash. El hacer un pago es similar a la autorización de una cantidad para ser transfenda desde esta cuenta a la cuenta del vendedor. Al mismo tiempo, el valor puede ser transferido entre las cuentas CyberCash e instituciones financieras ligadas al servidor vía la red bancaria.

CyberCoin es un sistema propietario y el protocolo detalla que no ha sido publicado en el tiempo de escritura. Los mensajes instalados usan criptografía de llave pública, y éstos se cargan en una cartera CyberCash con el dinero CyberCoin, y se pone un material de llave simétrica. Los mensajes similares deben ser usados para transferir el valor del dinero dentro de una cuenta real, pero esto no requiere verificar un pago.

El dinero CyberCoin puede ser gastado con algún vendedor, y durante una transacción de compra sólo la criptografía de llave simétrica es usada. Mientras éste le permite ser más eficiente para realizar pequeños pagos que Ecash o NetCash, una tercera parte (servidor CyberCash) debe todavía ser contactado durante una transacción.



Procedimiento de Compra por Internet (CyberCoin)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de monedas**	**comprador**									
.1	Compran dinero Cybercoin en un SM.										
.2	Carga las monedas a su cuenta de tarjeta de crédito o a su banco.										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	**comprador**									
1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos				5		*				
.2	Muestra los datos ingresados				5	*					
8.	**Elección de la dirección**	**comprador**									
1	Tiene que elegir la dirección a la cual quiere que se le envie el producto.				5	*					
9.	**Muestra datos del cliente y del artículo**	**vendedor**									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envío				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
1	Asigna una cantidad de compra.				5	*				*	
11.	**Señalización de las formas de envío**	**vendedor**									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)				5	*		*			
12.	**Elección de forma de envío**	**comprador**									
.1	Elige la opción más adecuada conforme a sus necesidades				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación				5	*					
.2	Menciona los procesos de pago.					*		*			
14.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación				30	*	*				
.2	Selecciona el método de pago.				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Envío del mensaje de pago**	**comprador**									
.1	Envía un mensaje de pago al vendedor										
16.	**Verificación del pago**	**vendedor**									
.1	Verifica las monedas con el servidor CyberCash.										
.2	Registra la transacción										
17.	**Envío de respuesta de la transacción**	**vendedor**									
.1	Envía la respuesta al comprador de que la transacción se ha concretado.										
18.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	*			*		
19.	**Envío del producto**	**vendedor**									
.2	Envía el producto.		25					*	*		
20.	**Recepción del producto**	**comprador**									
.1	Recibe el producto.		700			*					

3.3.5 Mondex

Se basa en tarjetas de prepago, las tarjetas Mondex fueron desarrolladas en NatWest, una gran organización bancaria en Inglaterra, en 1990.

Este esquema confia en el uso del contacto de una tarjeta de chip (tarjeta inteligente), su núcleo contiene un chip basado en un microcontrolador Hitachi H8/310. Es un microprocesador de 8 bits con un chip RAM, ROM y EEPROM, también como un controlador de comunicación serial que permite conversar con el mundo exterior. El programa de control para el esquema de pagos Mondex es implementado en el ROM del microcontrolador y permite que el valor sea transferido desde el chip Mondex a otro usando un protocolo propietario de chip a chip.

Para facilitar la transferencia de valores, un número Mondex soporta dispositivos que están disponibles. La tarjeta es inicialmente cargada contactando un banco usando un cajero automático Mondex (ATM), o usando un adaptador especial del teléfono. Esos dispositivos de acceso no necesitan saber como trabaja el protocolo chip a chip, pero ellos incorporan un dispositivo de interfaz (IFD) que contiene un procesador de control que media el diálogo entre la tarjeta y el banco. En el banco, una forma de dinero seguro llamada caja de valor Mondex es instalada. Este es un dispositivo de hardware que puede soportar grandes números de tarjetas Mondex y actúa como un almacén de valores para diálogos con los emisores de tarjetas. Las transferencias para y desde la caja de valor son monitoreadas por un sistema de software, referido como el valor de control y el sistema de manejo, y los movimientos entonces se reflejaran en las cuentas de banco de los tarjetahabientes.

El proceso inicia cuando una tarjeta Mondex es insertada en el ATM o adaptador telefónico, con lo cual diálogos chip a chip toman lugar entre el IFD y la tarjeta bajo el control del dispositivo ATM. El IFD Mondex entonces establece un diálogo con el banco. Una vez que el número de cuenta del tarjetahabiente ha sido establecido, y la identidad de la tarjeta verificada, el valor es transfendo desde las tarjetas en la caja de valor del banco por el protocolo chip a chip para el chip de destino final residente en la tarjeta. El sistema de control y manejo del valor informará al sistema de cuentas del banco deducir de la cuenta bancaria del tarjetahabiente la cantidad.

El gasto es un proceso similar, donde los vendedores son equipados con un dispositivo llamado terminal de transferencia de valores. Este contiene un dispositivo IFD, éste facilita las transferencias desde la tarjeta del cliente y la tarjeta del vendedor. No necesitan un diálogo en linea con el banco para verificar la transferencia. En un tiempo posterior, el vendedor quizá contacte al banco, para transferir el valor a la caja de valores del banco, y simultáneamente tener la cantidad acreditada en su cuenta.

La tarjeta mantiene un monedero resumen que recuerda cuales fueron las ultimas 10 transacciones en las que la tarjeta tomo parte, y el hardware del vendedor guarda los registros desde las últimas 300 transacciones. Este limita la anonimidad del sistema, el cual se ha visto como desventaja por algunos usuarios del sistema. Una estrategia es, que los emisores de tarjetas Mondex periódicamente, capturen información de las transacciones en orden para construir un ejemplo estadístico de las transacciones que toman lugar. Este medio es usado en un intento para detectar fraude dentro del sistema.

Si una tarjeta es perdida, el valor almacenado en ésta no puede ser recuperado. La tarjeta sin embargo puede ser protegida, para que el valor no pueda ser transferido sin ingresar un número de identificación personal (PIN), por medio del dispositivo de interfaz. Si la tarjeta es encontrada, un ID de la tarjeta puede ser leido por el banco, permitiéndoles reconocer al propietario.

Cada tarjeta tiene dos diferentes esquemas de seguridad, uno es el activo y el otro es el pasivo. Periódicamente las tarjetas activan el sistema pasivo, y también puede ser renovado constantemente.

Para proteccion contra el uso de la tarjeta por lavadores de dinero, cada tarjeta Mondex tiene una posición jerárquica en la estructura de clase del monedero. Esta estructura impone reglas que otras clases de tarjetas que pueden intercambiar valores con y asociar el valor máximo de las transacciones. Los emisores de tarjetas pueden asegurar que el solo valor de intercambio directamente con la industria bancaria, asegura que todas esas transacciones producen un rastro de auditoria.

3.4 Micropagos

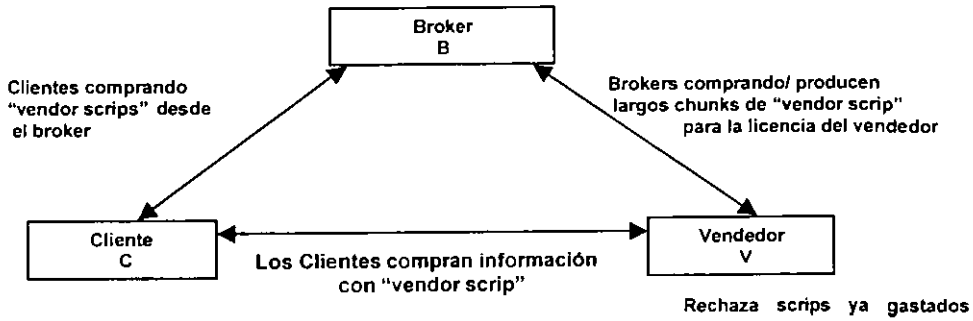
El concepto de Micropagos surge en 1995. Millicent, ha sido diseñado específicamente para suministrar la nueva forma de pago, mientras otros tales como μ-iKP, ha sido diseñado como un agregado para un existente esquema de macropago. Como hemos visto, hace el uso de alguna técnica de criptografía nueva, incluyendo el uso de los primero algoritmos de message digest para autenticar un mensaje y el uso de economías de escala en la emisión de monedas.

Una de las características de los micropagos, es que minimizan las comunicaciones necesarias durante una transacción y reducen el número de computaciones intensivas en las operaciones de llave pública. Millicent no usa la criptografía de llave pública y es optimó para repetidos micropagos al mismo vendedor. Es de acceso distribuido para permitir que un pago sea validado, y se previene el doble gasto, sin gastos para contactar una tercera parte centralizada en línea durante una compra. Con pagos tan bajos como un centavo son factibles, parece ser uno de los mejores candidatos para los micropagos, su única desventaja es, que para los pagos de múltiples vendedores, no se puede impedir el tener contacto con un corredor para cada nueva parte o vendedor encontrados.

3.4.1 Millicent

Permite pagos tan bajos como una décima de centavo ($0.001). Puede ser validado eficientemente por el site del vendedor sin necesitar el contacto de una tercera parte. Este acceso distribuido permite, sin alguna comunicación adicional, cifrado de llave pública, o procesos fuera de línea, permite adaptarse efectivamente para pagos pequeños constantes.

Usa una forma de moneda electrónica llamada Scrip (papel moneda), que es el cambio suelto que llevan en el monedero. Es rápido y eficiente para verificar que es válido, y si pierden una pequeña pieza de cambio por accidente éste no representa una gran preocupación. El Scrip es específico de cada vendedor en el cual tiene un valor también específico para el vendedor. La segundad del protocolo es diseñada para hacer que el costo del fraude cometido sólo sea el valor de la compra. El uso de un protocolo rápido de cifrado simétrico puede ser de poco peso y seguro.



Los participantes en una transacción Millicent son

a) Broker (corredor)

Un broker (corredor) media entre vendedores y clientes para simplificar las tareas que ellos ejecutan.

Le toma a un cliente muchas semanas o meses hacer micropagos suficientes para que un vendedor específico cubra el costo de un macropago estándar de una transacción financiera a ese vendedor. Por lo tanto podría no ser eficiente para un cliente que compra Scrips de cada vendedor al que ellos deseen comprar. Sin embargo, es probable que un cliente haga suficientes micropagos en total a diferentes vendedores para cubrir el costo de una transacción de un macropago. Un macropago es una transacción capaz de manejar pagos de varios valores en dólares o más

Vende Scrips a los clientes. El agregar diferentes vendedores de scrips justifica una transacción de macropagos para comprar esas piezas de scrip. El vendedor que vende su propio scrip no debería justificarlo normalmente

Remplaza el servicio de suscripción con un pago por acceso al sistema de micropago

Los corredores son los que administran el dinero real en Millicent, mantienen cuentas de clientes y vendedores. Los clientes compran al vendedor los scrips para un vendedor específico desde su corredor. El corredor tendrá un acuerdo con cada vendedor del que vende sus scrips. Hay dos caminos por los cuales un corredor obtiene scrips de los vendedores

1. Almacén de scrips. El corredor compra muchas piezas de scrips del vendedor desde el vendedor. Los scrips son almacenados y vendidos por pieza a diferentes clientes.

2. Producción de scrips licenciados. El corredor actual genera los scrips del vendedor, en nombre del vendedor. Es más eficiente porque.

   - El corredor no necesita almacenar un gran número de piezas de scrips.
   - El vendedor computa menos desde que el no tiene que generar sus propios scrips.
   - La licencia, la cual puede ser concedida y enviada a través de la red, es más pequeña para transmitir más grandes pedazos de scrip.

La licencia permitirá al corredor sólo generar cantidades específicas de scrips del vendedor. La licencia debería ser aplicable a través de la práctica de negocios normales. Los corredores típicamente serán instituciones financieras o proveedores de servicio de redes. Asumen ser confiables por otras entidades.

b) Vendedores

Son vendedores que venden servicios o información de bajo valor. Un vendedor acepta su propio scrip como pago de los clientes. El vendedor puede validar sus propios scrips localmente y prevenir el doble gasto. El vendedor vende sus scrips con descuento o produciendo la licencia de scrips a un corredor. Este descuento o comisión de venta es como el corredor obtiene una ganancia desde este esquema.

c) Clientes

Son los usuarios que compran un scrip al corredor con dinero real, pueden utilizar sistemas como SET o Ecash para adquirirlos. Usando el scrip del corredor, el cliente compra scrip para un vendedor en específico. El scrip puede ser usado para hacer compras.

Comprando con Millicent

El comprador adquiere los scrips por medio de un sistema de macropago, para gastarlos en el site del vendedor.

El scrip es enviado al vendedor con una solicitud de compra. El vendedor regresa un nueva pieza del scrip como cambio junto con el contenido de la compra. El cliente compra desde el mismo vendedor nuevamente usando el cambio. El cliente ya ha validado el scrip para el vendedor, así que no hay necesidad de contactar al corredor. Nuevamente, el scrip y la compra requieren ser enviadas al vendedor quien regresa el artículo y el cambio correcto.

Si se realizan repetidos pagos con un vendedor en específico son altamente eficientes por lo que se refiere a las conexiones de red. Si el cliente ya tiene un scrip válido para ese vendedor sólo una conexión a la red es requerida. Compare ésta con el número de conexiones requeridas en un esquema de macropagos seguro tal como SET o Ecash. Este incrementa la eficiencia de comunicación que es provista en el costo de la seguridad ligera.

Scrip

El Scrip es una pieza de datos usados para representar la micromoneda dentro del sistema Millicent. Tiene las siguientes propiedades:

- Una pieza de scrip representa un valor de prepago, tal como las tarjetas de teléfono de prepago o cupones.
- Puede representar algunas denominaciones de moneda. Espera valores de un rango de un centavo hasta 5 dólares, aunque no hay definidas cantidades más grandes o más bajas.
- La seguridad de un scrip está basada en la Asunción que es sólo usado para representar pequeñas cantidades de dinero.

- Es para un vendedor específico, y por lo tanto tiene valor sólo para un vendedor.
- Puede ser gastado sólo una vez. El doble gasto será detectado localmente por el vendedor en el momento de la compra.
- Sólo puede ser gastado por su propietario. Un secreto compartido es usado para prevenir el robo de scrip siendo gastado.
- El scrip no puede ser falsificado o su valor alterado.
- Es computacionalmente caro falsificar un scrip. El costo de hacerlo sobrepasa el valor del mismo scrip.
- El scrip no hace uso de criptografía de llave pública. Puede ser eficientemente producido, validado, y protegido usado una función hash one way y limitado por criptografía simétrica.
- El scrip no provee anonimato por completo. Tiene un número de serie visible que podría ser registrado y rastreado. Algunos limitan la anonimidad por medio de los corredores que compran los scrips usando un sistema de macropago anónimo.

La estructura del scrip, contiene los siguientes datos:

Dato	Descripción
Vendedor	Identifica al vendedor del cual tenemos el scrip.
Valor	Especifica cual es el valor del scrip.
#ID	Un identificador único del scrip, tal como el número de serie. Es usado para prevenir el doble gasto.
#CustID	Identificador usado para calcular la llave secreta compartida (CustomerSecret), que es usada para proteger el scrip.
Expira	La fecha en la cual el scrip llega a ser inválido.
Info	Detalles opcionales que describen al cliente para el vendedor.
Certificado	Este campo previene al Scrip de ser alterado de alguna manera y prueba que es auténtico.

Generación del Certificado del Scrip

Cuando una pieza de scrip es generada como una firma o como un certificado de autenticidad para ese scrip. El certificado previene que algún campo del scrip sea alterado.

Este es creado aplicando una función hash a otros campos del scrip con un secreto. Sólo el vendedor (o el corredor) quien emite el scrip conocerá el secreto, el cual es llamado el secreto maestro del scrip. El vendedor mantendrá una lista de los diferentes secretos maestros del scrip, numerados de 1 a N, para el propósito de la emisión del scrip. Este secreto es usado con una pieza de scrip en particular depende de alguna parte del ID# del scrip. El certificado previene de la falsificación y alteración.

Para validar el scrip el vendedor debe:

- Autenticar el scrip producido por el vendedor o el corredor licenciado.
- No debe haberse gastado antes.

El vendedor recalculara el certificado y lo comparara con el certificado del scrip desde el cliente. Ambos certificados deberán ser iguales al scrip sino ha sido alterado.

Previniendo el doble gasto

El vendedor tiene que checar que el #ID no haya sido gastado. El vendedor mantiene vectores de bits (estructura de datos para representar cada #ID), correspondientes al número de serie emitido (#IDs) para guardar la trayectoria de gasto del scrip. Los vectores que cubren rangos que han sido completamente gastados o expirados pueden ser descartados. Permite al vendedor guardar la base de datos de los #ID del scrip válidos en memoria, lo cual agiliza la transacción.

El costo computacional es más barato y eficiente.

Scirp en claro

El cliente envía el scrip sin protegerlo a través de la red al vendedor. El vendedor regresará el contenido de la compra y el cambio en claro. Ninguna seguridad de red es provista en este protocolo. Un atacante puede interceptar el scrip o cambiarlo y usarlo. Recuerda, el ratero del scrip puede gastarlo sólo con un vendedor en particular.

Encriptar conexiones de red

Para prevenir que el scrip sea robado, y prevenir que un intruso obtenga alguna información desde la transacción, la conexión de red debe ser encriptada.

Se puede realizar usando una llave simétrica compartida llamada, CustomerSecret, entre el cliente y el vendedor. Este secreto es usado para asegurar el canal de comunicación usando un algoritmo simétrico eficiente como DES, IDEA o RC4.

El scrip no puede ser robado y el intruso no puede ver la compra o los detalles del scrip. El VendorID y el #CustID son enviados en claro en ambos mensajes así que el receptor puede calcular el CustomerSecret

CustomerSecret: Es generado cuando el scrip es creado. Es formado aplicando la función hash al identificador del cliente con otro secreto, llamado MasterCustomerSecret. Sólo el vendedor (o un corredor confiable) conocerá este secreto. Como el MasterScripSecret, el vendedor mantendrá una lista de los diferentes MasterCustomerSecrets, numerados desde 1 a N. Parte del #CustID es usada para seleccionar el MasterCustomerSecret.

El vendedor puede recalcular el CustomerSecret en algún momento desde la pieza del scrip. El cliente debe obtener el CustomeSecret. Este es regresado al cliente cuando el scrip del vendedor está comprado desde un corredor. Para proteger el CustomerSecret, como éste pasa desde el corredor al cliente, la transacción podría ser ejecutada usando un protocolo seguro que no es Millicent. Alternativamente una transacción segura de Millicent podría ser usada, donde el CustomerSecret exista para el scrip del corredor usado por el cliente. El CustomerSecret podría ser usado para encriptar la conexión en la misma dirección. El CustomerSecret para el scrip del corredor debe ser obtenido usando un protocolo seguro fuera del sistema Millicent

Solicitando Firmas

Este protocolo remueve la encripción para mantener un nivel de seguridad que prevenga que el scrip sea robado.

El CustomerSecret es usado para generar una solicitud de firma en vez de usarlo para la encripción. Es similar al campo del certificado de una pieza del scrip, que es una función hash de otros campos. La solicitud de firma es generada por medio de aplicar la función hash a un scrip, CustomerSecret, y la solicitud. Es creado por el cliente y enviado junto con el scrip y la solicitud al vendedor.

El vendedor verifica la solicitud de firma recomputandola. El vendedor puede computar el CustomerSecret usando el scrip y el MasterCustomerSecret. Si la solicitud ha sido alterada, entonces las dos firmas solicitadas no serán iguales y el vendedor refutará el proceso de la transacción.

Para una solicitud válida, el vendedor regresa la respuesta de compra, el cambio en el scrip y la respuesta de la firma. La firma de respuesta es generada de la misma manera que la firma de la solicitud, usando el mismo CustomerSecret. El cambio no puede ser robado por algún atacante, porque éste no puede ser gastado sin conocimiento del CustomerSecret, ya que la firma solicitada no puede ser calculada, y el vendedor refuta la transacción.

Por lo tanto, mientras un intruso puede ver todas las partes de la transacción (no privacidad), la solicitud de la compra no puede ser alterada y el scrip no puede ser robado. La seguridad ha sido provista más eficientemente que usando la encripción, pero el costo es perder la privacidad.

Millicent con el Web: Puede ser implementado como una extensión de protocolo de Web HTTP. Consiste de una cartera de usuario, un servidor del vendedor, y un servidor del corredor.

Extensiones: Se puede usar también de la siguiente manera:

- Autenticación para servicios distribuidos: El scrip podría ser usado para proveer autenticación como Kerberos para acceso de servicios de red. Al inicio del día, un usuario obtiene un scrip de autenticación desde un corredor. Este scrip de autenticación es entonces usado para comprar scrips para accesar a los servicios de una red en especial. El acceso es dinámicamente provisto basado en un usuario teniendo un scrip para ese sistema.

- Uso contable: Podría ser usado con una cuenta y aplicaciones contables dentro las redes privadas. La organización actúa como un corredor, con empleados como los clientes. El vendedor será el servidor al cual los empleados tengan acceso.

- Cargos basados en uso: Podría ser usado para cargos de preconexión para servicios como el e-mail, transferencia de archivos, teléfono de Internet, teleconferencia, y otros servicios en línea. Sin embargo éste no sería lo suficientemente eficiente para paquetes de nivel de cargo para esos servicios.

- Cupones de descuento: Adicionales campos podrían ser agregados al scrip para proveer descuentos de ciertos contenidos.

- Previniendo el compartir subscripciones: Usando un scrip para accesar un servicio de subscripción de prepago, compartiendo esa cuenta de subscripción puede ser prevenido. El scrip actua como una capacidad de acceso a los servicios, con el cambio del scrip estamos dando el acceso a la siguiente vez. Sin embargo, tratando de ganar acceso con una pieza ya usada de scrip puede ser fallido.

Procedimiento de Compra por Internet (Millicent)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Obtención de scrips**	**comprador**									
.1	Compra scrips con un corredor por medio de un sistema de macropago.										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados.				5	*					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
9.	**Muestra datos del cliente y del artículo**	**vendedor**									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
.1	Asigna una cantidad de compra.				5	*				*	
11.	**Señalización de las formas de envío**	**vendedor**									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional).				5	*		*			
12.	**Elección de forma de envío**	**comprador**									
1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
1	Pide password y su confirmación.				5	*					
2	Menciona los procesos de pago.					*		*			
14.	**Selección de un método de pago**	**comprador**									
1	Ingresa password y confirmación.				30	*	*				
.2	Selecciona el método de pago				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Envío de la solicitud de compra**	**comprador**									
.1	Envía la solicitud de compra junto con un scrip.										
16.	**Recepción de la solicitud de compra**	**vendedor**									
.1	Recibe la solicitud de compra y el scrip.										
2	Regresa al comprador un nuevo scrip, como el cambio.										
17.	**Validación del scrip**	**vendedor**									
.1	El comprador ya ha validado el scrip para el vendedor.										
2	Regresa el scrip junto con la compra.										
18.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	*			*		
19.	**Envío del producto**	**vendedor**									
2	Envía el producto		25					*	*		
20.	**Recepción del producto**	**comprador**									
1	Recibe el producto		700			*					

3.4.2 SubScrip

Protocolo de micropago diseñado para eficientes pagos por evento (pay-per-view) en Internet. Desarrollado en la Universidad de NewCastle, Australia, y es un sistema de prepago sin necesidad de identificación del usuario.

Trabaja creando cuentas de prepago temporal para usuarios con un vendedor en específico. El usuario hace su compra desde el vendedor contra esta cuenta. Desde que la cuenta es temporal y de prepago, no carga el sobrecargo normal asociado con los servicios de subscripción. El sistema no requiere su propia jerarquía de facturación o bancaria. Ecash o SET pueden ser usados para hacer el pago inicial a un vendedor para colocar la cuenta de prepago.

El nivel de seguridad es poco para el bajo valor de las transacciones. La encripción no es usada del todo.

Un micropago puede ser verificado localmente por un vendedor, sin la necesidad de algún aclaramiento en línea con una tercera parte. Similarmente hay un sobrecargo inicial asociado con hacer un pago a un nuevo vendedor. Ambos sistemas son óptimos para repetidos pagos con el mismo vendedor, sobre un corto periodo.

No se usa un corredor, sino en vez de eso se usa un esquema de macropago que acepte el vendedor. El usuario hace un gran pago suficiente para cubrir el costo de la transacción del macropago para el vendedor. Este pago será de pocos dólares y es usado para poner una cuenta temporal en el vendedor.

Para hacer una compra de micropago contra la cuenta temporal, el usuario necesita algún tipo de identificador de la cuenta, más conocido como ticket SubScrip. El vendedor regresa el ticket al usuario para accesar una nueva cuenta.

Dando anonimato: Este dependerá del anonimato del sistema de macropago usado inicialmente para pagar al vendedor. Si un sistema no anónimo es usado, el vendedor puede ligar el nombre de la cuenta temporal, y rastrear todos los pagos hechos desde esa cuenta. Con un sistema anónimo, el vendedor sólo conocerá la dirección de red de la solicitud del cliente del cual la envío. El cliente y el vendedor tendrán que acordar el mismo protocolo de pago a usar.

Un ticket SubScrip: Es el identificador especial de una cuenta, usado para autenticar al propietario de la cuenta, para el administrador de cuentas en el site del vendedor, para poder realizar una compra de micropago. Es válido con sólo un vendedor. Consiste de:

AccID	Un identificador de la cuenta que únicamente identifica al vendedor. Es escogido de manera que a un atacante le sea difícil adivinarlo
Val	La cantidad monetaria en la cuenta del vendedor
Exp	La fecha en la cual la cuenta expira. Está limita el numero de cuentas que deben ser mantenidas por el vendedor.

El vendedor mantiene una base de datos de ID's de cuentas con la cantidad y la fecha de expiración de cada una. El conocimiento del ID de la cuenta es la única manera de obtener el acceso a la cuenta. El ticket actualmente no tiene valor en si mismo y por lo tanto es una moneda electrónica. Sin embargo, sin este el valor de prepago en el vendedor no puede ser accesado.

El valor de SubScrip es transfenble a otro usuario. Es hecho dando al usuario un ticket válido para el balance de la cuenta con un vendedor específico.

Una compra SubScrip: Para hacer una compra, el usuario envía el ticket SubScrip al vendedor, quien verifica que es válido, verificándolo en la base de datos. La cantidad del micropago es deducida desde la cuenta de balance. Un nuevo y aleatorio identificador de la cuenta y la comparación del ticket con el nuevo balance es entonces generado para la cuenta y regresado al usuario junto con la información de la compra o servicio. El usuario almacena el nuevo ticket, junto con la dirección del vendedor, para compras adicionales.

Esto no es posible para que usuarios comentan fraudes alterando los campos de valor o expiración en el ticket SubScrip. Esto es porque esos campos son incluidos en el ticket para la información del usuario. La base de datos de cuentas administrada por el vendedor siempre tendrá un balance de cuenta real y fechas de expiración.

Seguridad y Privacidad: Los tickets son enviados en claro, sin encripción usada durante la compra. Un intruso puede ver exactamente que está comprando y por cuanto es la transacción. La cantidad permanece en la cuenta del usuario en el vendedor puede también ser vista en claro desde el ticket nuevo que se regresa. La no privacidad puede ser provista por el protocolo en esta forma.

Es posible para un intruso obtener un ID de cuenta válido cuando un nuevo ticket es regresado al cliente como cambio. Un ticket robado podría ser gastado por un atacante, y cuando el usuario siguiente tratará de gastarlo éste podria ya ser inválido. Un atacante activo podría también interceptar un ticket válido que está siendo enviado al vendedor como una solicitud de compra. Una vez que un ticket válido alcanza al vendedor, su invalidación, y el atacante tendría que prevenir a este ticket o una retransmisión de éste alcanzando su destino para exitosamente robarlo.

Protegiendo el SubScrip: Para proveer mayor seguridad, utiliza un protocolo de SupScrip protegido usando criptografía de llave pública.

Cuando un cliente compra primero una cuenta SubScrip temporal con el vendedor, la llave pública del cliente Kpu_C, es también enviada. El vendedor almacena esta llave pública con el ID de la cuenta en la base de datos de cuentas. Cuando quiera el vendedor envía un nuevo ticket para esta cuenta al cliente, encriptandolo con la llave pública del cliente.

El ticket no está encriptado cuando es enviado desde el cliente al vendedor. Los diseñadores sienten que es improbable, que un atacante vaya hacia el problema de prevenir que el ticket alcance su destino (donde fuera inválido) para ordenar el robo.

Reembolso de fondos: Otra extensión permite a los clientes convertir tickets sin gastar a dinero real. Esto sería hecho enviando el ticket al vendedor, quien pagaría el resto del balance de la cuenta al usuario usando un sistema de macropago existente. Un sistema en el cual algún usuario pueda aceptar pagos, tales como los sistemas de dinero electrónico, tendrán que ser usados para éste propósito. Los sistemas de tarjeta de crédito no pueden hacer esto. El costo de la transacción de macropago quizá tenga que ser cubierta por el vendedor para cargar los honorarios por este servicio.

Tickets perdidos: Las cuentas de ID's perdidos quizá sean recuperadas enviando la dirección de entrega y el tiempo aproximado del último acceso para recobrar la cuenta. El SubScrip provee una carga ligera, eficiente, cuentas basadas en sistemas de micropago con seguridad limitada. Este reduce el peso requerido para mantener una subscripción de base de datos y permitir algún anonimato.

Procedimiento de Compra por Internet (SubScrip)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
1.	**Obtención de SubScrips**	**comprador**									
.1	Compra SubScrips por medio de un sistema de macropago que acepte el vendedor.										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados.				5	*					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envie el producto				5	*					
9.	**Muestra datos del cliente y del artículo**	**vendedor**									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envio.				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
1	Asigna una cantidad de compra.				5	*				*	
11.	**Señalización de las formas de envio**	**vendedor**									
1	Da las diferentes formas de envio y una breve descripción (Nacional/Internacional)				5	*		*			
12.	**Elección de forma de envio**	**comprador**									
1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
1	Pide password y su confirmación				5	*					
2	Menciona los procesos de pago.					*		*			
14.	**Selección de un método de pago**	**comprador**									
1	Ingresa password y confirmación				30	*	*				
2	Selecciona el método de pago.				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Envío del SubScrip**	**comprador**									
.1	Envía el SubScrip al vendedor.										
16.	**Verificación del SubScrip**	**vendedor**									
.1	Verifica que el SubScrip sea válido, en la base de datos.										
.2	Deduce la cantidad del micropago desde la cuenta de balance.										
.3	Genera un nuevo identificador de la cuenta y otro subscrip es generado regresado al comprador.										
18.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	*			*		
19.	**Envío del producto**	**vendedor**									
.2	Envía el producto.		25					*	*		
20.	**Recepción del producto**	**comprador**									
.1	Recibe el producto		700			*					

3.4.3 PayWord

Es un sistema de crédito basado en el micropago diseñado por Ron Rivest (Laboratorio de Ciencias de la Computación del MIT, MA, USA) y Aid Shamir (Instituto de Ciencia Weizmann, Rehoboth, Israel.) Este esquema está dirigido para reducir el número de operaciones de llave pública requeridos por pago usando funciones hash, las cuales son más rápidas.

Usa cadenas de valores hash para representar el crédito del usuario dentro del sistema. Cada valor hash, llamado payword, puede ser enviado a un vendedor como pago. Una cadena payword es de un vendedor especifico y el usuario digitalmente firma un compromiso de honor de pago para esta cadena.

Los corredores median entre usuarios y vendedores y mantienen las cuentas para ambos. Citan para usuarios emitiendo un certificado PayWord permitiendo al usuario generar los PayWords. Redimen el gasto de las cadenas de payword a los vendedores. No es necesario para vendedor y usuario tener una cuenta con el mismo corredor

Las partes que abusen del sistema pueden ser detectadas y removidas

Certificados de Usuario PayWord

Este certificado autoriza a un usuario a generar una cadena payword, y garantiza que un corredor especifico los redimirá. Los corredores y vendedores no necesitan un certificado en PayWord

Los usuarios obtienen el certificado cuando ellos inicialmente abren una cuenta con el corredor. Un esquema de macropagos o pago con tarjeta de crédito podría ser usado para pagar dinero dentro de la cuenta. El certificado típicamente tendrá que ser renovado cada mes. Esto limita el fraude para asegurar que esos usuarios quienes han excedido sus cuentas no les sea emitido un nuevo certificado, el cual les permitiría continuar generando pagos. El certificado es de la forma:

$C = (B, U, A, Kpu, E, I)SK_B$

El certificado es firmado por el corredor (B). Los campos son:

- B — Identifica al corredor quien emite el certificado. Los Paywords aceptados desde el usuario (U) solamente serán amortizables en este corredor.
- U — Identifica al usuario quien está autorizado por este certificado para generar cadenas payword
- A_U — La dirección de entrega del usuario. Esta podría incluir una dirección host de Internet, e-mail, o dirección de correo. Para prevenir los fraudes, los artículos comprados por el usuario deberían sólo ser entregados en esta dirección.
- Kpu_U — Llave pública del usuario. Para verificar la firma digital del usuario en una comisión para una nueva cadena de pago
- E — Fecha en la que el certificado expira
- I_U — Información opcional. Esta podría incluir límites de crédito por vendedor, los detalles específicos del usuario, o detalles del corredor

Para verificar la firma del corredor en un certificado, un vendedor debe seguramente obtener la llave pública del corredor, Kpu_B, de alguna manera.

Desde que los certificados son identificados con un identificador del usuario y una dirección son usados, no proveen anonimato.

Certificados Revocados: Un corredor quizá mantenga una lista negra de certificados que han sido revocados, tal como las listas de revocación en SET. Un certificado de usuario debería ser revocado si su llave secreta fue perdida o robada, éste permitiría a otros generar cadenas payword bajo su nombre. Es responsabilidad de un vendedor obtener alguna lista de certificados revocados desde un corredor

Cadenas PayWord: Una cadena payword representa el crédito del usuario con un vendedor específico. Esta es una cadena de valores hash . Cada payword (valor hash) en la cadena, tiene el mismo valor, normalmente un centavo. Para generar esta cadena seguimos los siguientes pasos:

1. Decidir una longitud, N, de la cadena. Una cadena payword de longitud 10 debería tener el valor de 10 centavos si el valor payword es 1 centavo. El valor de la cadena debería ser más grande que la cantidad puede ser seguramente desechado. Desde que representa el crédito del usuario, el valor no es perdido.
2. Seleccionar un numero aleatorio, W_N.
3. Ejecutar N repetidos hashes de W_N. Cada valor hash forma una payword. MD5 podrá ser usado como una función hash.
4. La cadena final debería ser:$\{W_0, W_1, W_2, \ldots, W_N\}$

Comisión para una cadena PayWord

El vendedor y el corredor necesitan conocer quien gasta los paywords pertenecientes a la cuenta del usuario que pueden ser cargados apropiadamente. El usuario es autenticado firmando un compromiso para una cadena payword. La comisión autorizará al corredor para amortizar algún payword desde la cadena de comisión. Este permitirá al vendedor confiarse de que ellos pagaran por los paywords aceptados desde el usuario. La comisión tiene la forma

$C_{comm} = \{V, C_U, W_0, E, I_{Comm}\}SK$

Es firmado con la llave secreta del usuario. Los campos que contiene son:

- V — El vendedor en el cual la comisión de la cadena payword es válida. Una cadena payword es de un vendedor en específico.
- C_U — El certificado payword del usuario. Usado para verificar la firma del usuario y para verificar autorización desde un corredor.
- W_0 — La raíz de la cadena de payword. Identifica la cadena y permite que los paywords sean verificados que pertenecen a esa cadena.
- E — La fecha en la cual la comisión expira. Esta limita la longitud de tiempo para los usuarios y vendedores que necesiten almacenar alguna información acerca del estado de una cadena de pago.
- I_{Comm} — Información adicional. Esta podría contener la longitud, N, de la cadena. También podría ser definido el valor del payword. Típicamente, cada payword debe ser valuado en un centavo, pero otras cadenas de valores quizá también sean útiles. El máximo límite del valor de un payword dependerá en el riesgo que un vendedor o corredor éste preparado a aceptar. El corredor quizá recomiende un límite máximo dentro de un certificado de usuario. Los paywords con valores más grandes que 1 dólar tienen demasiado riesgo de ser asociado con ellos.

Gastando PayWords

Cuando un usuario se encuentra a un vendedor del cual desea comprar bienes, ellos generan un nuevo PayWord y una comisión. La comisión es entonces enviada al vendedor, para mostrar las intenciones de gasto del payword.

Para hacer el pago de un centavo, el usuario entonces envía el primer payword W_1 al vendedor. Este es verificado, tomando el hash del payword W_1. Si el payword es válido, el hash debería ser el mismo a la raiz de la cadena (W_0) encontrada en la comisión. Este trabaja porque sólo el usuario podía poseer el payword válido W_1. Es computacionalmente difícil para generar un valor que aplicaría un hash a W_0 debido a la naturaleza de la funciones hash one way. Por lo tanto, conocimiento constante W_0 , un atacante o un vendedor fraudulento no puede generar válidos PayWords en la cadena.

Para hacer un pago adicional de un centavo, el usuario enviará W_2. El vendedor entonces compara el valor obtenido tomando el hash de W_2, $H(W_2)$ al previo PayWord válido recibido (W_1). Si W_2 es válido, entonces los valores serán iguales.

Tamaño de Pago variable

El valor de los pagos más grandes que un centavo pueden ser hechos enviando un payword adicional a la cadena, sin haber enviado saltos sobre un payword. Por ejemplo, para hacer un pago de tres centavos después de haberlos gastado W_2, el quinto payword, W_5, puede ser enviado. El mensaje de pago actual consiste de un payword y su índice dentro de la cadena:

$P = (W_5, 5)$

Esto le permite al vendedor saber cuantas funciones hash debe ejecutar. En el ejemplo, el vendedor debe ejecutar tres repetidas funciones hash en W_5. El nombre del usuario quizá también tenga que ser incluido en el mensaje de pago para permitir al vendedor identificar al usuario, dependiendo de los detalles de implementación. El vendedor es el responsable de registrar el último payword válido aceptado del usuario.

El corredor no necesita ser contactado durante un pago. Los paywords pueden rápidamente ser verificados localmente por el vendedor. Después de la comisión inicial, el tamaño actual de los mensajes de pago, P, envía en pequeño, el cual adicionalmente improvisa eficiencia de comunicaciones. Como muchos sistemas de pago electrónicos, no hay garantía que el artículo de compra sea entregado por el vendedor.

Los usuarios no gastan los paywords, hasta que han terminado de gastar con el vendedor o hasta que el compromiso para la cadena payword haya expirado. Un vendedor debería guardar cada compromiso de usuario y validar el último payword recibido. Después de redimir una cadena gastada, el vendedor debería retener una comisión que no ha expirado para prevenir los ataques de repetición.

Redimiendo el gasto de los PayWords: Para recibir un pago, un vendedor redime la cadena payword con el corredor apropiado, quizá al final de cada día. Para cada cadena, el vendedor debe enviar lo siguiente:

- Firma del compromiso del usuario para esa cadena.
- El más alto índice de payword gastado.

El corredor verifica el payword más grande, W_1, para ejecutar L funciones hash en éste. El valor obtenido debe ser igual que W_0 en la comisión del usuario si W_L es válida. Si la firma del usuario y W_L son válidos, el corredor deduce la cantidad gastada desde la cuenta del usuario y paga al vendedor.

Costos Computacionales

Corredor
- Una firma / usuario /mes (C_U);
- Una verificación de firma / usuario / vendedor / día (Compromiso),
- Una función hash por payword gastado.

Vendedor
- Dos verificaciones de firma / usuario / día (Compromiso y C_U),
- Una función hash por payword gastado.

Usuario
- Una firma / vendedor / dia (Compromiso),
- Una función hash por payword construido.

Sólo el usuario necesita ejecutar la computación intensiva de la firma de llave pública en línea, y entonces sólo una vez por vendedor y por día. La verificación de la firma es menos computación intensiva y están también guardando un mínimo. Las funciones hash son computacionalmente baratas y se ejecutan una vez por payword por todas las partes. El corredor podría ejecutar la generación del certificado y la redención del payword fuera de línea para eficiencia. El PayWord es más eficiente para micropagos repetidos con un vendedor específico.

Procedimiento de Compra por Internet (PayWord)

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
1.	**Generación de la comisión y el PayWord**	**comprador**									
.1	Genera la comisión y el PayWord.										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del artículo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos				5		*				
.2	Muestra los datos ingresados				5	*					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto				5	*					
9.	**Muestra datos del cliente y del artículo**	**vendedor**									
1	Despliega la información del artículo a adquirir y los datos de la dirección de envío.				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
1	Asigna una cantidad de compra				5	*				*	
11.	**Señalización de las formas de envío**	**vendedor**									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional).				5	*		*			
12.	**Elección de forma de envío**	**comprador**									
1	Elige la opción más adecuada conforme a sus necesidades.				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
.1	Pide password y su confirmación.				5	*					
.2	Menciona los procesos de pago					*		*			
14.	**Selección de un método de pago**	**comprador**									
.1	Ingresa password y confirmación.				30	*	*				
.2	Selecciona el método de pago				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
15.	**Envio de la comisión**	**comprador**									
.1	Envia la comisión al vendedor, para informarle sus intenciones de compra.										
16.	**Realización del pago**	**comprador**									
.1	Envia un PayWord.										
17.	**Verificación del PayWord**	**vendedor**									
.1	Verifica el PayWord por medio del resultado de aplicar una función hash con la cadena enviada por el comprador.										
18.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	*			*		
19.	**Envio del producto**	**vendedor**									
.2	Envia el producto.		25					*	*		
20.	**Recepción del producto**	**comprador**									
1	Recibe el producto.		700			*					

3.4.4 Protocolo de Micropago iKP

Los creadores de los protocolos iKP han desarrollado un esquema de micropago que puede ser usados junto con 3KP pero no depende de éste para hacer los micropagos. Este esquema se basa en la creación de una cadena de valores hash usando una función one way. Una fuerte función one way (F) es tal que dado un valor (x) es fácil computar F(x). Pero dado un valor (y), es computacionalmente infactible encontrar x tal que y=F(x). Usando tal función F, un cliente escoge un valor aleatorio X y computa una cadena de valores hash usando lo siguiente:

$$A^0(X) = X$$
$$A^{i+1}(X) = F(A^i(X))$$

Los valores $\{A^0,..., A^{n-1}\}$ son referidos como cupones. Esos cupones habilitan al cliente para hacer n micropagos de valores acordados (val) para un vendedor. El cliente envía A^n al vendedor junto con el valor(val) por cupón y el total de número de cupones n usando un arbitrario sistema de macropago. Los micropagos son ejecutados sucesivamente revelando $\{A^{n-1}, A^{n-2},..., A^0\}$ al vendedor. El vendedor puede verificar esto conforme vaya obteniendo A^n.

$$A^i(X) = F(A^{i-1}(X))$$

Si n=100, el cliente realizara el cupón A^{99} para el primer artículo a ser comprado. El vendedor puede verificar éste como $A^{100}(X) = F(A^{99}(X))$. El cliente realiza los cupones subsecuentes para cada pago adicional al vendedor.

Protocolo 3KP

Es el modelo usado en 3KP, consta de un cliente (C), un vendedor (V) y el gateway del adquirente (A), cada uno posee su par de llaves públicas, que se usan para proveer verificación de la autenticidad de cada participante y del no repudio de mensajes entre ellos. En la autenticación inicial de un cliente a un vendedor, une al cliente a una cadena hash específica. Esto es hecho enviando un mensaje Solicitud de Crédito firmado con la llave secreta del cliente.

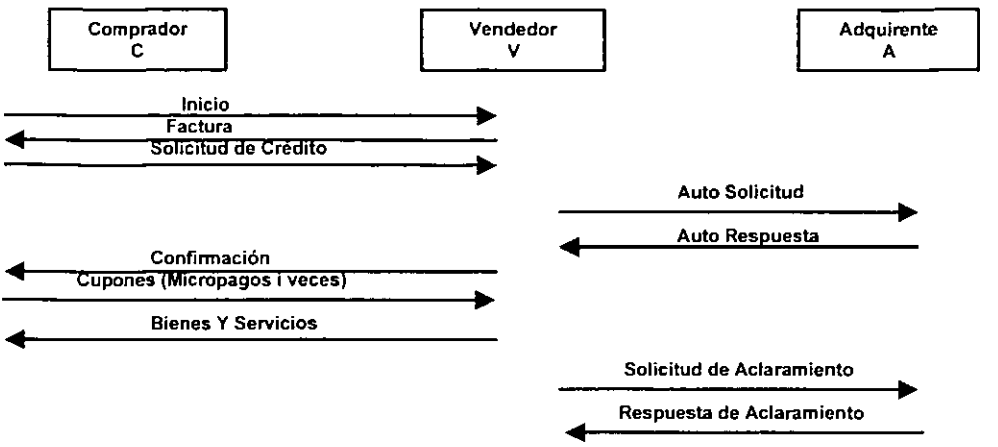
Una vez que el vendedor ha obtenido la autorización para el cliente desde el adquirente, el cliente puede iniciar haciendo micropagos. Nota antes, el cliente y el vendedor acuerdan la descripción y el valor de los artículos iniciando el protocolo 3KP.

El vendedor acumula los cupones depositados por el cliente, hasta que el último cupón en la cadena es alcanzado o hasta que el vendedor está satisfecho, de que lo que ha acumulado han sido suficientes cupones para garantizar el envío de un Solicitud de Aclaramiento al adquirente (no hay fecha de expiración de los cupones). Hay un acuerdo entre los cupones de aclaración intermediario, en los caso de que quizá sufra de múltiples cargos de aclaramiento y espere por todos los cupones para ser depositados por un cliente, por lo cual el vendedor quizá pierda alguna cantidad de intereses. El vendedor recibe un mensaje Respuesta de Aclaramiento de regreso desde el adquirente indicando si el pago ha sido aceptado o refutado.

Hay dos posibles patrones de comportamiento que quizá sean observados entre usuarios de protocolo de micropagos.

- Clientes que se comprometen con repetidas transacciones de micropago con un vendedor
- Clientes que se comprometen con una sola transacción con un vendedor en particular.

Los posteriores requerimientos de una tercera parte de confianza (TTP), tal como un corredor acumula las transacciones de micropago desde un número de usuarios, y las envía al vendedor para hacer el protocolo económicamente factible.



Repetición de Micropagos.

En circunstancias donde un cliente está teniendo una gran relación con el vendedor es económicamente factible el establecer una relación directa de macropago con el vendedor. El cliente escoge la raiz de la cadena hash x y calcula una cadena de valores hash (n cupones) { A^0, A^1,..., A^n} usando una función one way tal como MD5 o SHA. Entonces inicia el protocolo μ-3KP para la verificación del crédito desde el vendedor

Datos intercambiados en una transacción iKP y símbolos

Dato	Descripción
A, V, C	Participantes en el Protocolo
H(.)	Función hash one way fuerte.
CAN	Número de cuenta del cliente.
ID	ID del vendedor. Identifica al vendedor
TID	ID de la transacción. Único identificador de la transacción
DESC	Descripción de los bienes o servicios de compra, como una cadena oculta. Incluye información del pago tal como el nombre del tarjetahabiente y un número de identificación del banco.
SALT	Número aleatorio generado por C, usado para asegurar la privacidad de la información del pedido en el canal V ↔ A.
NONCE	Número aleatorio generado por el vendedor para proteger de la repetición
DATE	Fecha/Hora actual del vendedor
Y/N	Respuesta desde la tarjeta del emisor. Si/No o un código de autorización
R	Número aleatorio escogido por C para formar CID
CID	Un pseudo-ID del cliente el cual únicamente identifica a C. Computado como CID=H(R_C,CAN).
K	Número aleatorio generado por el vendedor. Usado para unir la confirmación a los mensajes de factura y pago.
K'	Segundo número aleatorio generado por el vendedor. Usado para unir los mensajes de Auto Respuesta y de Respuesta de Aclaración

Datos formados con la combinación de los datos mencionados anteriormente

Dato	Descripción
Common	Información común por todas las partes: A^n, n, val, ID_V, TID_V, DATE, $NONCE_V$, CID, H(DESC,$SALT_C$), [H(W)], [H(W')]
Clear	Información transmitida en la aclaración: ID_V, DATE, $NONCE_V$, H(Common), H(W), A^n
SLIP	Instrucciones de pago: n, val, H(Common), CAN, R_C
EncSlip	Instrucciones de pago encriptadas con la llave pública del adquirente: Kpu_A(SLIP)
CERT.	Certificado de llave pública de X, emitida por un AC
Sig_A	Firma del adquirente en respuesta al mensaje de solicitud de crédito: Kpr_A[H (Y/N, H(Common))]
Sig_A'	Firma del adquirente en respuesta al mensaje de solicitud de crédito: Kpr_A[H (Y/N, Sig_A, W',A^{n-1})]
Sig_V	Firma del vendedor: Kpr_V[H (H(Common),[H(W)], [H(W')])]
Sig	Firma del tarjetahabiente: Kpr_C[H (EncSlip,H(Common))]

Los mensajes básicos son:

- Inicio: El cliente inicia la transacción de pago enviando al vendedor su identidad (CID), la raíz de los valores de las cadenas hash A^n de cada cupón
- Factura: La respuesta del vendedor contiene la identidad del vendedor (ID_V), el identificador de la transacción, la fecha y un nonce. Esos campos son transferidos como parte de Clear. El vendedor y el cliente comparten alguna información, tal como la cantidad y descripción de los bienes (Common). El vendedor crea un message digest a Common y un número aleatorio (W). Forma una firma digital (Sig_V) en los dos resúmenes e incluye éste en la Factura. Permite al cliente verificar que él y el vendedor están de acuerdo en los detalles de la transacción.
- Respuesta de Aclaración: Este es una respuesta firmada desde el adquirente para el vendedor indicando si la transacción de pago fue exitosa o no. Esta contiene una respuesta positiva o negativa también como una firma digital (Sig'_A) en el segundo número aleatorio (W'), el número total de cupones (A^{n-1}), y la firma previa del adquirente (Sig_A).
- Solicitud de Crédito: El cliente envía una solicitud al vendedor que contiene el número total de cupones (n), el valor de cada cupón (val), y el número de la cuenta del cliente en SLIP, éste último es encriptado con la llave pública del adquirente para forma EncSlip. El cliente entonces forma Common y crea un message digest de esto. Esto debe ser igual al enviado por el vendedor en la Factura. Crea una firma digital en EncSlip y H(Common) para formar Sig_C. El cliente envía Sig_C y Encslip al vendedor
- Solicitud de Autorización: Esta solicitud es del vendedor al adquirente para solicitar la transacción de pago. El vendedor crea una firma digital Sig_V. Envía Clear, el hash aleatorio de la descripción de los bienes, EncSlip, la firma del cliente y su firma al adquirente. La transferencia actual de dinero es iniciada en una fecha posterior usando el flujo del mensaje da Respuesta de Aclaramiento
- Respuesta de Autorización: El adquirente envía una respuesta firmada que contiene una indicación de aprobado o falla. Una respuesta de aprobación le da la garantía al vendedor del límite de crédito del cliente.
- Confirmación: El vendedor envía la respuesta firmada al adquirente para el cliente y el primer número aleatorio W. Incluir W en Confirmación le dice al cliente que el vendedor ha aceptado la respuesta de autorización.
- Micropagos: El cliente puede hacer múltiples transacciones de micropago hasta que ha comprado todos los bienes que se requieren para volver a suplir los cupones para el vendedor. El cliente quizá provea el identificador de la transacción con un micropago así que el vendedor puede asociar un cupón con una cadena particular
- Solicitud de Aclaración: El vendedor pregunta al adquirente para ejecutar un pago, y consiste en un número de microgagos.

Micropagos no repetidos

El corredor es el TTP quien actúa como intermediario y colecta los migropagos en medio de un vendedor desde los clientes. El volumen de transacciones procesadas por el corredor es más grande para el contexto de un macropago para ser establecido entre el corredor y los vendedores Los pasos del protocolo son los siguientes:

- El cliente establece una relación de micropago con el corredor. También establece una llave de sesión compartida con el corredor (K_{CB}). Lo ultimo no es parte del protocolo μ-3KP.
- Cuando el cliente quiere hacer una compra desde un vendedor especifico, envía un cupón $A'_{CB}(X)$, el nombre del vendedor (V), y la descripción de los bienes (DESC). En el contexto de WWW, el DESC podría ser una URL. Los campos del mensaje son encriptados usando una llave de sesión compartida establecida anteriormente entre el cliente y el corredor.
- El corredor traduce el cupón del cliente dentro de un cupón para el vendedor $A^{K}{}_{BV}(X)$ y agrega el nombre del cliente y la descripción de los bienes solicitados. Encripta los campos del mensaje con la llave de sesión compartida entre el cliente y el vendedor. El mensaje encriptado es también enviado directamente al vendedor o al cliente, quien lo envía de manera transparente al vendedor.
- El vendedor envía los bienes al cliente.

El tener a un corredor como intermediario no provee ninguna seguridad, pero si simplifica la complejidad de las transacciones en el site del vendedor, como la relación entre vendedor y corredor usualmente es más larga que con compradores. Por lo tanto, más micropagos pueden ser ejecutados por relación de macropago.

Procedimiento de Compra por Internet (iKP)

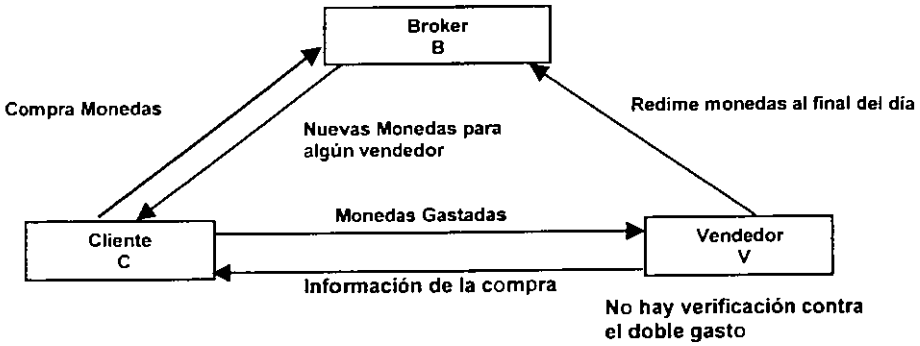
	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	O	□	→	D	▽	
1.	**Generación de cupones**	**comprador**									
.1	Genera cupones de pago										
2.	**Ingreso a Internet**	**comprador**									
.1	Ingresa a Internet.				20	*					
.2	Escribe la dirección de la ubicación de la tienda Virtual				5	*					
3.	**Selección del articulo a adquirir**	**comprador**									
.1	Entra a la tienda virtual				5	*					
.2	Busca el artículo a adquirir			5		*			*		
.3	Selecciona el artículo				5	*					
.4	Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra.				5	*				*	
.5	Muestra el artículo seleccionado				15	*					
4.	**Alta de dirección e-mail de un cliente**	**comprador**									
.1	Se va al botón de nuevo				5	*					
.2	Pide dirección e-mail						*				
5.	**Ingreso de dirección e-mail del cliente**	**comprador**									
.1	Ingresa dirección e-mail				10	*				*	
6.	**Ingresa sus datos el cliente**	**comprador**									
.1	Ingresa su nombre, apellidos, dirección y teléfono en el formulario.			5		*				*	
7.	**Verificación del llenado de los datos**	**vendedor**									
.1	Checa que los campos tengan datos.				5		*				
.2	Muestra los datos ingresados.				5	*					
8.	**Elección de la dirección**	**comprador**									
.1	Tiene que elegir la dirección a la cual quiere que se le envíe el producto.				5	*					
9.	**Muestra datos del cliente y del artículo**	**vendedor**									
.1	Despliega la información del artículo a adquirir y los datos de la dirección de envío				5	*			*		
10.	**Asignación de una cantidad del artículo**	**comprador**									
1	Asigna una cantidad de compra				5	*				*	
11.	**Señalización de las formas de envío**	**vendedor**									
1	Da las diferentes formas de envío y una breve descripción (Nacional/Internacional)				5	*		*			
12.	**Elección de forma de envío**	**comprador**									
1	Elige la opción más adecuada conforme a sus necesidades				5	*				*	
13.	**Indica las formas de pago**	**vendedor**									
1	Pide password y su confirmación				5	*					
2	Menciona los procesos de pago.					*		*			
14.	**Selección de un método de pago**	**comprador**									
1	Ingresa password y confirmación				30	*	*				
2	Selecciona el método de pago				5	*				*	

	DESCRIPCION	RESPONSABLE	TIEMPO			SIMBOLOS					OBS
			Hr	Min	Seg	○	□	→	D	▽	
15.	**Envío de cupones y su identificación.**	**comprador**									
.1	Envía los cupones junto con el valor total de la compra e identificador.										
16.	**Facturación**	**vendedor**									
.1	Envía el mensaje de factura que contiene la identidad del vendedor, el identificador de la transacción, etc.										
17.	**Solicitud de Crédito**	**comprador**									
.1	Envía la solicitud de crédito al vendedor.										
18.	**Autorización de la Solicitud**	**vendedor**									
.1	Verifica los datos enviados.										
.2	Envía este mensaje para el aclaramiento del crédito al adquirente.										
.3	Aclara y autoriza la solicitud.	**adquirente**									
.4	Envía una respuesta de autorización de la solicitud firmada al vendedor.										
19.	**Finalizando la transacción**	**vendedor**									
.1	Envía un mensaje al comprador de que la transacción se concreto o no.										
19.	**Muestra de la orden de compra**	**vendedor**									
.1	Despliega la información total de la compra.				5	*			*		
20.	**Envío del producto**	**vendedor**									
.2	Envía el producto.		25					*	*		
21.	**Recepción del producto**	**comprador**									
.1	Recibe el producto.		700			*					

3.4.5 MicroMint

Desarrollado por Ron Rivest y Adi Shamir. Basado en dinero electrónico que no requiere criptografía de llave pública. Las monedas MicroMint pueden ser gastadas eficientemente con algún vendedor sin necesidad de contactar un banco o broker para verificación en el periodo de compra.

La seguridad provista es poca, pero es el más eficiente de los micropagos.



Dentro de este sistema, las monedas son emitidas por un corredor, quien las vende a los usuarios. Este quizá mantenga cuentas del usuario y del vendedor que pueden ser establecidas usando un esquema de macropago. Un usuario puede gastar las monedas con un vendedor. El doble gasto es posible desde que no verifica su ejecución para ver si una moneda ya fue gastada, en el tiempo de compra. Sin embargo, un corredor registra cuales monedas son emitidas para un usuario. El doble gasto sería detectado, después del fraude, al final del día cuando los vendedores rediman las monedas gastadas con un corredor. Las monedas de los usuarios que son repetidamente gastadas otra vez se colocan en la lista negra y expulsadas desde el sistema.

MicroMint usa un esquema que lo hace muy difícil computacionalmente para alguien excepto al corredor que emite monedas válidas. Sin embargo, es rápido y eficiente para alguien que quiere verificar una moneda.

Una moneda Micromint es una colisión de una función hash k-way. Una función hash one way o message digest mapea a un valor x para un valor y una longitud específica:

$$H(x) = y$$

Una colisión de una función hash ocurre cuando dos o más valores diferentes de x mapean el mismo valor de y

$$H(x_1) = H(x_2) = y$$

Es usualmente duro generar dos valores que mapeen al mismo valor de y. Una colisión de una función hash k-way ocurre cuando k diferentes valores de entrada mapean al mismo valor de salida y.

$$H(x_1) = H(x_2) = H(x_3) = \ldots = H(x_k) = y$$

Si k es igual a 4 (k=4), una moneda MicroMint será una colisión de una función hash de 4-way.

Cada moneda es valuada en un centavo, y la moneda, C, consiste de los 4 valores de entrada que coluden al mismo valor y cuando la función hash es aplicada.

$$C = (x_1, x_2, x_3, x_4)$$

Verificando una moneda

- Ejecutando cuatro funciones hash en cada x, para obtener el mismo valor y

$$H(x_1)\ H(x_2)\ H(x_3)\ H(x_4) = y$$

- Asegurando que cada x es diferente. De otra manera, los valores de x podrían ser colocados para ser el mismo valor, y ellos entonces mapearían al mismo valor y.
- Verificando una moneda sólo prueba que una moneda es auténtica. No será usada para detectar el doble gasto. Para hacer esto, el corredor necesita mantener una copia de cada moneda que ya se gasto para verificarla contra ésta.

Emisión de monedas

La emisión de monedas involucra encontrar los múltiples valores de x de ese hash para el mismo valor de y. Dentro de MicroMint, cada valor de x es restringido para ser de la misma longitud(m bits). La función hash usada definirá la longitud de y (n bits). La función hash deberá mapear cada valor x dentro de algún valor y (H(x)=y). Desde que y es n bits de longitud, hay 2^n posibles valores de y.

Es computacionalmente caro emitir la primer moneda, pero al emitir más monedas después de esa llega a ser progresivamente más barato. Esto es lo que lo hace difícil para un atacante eliminar monedas falsificadas. El corredor puede comprar hardware especial para ejecutar las funciones hash, y para emitir un gran número de monedas será capaz para producir monedas de manera barata, tal como en una emisión de monedas reales.

Costos computacionales

El número de aplicación de un hash es necesitado un promedio para producir la primera moneda (colisiones k-way) es.

$$T = 2^{n/k+1}$$

Donde n es la longitud en bits del valor hash y. El valor k es el número de valores x, de las funciones hash que deben aplicársele al mismo valor y para producir una moneda

Poniendo k=4, n=48, entonces

$$T = 2^{48/4+1} = 2^{13}$$

Para generar la primera moneda por lo tanto requieres 2^{36} o aproximadamente 69 billones de lanzamientos.

Múltiples monedas por bin

El corredor deberá sólo producir un máximo de una moneda desde cada bin. Si más que k pelotas caen dentro del mismo bin, muchas monedas podrían ser hechas desde subconjuntos de valores en el bin. Para un bin con 5 valores, las posibles monedas incluyen

$$C1 = (X1, X2, X3, X4)$$
$$C2 = (X1, X2, X3, X5)$$
$$C3 = (X1, X2, X4, X5)$$

y así sucesivamente.

Sin embargo, un atacante quien obtiene algunas de esas dos monedas pueden generar otras monedas producidas desde este bin. El valor C3 puede ser producido conociendo C1 y C2, por ejemplo. por esta razón, sólo una moneda puede ser producida desde cada bin.

Criterio de validación de monedas

Usando un hardware especial, un corredor será capaz de calcular un gran número de funciones hash en un corto período de tiempo cuando emiten monedas. Sin embargo, para recordar el valor de cada pelota y el bin requerirá espacio de almacenamiento substancial.

Para reducir este requerimiento sin tener que reducir el número de funciones hash ejecutadas, parte del valor hash y de las monedas puede ser requerido para ser igual a un patrón especifico. Sino hay uno igual, la moneda puede ser descartada como inválida. Cuando las monedas son verificadas para vendedores o usuarios, estos son requerimientos de validación que también tendrán que ser checados.

Un valor hash y es dividido en dos partes, el gran orden de bits a y el bajo orden de bits b:

y: a, b

El corredor escoge un valor z que es igual en longitud para a. La elección de z podría ser aleatoria, y deberia ser guardada en secreto mientras las monedas están siendo emitidas. Para que las monedas sean válidas, a (el orden más grande de bits de y) debe ser igual a z

x : a para una moneda buena

Esos valores de x que no sean mapeados para un valor y que satisface este criterio puede ser descartado, y su valores no necesitan ser almacenados. Para la variación de la longitud de a (la parte de y que debe ser igual que el patrón z), el corredor puede controlar el número de lanzamientos de pelotas que tendrán que ser recordadas y que llegarán a ser monedas válidas. Sin embargo, como decrecen los requerimientos de almacenamiento, menos monedas serán producidas por el mismo esfuerzo computacional. En consecuencia, más computación tendrá que ser ejecutada para producir un número adecuado de monedas.

Previniendo el fraude

- Hardware especial: El corredor invierte en hardware que da una ventaja computacional sobre atacantes. El hardware casi consiste de un chip de propósito especial que puede computar valores hash rápidamente. El corredor puede asegurar que los valores hash y requieren mucha computación para descubrir incrementos en la longitud de (y=a,b) requeridos para igualar algún patrón z.
- Corto período de validación de monedas: A las monedas le es dada una corta vida de un mes. Esto da a un atacante menos tiempo para tratar y computar monedas válidas. Las monedas que no son usadas son regresadas para el corredor al final de cada mes.
- Emisor temprano: El corredor iniciará la emisión de monedas adelantándose a su versión. Las monedas que serán usadas en Julio se emiten en Mayo. El corredor tiene mucho más tiempo que un atacante para emitir monedas.
- Criterio de validación de monedas: El corredor revelará un nuevo criterio de validación de monedas al inicio del mes cuando las nuevas monedas son liberadas. Las monedas fraudulentas no pueden ser generadas hasta que éste es conocido. El criterio de validación de monedas puede también ser del valor z, los valores hash deben ser iguales, o esto podría definir H para ser una nueva función hash y guardar el mismo z.
- Diferentes bins (valores y): El corredor no computa todas las posibles monedas , sólo lo suficiente para períodos necesarios. Es como algunas monedas fraudulentas quizá mapean diferentes bins que son usados por el corredor. Para recordar los bins usados por un lote de monedas, un corredor puede detectar monedas fraudulentas viniendo desde otros bins. Un arreglo de bits (una lista indexada de 0's o 1's), con un bit (un solo 0 ó 1) para cada bin (valor y) puede ser usado para este propósito. Para registrar un bin y como se ha estado usando, un 1 es colocado en la posición y en el arreglo. Esos bins que no fueron usados tendrán un 0 en el indice apropiada en el arreglo.
  k > 2 Si las monedas son de colisión de dos caminos, es más fácil computar monedas válidas. El valor de k debería ser más grande que 2. Poniendo k=2 parece trabajar bien en la teoria.
- Extensiones: Además las extensiones son posibles para hacer el fraude más difícil.

Una compra MicroMint

Consiste en el envío de monedas junto con la solicitud de compra para un vendedor. Desde que cada moneda vale un centavo, la cantidad exacta requerida puede ser pagada, y el cambio no es necesario.

No es usada la encripción dentro de MicroMint y los canales de comunicación no son seguros. Las monedas pueden ser robadas e interceptadas en alguno de los pasos. Si éste es un problema de comunicación usuario / corredor y vendedor / corredor puede ser encriptado usando un acuerdo de llaves de encripción. Esto es una emisión de implementación y los detalles no son provistos en el esquema MicroMint. La solución encriptada no es adecuada para las ligas de comunicación entre un usuario y un vendedor no conocido. Esto requeriría encripción de llave pública cara y certificados para asegurar la liga.

Doble gasto

La verificación no es ejecutada en el vendedor contra el doble gasto. Si las monedas son válidas, el artículo de compra es regresado Aunque no ofrece anonimato, el corredor detectara las monedas de doble gasto sólo cuando el vendedor las redima. Los fraudes del vendedor y del usuario son posibles. Los vendedores quizá rediman monedas ya gastadas en otros vendedores. El corredor quizá no sea capaz de distinguir si un usuario o vendedor están cometiendo el fraude.

El corredor registra al usuario, el cual emite las monedas, y el vendedor desde el cual son recibidas las monedas, entonces guarda la ruta de muchas monedas de doble gasto son conectadas con cada usuano o vendedor. Repetidos atacantes son agregados en la lista negra y deniega acceso adicional al sistema. Los diseñadores sienten que alguna pequeña escala de doble gasto es aceptable. Los propósitos que un corredor no paga a un vendedor para una moneda ya gastada.

4. PROTOCOLOS

Un protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica.

El ejemplo más común es SSL (Secure Sockets Layer) que vemos integrado en el Browser de Netscape y hace su aparición cuando el candado de la barra de herramientas se cierra y también si la dirección de Internet cambia de HTTP a HTTPS, uno más es el conocido y muy publicitado SET que es un protocolo que permite dar seguridad en las transacciones por Internet usando tarjeta de crédito.

Estos y cualquier protocolo de seguridad procura resolver algunos de los problemas como la integridad, la confidencialidad, la autenticación y el no repudio, mediante sus diferentes características.

Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

4.1 De la Capa de Comunicaciones

Son protocolos que permiten que propiedades como privacidad, autenticidad, integridad y no repudiación existan en el nivel del flujo de las comunicaciones o de la transmisión de un objeto. Al entrar en un comercio en Internet, quizá se autentique a un usuario con una tarjeta de crédito válida, y todas las demás comunicaciones durante la transacción serán seguras.

4.1.1 SSL (Secure Socket Layer)

El crecimiento reciente de Internet y el WWW ha traido la necesidad de proteger las comunicaciones sensitivas enviadas sobre una red abierta. Secure Socket Layer (SSL), protocolo de seguridad desarrollado por un staff de Netscape Corporation en 1994. Proporciona privacidad en las comunicaciones en Internet. El protocolo permite que las aplicaciones cliente/servidor se comuniquen en un camino diseñado para prevenir que alguien se entrometa, o se falsifiquen mensajes.

Se compone de dos capas, que se encuentran sobre el protocolo de transporte.

- Protocolo SSL de Registro. Se usa para la encapsulación de varios protocolos de niveles más altos.
- Protocolo SSL Handshake. Permite al servidor y a cliente autenticarse el uno al otro y negociar un algoritmo del cifrado y llaves criptográficas, antes de que el protocolo de aplicación transmita o reciba el primer byte de datos.

El objetivo principal de SSL es proporcionar privacidad y confiabilidad entre dos aplicaciones cliente/servidor.

1. Seguridad de criptográfica
   SSL debería ser usado para establecer una conexión segura entre dos partes.

2. Interoperabilidad
   Los programadores independientes deben ser capaces de desarrollar aplicaciones que utilizan SSL 3.0 para poder intercambiar los parámetros criptográficos con éxito sin el conocimiento de algún otro código.
   Nota: No ocurre en todos los casos de las instancias de SSL se podrá conectar con éxito.

3. Extensibilidad
   SSL busca proporcionar un marco en los métodos de encripción de llave pública y bulk que puedan incorporarse como sea necesario. Esto también tiene sus objetivos:

   - prevenir la necesidad de crear un nuevo protocolo (y arriesgarse a nuevas debilidades), y
   - evitar la necesidad de implementar una nueva biblioteca de seguridad.

4 Eficiencia Relativa
   Las operaciones criptográficas tienden a ser altamente intensivas en CPU, particularmente las operaciones de llave pública. Por esta razón, el protocolo de SSL ha incorporado una sesión opcional que esconde el esquema para reducir el número de conexiones que necesitan ser establecidas desde el principio. Se reduce la actividad de la red

Ventajas

- Es un protocolo de aplicación independiente.
- Un protocolo de un nivel más alto puede colocarse transparentemente encima de SSL.
- Soporta muchas aplicaciones y protocolos.
- Su uso es disponible basado en redes TCP/IP.
- Las aplicaciones necesitan soportar SSL, pero no necesitan preocuparse acerca de la generación de llaves y técnicas de negociación
- La privacidad se da a través de la encripción. La información puede ser interceptada, pero será más difícil su lectura sino conoces las llaves de encripción.
- Se asegura la integridad a través de la encripción.
- Se provee autenticación a través de certificados digitales.
- Funciona con Internet Explorer y Netscape Navigator

Desventajas

- Tamaño de la llave: limitada a 40 bits.
- Incertidumbre: mucha gente se siente insegura al dar sus datos, por ejemplo de tarjetas de crédito por Internet, porque sienten que no están seguros.

La seguridad de las conexiones SSL tienen 3 propiedades básicas:

1) Conexión privada. La encripción es usada después del handshake inicial para definir una llave secreta. La criptografía simétrica se usa para el encripción de los datos (DES[DES], RC4[RC4], etc.)
2) La identidad de las partes puede ser autenticada usando criptografía de llave pública, criptografía (RSA[RSA], DSS[DSS], etc.).
3) Conexión confiable. El transporte del mensaje incluye la verificación de la integridad del mensaje usando un MAC codificado. Las funciones hash seguras (SHA, MD5, etc.) se usan para calcular el MAC

Funcionamiento de SSL

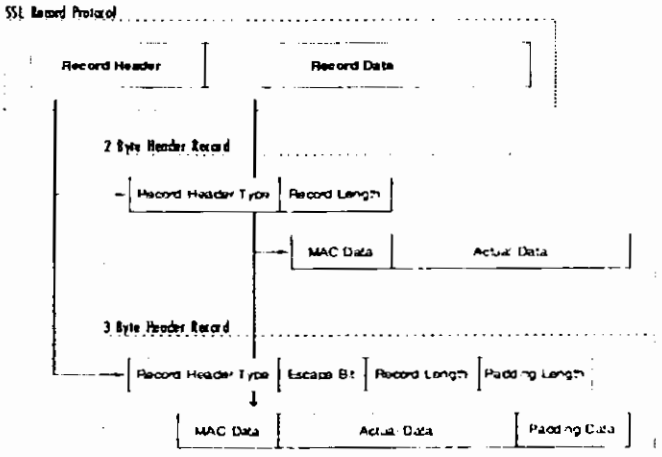
Protocolo transparente para la aplicación en la que se usa. Una vez que ambos lados son equipados con la implementación de SSL, los datos de la aplicación deberían pasar a través del socket seguro del mismo modo como un socket normal (inseguro)

SSL se divide en dos capaz, cada una usa los servicios provistos por una capa baja y proveen funcionalidad a capas altas. La capa de registro SSL provee confidencialidad, autenticidad y repite protección sobre una conexión confiable de protocolos de transporte como TCP. Las capas anteriores a la capa de registro son el protocolo handshake, un protocolo de intercambio de llaves el cual inicializa y sincroniza criptográficamente el estado en dos endpoints. Después el protocolo de intercambio de llaves se completa, los datos de la aplicación sensitiva pueden ser enviados vía la capa de registro.

Fallas en SSL 2.0

- Innecesariamente debilitan las llaves de autenticación a 40 bits.
- Usa un MAC débil, aunque el post-cifrado parece detener los ataques.
- Alimenta bytes de relleno dentro del MAC en un modo de cifrado de bloque, pero deja la longitud del campo del relleno sin autenticar, lo que quizá permita a atacantes activos borrar bytes desde el final de los mensajes. Hay un ataque rollback de suite de cifrado, donde un atacante activo edita la lista de preferencias de la suite de cifrado en los mensajes hello, para forzar invisibles endpoints a usar una forma de cifrado más débil, que de otra manera escogería, esta falla seria limita la fortaleza a una seguridad de un mínimo común denominador cuando ataques activos son una amenaza

a) Protocolo De Registro



Asumimos que el protocolo de intercambio de llaves tiene seguramente un estado de sesión, llaves y parámetros de seguridad.

En SSL, todos los datos enviados son encapsulados en un registro, compuesto de una cabecera y una cantidad de datos non-zero. Cada cabecera del registro contiene un código de 2 a 3 bytes de longitud. Si el bit más significativo es colocado en el primer byte del código de longitud de registro, entonces el registro no tiene relleno y el total de la longitud de la cabecera será de 2 bytes, de otra manera el registro tiene relleno y el total de la longitud de la cabecera será 3 bytes. La cabecera de registro es transmitida antes de la porción de datos del registro.

Cuando la longitud de la cabecera es tres, el segundo bit más significativo en el primer byte tiene un significado especial. Cuando es cero, el registro que está siendo enviado es un registro de datos. Cuando es uno, el registro que está siendo enviado es un escape de seguridad. El código de la longitud describe cuantos datos están en el registro. El código de longitud de registro no incluye el número de bytes consumidos por la cabecera de registro.

La cabecera de registro define un valor llamado relleno (padding). El valor de relleno especifica cuantos bytes de datos fueron agregados al registro original por el emisor. Los datos de relleno son usados para hacer que la longitud del registro sea un múltiplo del tamaño de los bloques de cifrado, cuando son usados para encripción

El emisor de un registro de relleno agrega los datos de relleno al final de sus datos normales, entonces cifra la cantidad total. El valor actual de los datos de relleno es menos importante, pero la forma encriptada debe ser transmitida para el receptor propiamente decriptando el registro. Una vez que la cantidad total está siendo

transmitida, es conocido que la cabecera puede ser construida propiamente con el conjunto de valores de relleno

El receptor de un registro rellenado decripta los datos de registro, para obtener el dato en claro, entonces substrae el valor de relleno de la longitud del registro para determinar la longitud del registro final. La forma en claro de los datos de relleno debe ser descartada.

Los datos que componen un registro SSL son:

```
MAC_DATA[MAC_SIZE]
ACTUAL_DATA[N]
PADDING_DATA[PADDING]
```

ACTUAL_DATA: Son los datos actuales que están siendo transmitidos.
PADDING_DATA: Son los datos de relleno enviados cuando un bloque de cifrado es usado y el relleno es necesitado.
MAC_DATA: Es el MAC (Message Autentication Code/ Código de Autenticación de Mensajes).

Si los registros SSL son enviados en claro, la cantidad de PADDING_DATA y de MAC_DATA será cero. Cuando la encripción es un efecto, el PADDING_DATA será una función del tamaño del texto cifrado. El MAC_DATA es una función de CIPHER_CHOICE.

El MAC_DATA se calcula como sigue:

```
MAC_DATA = HASH (SECRET, ACTUAL_DATA, PADDING_DATA, SEQUENCE_NUMBER)
```

SEQUENCE_NUMBER es un valor de 32 bits que se presenta en la función hash como cuatro bytes, con el primer byte es el byte más significativo, y así sucesivamente con los otros 3 bytes.

El MAC_SIZE es una función hash, MD2 y MD5, el MAC_SIZE será 16 bytes (128 pedazos).

El valor SECRET es una función de la parte que está enviando el mensaje. Si el cliente está enviando el mensaje entonces el SECRET es el CLIENT_WRITE_KEY (el servidor usará el SERVER_READ_KEY para verificar el MAC). Si el cliente está recibiendo el mensaje entonces el SECRET es el CLIENT_READ_KEY (el servidor usará SERVER_WRITE_KEY para generar el MAC).

El SEQUENCE_NUMBER es un contador que se incrementa por el emisor y el receptor. Para cada dirección de la transmisión, un par de contadores se guarda (uno emisor, uno receptor). Cada vez que un mensaje es enviado por un emisor el contador se incrementa. Los números de la secuencia son cantidades de 32 sin firmar y deben volver a cero después de que el incremento haya transcurrido hasta 0xFFFFFFFF.

El receptor de un mensaje usa el valor esperado de la secuencia numérica como la entrada del MAC en la función HASH. Los MAC_DATA calculados deben ser iguales bit por bit con el MAC_DATA transmitido. Si la comparación no es idéntica entonces el registro es considerado dañado, y será tratado como si un "Error de I/O" hubiera ocurrido (es decir un error irrecuperable se afirma y la conexión está cerrada).

Un último chequeo de consistencia se hace cuando el bloque de cifrado se usa y el protocolo está usando encripción. La cantidad de datos presentados en un registro (RECORD_LENGTH) debe ser un múltiplo del tamaño del bloque cifrado. Si el registro recibido no es un múltiplo del tamaño del bloque cifrado entonces el registro es considerado dañado, y será tratado como si un "Error de I/O" hubiera ocurrido (error irrecuperable y la conexión es cerrada).

El Protocolo de Registro SSL se usa en todo momento por el cliente y el servidor.

Para una cabecera de dos bytes, la longitud máxima del registro es de 32767 bytes. Para la cabecera de tres bytes, la longitud máxima del registro es de 16383 bytes. Los mensajes del protocolo handshake de SSL encaja un solo registro, del protocolo de registro SSL.

Antes de que el primer registro sea enviado usando SSL todos los números de la secuencia se inicializan a cero. La transmisión del número de la secuencia se incrementa después de que cada mensaje es enviado, inicia con los mensajes CLIENT_HELLO y SERVER_HELLO.

Ataques y Soluciones del Protocolo de Registro

a) Confidencialidad: Intruso: Este protocolo cifra todos los datos de la capa de aplicación con un cifrado y una llave de sesión definida en el protocolo handshake. Una extensa variedad de fuertes algoritmos usada en modos estándar, están disponibles en las preferencias de la suite local y cada aplicación deberá ser capaz de encontrar el algoritmo de seguridad conforme al nivel de seguridad requerido. La administración de llaves está bien manejada. las llaves de sesión son generadas por aplicar el hash a aleatorios a salts de preconexión y aún secreto compartido fuerte.

b) Análisis Del Trafico: El análisis del tráfico es otro ataque pasivo persigue recobrar la información confidencial acerca de la protección de sesiones examinando paquetes de campos sin encriptar y paquetes de atributos sin proteger. Por ejemplo fuentes IP sin encriptar y direcciones de destino (puertos TCP), o examinando el volumen de flujo del tráfico de la red, un analista de tráfico puede determinar que partes interactúan, que tipo de versiones están en uso, y algunas veces recobrar información de negocios o de relaciones personales.

El checar las longitudes de texto cifrado pueden revelar información acerca de la petición URL en SSL o en el tráfico de Web cifrado en SSL. Cuando un Web browser se conecta a un Servidor Web vía SSL, la petición GET contenida en el URL es transmitida en forma encriptada. Exactamente la página Web que fue bajada por el browser fue claramente considerada como información confidencial, el análisis de tráfico puede recobrar la identidad del servidor Web, la longitud de la petición de URL, y la longitud de los datos html regresados por el servidor Web. Lo anterior permite a un intruso descubrir que página Web fue accesada.

La vulnerabilidad se da porque la longitud del texto cifrado revela la longitud del texto plano. Incluye soporte para bits aleatorios que complementan los modos de cifrado de bloques. SSL debe soportar el uso de longitudes de bits aleatorias que complementan todos los modos de cifrado, y también deberían considerarse fuertemente requeridas para ciertas aplicaciones.

c) Ataques Activos: El ataque corta y pega, es un ataque activo en ipsec. El lograr confidencialidad usando encripción no es suficiente. Explota el principio de que la aplicación más al extremo trata hacia el interior de los datos cifrados, diferentemente dependiendo del contexto, proteger es más asiduamente cuando aparece más en algunas formas que en otras. Modo de cambio de bloques de cifrados: éste se recupera desde errores dentro de un bloque, trasplantando así pocos cifrados de bloque consecutivos entre locaciones dentro de resultados de texto cifrado en flujo, en una transferencia correspondiente de bloques de texto plano, excepto para un error de bloque al inicio de la unión. Este ataque corta un texto cifrado encriptado desde algún paquete que contiene datos sensitivos, y los une dentro del texto cifrado de otro paquete el cual es cuidadosamente escogido así que será probable que los endpoint receptores se escapen inadvertidamente a su texto plano después de su desencripción. Por ejemplo, si fuera posible uno de estos ataques en la capa de registro, podrá ser usado para comprometer la seguridad del site: el ataque en un servidor SSL a una transferencia de página Web del cliente se le podría unir el texto cifrado desde una parte sensitiva de la transferencia de html, dentro de la porción del hostname de un URL, incluido en otra parte en la página Web transferida, así que cuando un usuario da click en la trampa de la liga URL su browser podría interpretar la decripción de los datos sensitivos unidos al texto cifrado como un hostname y envía a un nombre de dominio DNS buscándolo en claro, listo para ser capturado por el atacante. Este ataque enlista receptores confiados para decriptar y se escaparan inadvertidamente datos sensitivos para ellos.

SSL 3.0 detiene este ataque. usando llaves de sesión independientes para cada dirección de cada encarnación de cada conexión. Todavía el cortado y pegado dentro de una dirección de una transferencia no es prevenido dentro de este mecanismo. La defensa contra este ataque usa autenticación fuerte en todos los paquetes encriptados, para prevenir modificaciones enemigas de los datos del texto cifrado. El protocolo de registro emplea esta defensa, frustrando estos ataques.

El ataque de cortos bloques es otro ataque activo de ipsec, se aplica principalmente contra datos TCP protegidos ipsec DES-CBC cuando al final del bloque del mensaje contiene un corto byte de texto plano y el resto es llenado por bits aleatorios. Uno supone que en el byte de texto plano, sin conocerlo reemplazan el bloque final de texto cifrado con otro bloque de texto cifrad, desde un par de texto cifrado y plano escogido. Las suposiciones correctas pueden ser reorganizadas para validar el checksum de TCP: una incorrecta suposición causará que el paquete sea silenciosamente dejado por el stack TCP del receptor, pero la correcta suposición causará un reconocible ACK para ser regresado. El conocimiento del correspondiente texto plano para un reemplazo correcto de bloques de texto cifrado habilitara al enemigo a recuperar el byte de texto plano sin conocer. Porque los stacks ipsec recibidos ignoran los bytes de relleno, los ataques de bloques cortos requieres de 2^8 de texto plano conocido y 2^8 procesos en línea activos para recuperar el rastro del byte sin conocer

No hay obvios ataques de bloques cortos en SSL, pero el formato del protocolo de registro de SSL es similar a las viejas vulnerabilidades de la estructura de ipsec, por lo que alguna modificación de este ataque puede actuar contra SSL. No es algo probable ya que los servidores Web de cifrado SSL no permiten cifrar pequeños bloques.

d) Autenticación de mensajes: Protege confidencialidad de los datos de la aplicación, SSL cnptográficamente auténtica las comunicaciones sensitivas.

Protege la integridad de los datos de la aplicación usando un MAC criptográfico, usan el HMAC, que es un hash rápido y fuerte. En un área donde muchos ad-hoc propuestos para MACs han sido criptoanalizados, esos resultados probables de seguridad son muy atractivos. Parece improbable que HMAC sea roto en un futuro cercano

Se indica que SSL 3.0 usa una versión muy vieja y obsoleta de la construcción de HMAC. Debería de actualizarse al HMAC actual, para máxima seguridad.

SSL 3.0 se ve muy seguro contra ataques criptoanaliticos o directamente exhaustivos en el MAC. SSL 2.0 tiene fallas serias de diseño debido al uso de un MAC inseguro –aunque la post-encripción salve esto desde ser una directa vulnerabilidad- pero SSL 3.0 ha compuesto este error. Las llaves MAC de SSL contienen por lo menos 128 bits de entropía, incluso en exportar modos debilitados, lo cual debería proveer seguridad para la implementación de exportación debilitada y doméstica. Independientemente de las llaves usadas para cada dirección de cada conexión y para cada nueva encarnación de una conexión. El tener HMAC debería detener los ataques criptoanalíticos. No provee servicios de no repudio, y parece razonable deliberadamente dejar esos protocolos especiales de aplicación de capa de más alto nivel.

e) Ataques de Repetición: SSL protege contra ataques de repetición incluyendo un número de la secuencia en datos con MAC. Este mecanismo también protege contra retardos, reordenes, o datos borrados. Los números de la secuencia son de 64 bits de longitud, y empaquetarlos o guardarlos no debería ser un problema, se mantienen separadamente para cada dirección de cada conexión, y son actualizados en cada nuevo intercambio de llaves, no hay vulnerabilidades obvias.

El principio Horton

Provee protección de la integridad del mensaje, cuando los datos pasados desde la capa de registro SSL del receptor a la aplicación protegida, exactamente marcan los mismos datos emitidos por la aplicación protegida del emisor para la capa de registro SSL del emisor. Significa aproximadamente, que no es suficiente aplicar un MAC seguro para los datos de la aplicación como su transmisión sobre el canal –también se debe autenticar algún contexto que el mecanismo de SSL dependa de interpretar los datos de la red entrantes. Lo antenor es denominado "Principio Horton". SSL lo queremos para

"Autenticar lo que significa, no lo que se dice"

de otra forma

"evitar la no autenticación del contexto crítico de seguridad"

SSL 2.0 tiene por lo menos una falla a lo largo de estas líneas: incluir los datos de relleno pero no la longitud del relleno en la entrada del MAC, así un atacante activo puede manipular el texto en claro que rellena la longitud del campo para comprometer la integridad del mensaje.

```
Análisis del contexto crítico de seguridad

Encrypted fragment**
                [read key*, read IV (1)]
padded compressed fragment
                [cpher type* (2)]
SSLCompressed.fragment
                [CompressionMethod*]
SSLPlaintext.fragment
                [ContentType**(3), ProtocolVersion, SSLPlaintext.length**]
"protocol"
```

Notas:

* Estado de sesión sincronizada por el protocolo de intercambio de llaves
** Protegido por el MAC
1) read_IV es inicialmente tomada desde el estado de la sesión, después tomada desde el último bloque de texto cifrado del previo encrypted_fragment
2) para cifrados de bloque, el relleno es removido desde el final del fragmento rellenado.

La protocolo de registro SSL depende mucho del contexto a interpretar, descifrar, descomprimir, demultiplexar y despachar datos desde el canal (cable).

SSL 3.0 sigue el principio Horton, una excepción menor es que la integridad del campo ProtocolVersion no es protegida (Específicamente al campo SSLCiphertext.ProtocolVersion en el protocolo de registro, no en el campo ClientHello client_version desde el protocolo handshake, éste es protegido pero el anterior no) Si el campo ProtocolVersion si siempre es usado por SSL, debería ser autenticado; sino, no debería presentarse en el formato del paquete. También, es el resultado final del valor del procesamiento de entrada, que es un flujo de bytes desde el flujo de datos de la aplicación, y los límites no son preservados.

b) Protocolo De Intercambio De Llaves o HandShake

El Protocolo Handshake SSL tiene dos fases principales. La primera fase se usa para establecer las comunicaciones privadas. La segunda fase se usa para la autenticación del cliente.

Fase 1

La primera fase es de conexión inicial dónde, el protocolo handshake hace un trabajo inicial para establecer las identidades de las partes y negociar parámetros criptográficos para la sesión Además los datos de la aplicación son manipulados, en acuerdo con esos parámetros y enviados en paquetes de datos de aplicación a través de la conexión del socket subyacente.

Dentro del protocolo handshake, hay una gran variedad de opciones dependiendo de si el cliente, el servidor, o ambos serán autenticados, y que algoritmo de cifrado e intercambio de llaves debería ser usado

Un típico proceso handshake, se da cuando la aplicación del cliente inicia una conexión al servidor, la capa de registro SSL emite un mensaje Hello del cliente. Contiene 28 bytes de datos producidos por un generador de números aleatorios seguros en suma para una lista de métodos criptográficos del cliente y de compresión,

listados en orden de su preferencia. Un ID único de sesión es también establecido y puede ser usado para permitir que esta sesión sea resumida después en una conexión subsecuente.

Ambas partes comunican sus mensajes "hello". El cliente comienza la conversación enviando el mensaje CLIENT_HELLO. El servidor recibe el mensaje CLIENT_HELLO y procesa éste respondiendo con el mensaje SERVER_HELLO.

A estas alturas el cliente y el servidor tienen bastante información para saber si o no se necesita una nueva llave maestra. Cuando una nueva llave maestra no se necesita, el cliente y el servidor proceden a la fase 2 inmediatamente.

Cuando una nueva llave maestra se necesita, el mensaje SERVER_HELLO contendrá bastante información para que el cliente la genere. Esto incluye el certificado firmado del servidor, una lista de especificaciones del cifrado bulk, y un conexión-id (valor al azar generado por el servidor que se usa por cliente y servidor, durante una sola conexión). El cliente genera la llave maestra y responde con un mensaje CLIENT_MASTER_KEY (o un mensaje de ERROR si la información del servidor indica que cliente y servidor no pueden acordar un cifrado bulk)

Debe notarse aquí que cada endpoint de SSL usa un par de cifrados por conexión (para un total de cuatro cifrados). Para cada endpoint, un cifrado es usado para las comunicaciones salientes, y uno se usa para las comunicaciones entrantes. Cuando el cliente o el servidor generan una llave de sesión, ellos generan dos llaves, SERVER_READ_KEY (conocida como CLIENT_WRITE_KEY) y SERVER_WRITE_KEY (conocida como CLIENT_READ_KEY). La llave maestra se usa por cliente y servidor para generar varias llaves de sesión.

Finalmente, el servidor envía un mensaje SERVER_VERIFY al cliente después de que la llave maestra ha sido determinada. Este paso final autentica al servidor, porque sólo un servidor que tiene la llave pública apropiada puede saber la llave maestra.

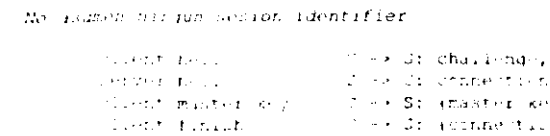
Fase 2

La segunda fase es la fase de la autenticación. El servidor ya ha sido autenticado por el cliente en la primera fase, esta fase se usa para autenticar al cliente principalmente. En típico escenario, el servidor requerirá algo del cliente y enviará una petición. El cliente contestará positivo si tiene la información necesitada, o enviará un mensaje de ERROR sino . Esta especificación protocolar no define la semántica de una respuesta de ERROR a una petición del servidor (por ejemplo, una aplicación puede ignorar el error, cerrar la conexión, etc. y todavía conforma a esta especificación).

Cuando una parte está autenticando a la otra parte, envía su mensaje finished. Para el cliente, el mensaje CLIENT_FINISHED contiene la forma encriptada del CONNECTION_ID para verificar al servidor. Si la comprobación falla, el servidor envía un mensaje de ERROR.

Una vez que una parte ha enviado su mensaje finished, éste debe continuar escuchando los mensajes hasta que recibe un mensaje finished. Una vez que ambas partes han enviado un mensaje finished y han recibido el mensaje finished, el protocolo handshake SSL es concluido. En este punto el protocolo de aplicación empieza a operar (Nota: el protocolo de aplicación continúa siendo el layered en el SSL Registro Protocolo)

Los flujos típicos del protocolo del mensaje son:



Asumiendo un sesion-identifier que fue encontrado por ambos cliente y servidor

➢	client-hello	C -> S: challenge, session_id, cipher specs
➢	server-hello	S -> C: connection-id, session id hit
➢	client-finish	C -> S: {connection-id}client_write key
➢	server-verify	S -> C: {challenge}server_write key
➢	server-finish	S -> C: {session id}server write key

Asumiendo un sesion-identifier que fue usado y una autenticacion del cliente es usada

```
client-hello        C -> S: challenge, session id, cipher specs
server-hello        S -> C: connection-id, session id hit
client-finish       C -> S: {connection-id}client write key
server-verify       S -> C: {challenge}server write key
request-certificate S -> C: {auth type,challenge'} server write key
client-certificate  C -> S: {cert type,client cert, response data}client write key
server-finish       S -> C: {session id}server write key
```

Ataques y Soluciones del Protocolo Handshake

a) Ataques Rollback De Suites De Cifrado. El protocolo de intercambio de llaves en el SSL 2.0 tiene una serie de fallas: un atacante activo podria silenciosamente forzar a un usuario doméstico para usar cifrado debilitado de exportación, si ambas partes apoyan y prefieren algoritmos de grado fuerte. Es conocida como un ataque rollback de suites de cifrado, puede ser ejecutado editando la lista de texto claro de apoyo a las suites de cifrado enviada en los mensajes hello. SSL 3.0 arregla esta vulnerabilidad para autenticar todos los mensajes del protocolo handshake con la ayuda de la llave secreta, la persona que se entrometa podrá ser determinada al final del handshake y si es necesario la sesión se terminará.

Todos los mensajes iniciales del handshake son enviados, sin protección, en claro. En vez de modificar los parámetros en uso en ese momento, el protocolo de intercambio de llaves modifica un estado de sesión pendiente. Después de que la negociación se completa, cada parte envía un pequeño mensaje denominado change cipher spec (CCS), el cual simplemente alerta a otro para actualizar el estado de sesión pendiente a actual. El nuevo estado de la sesión es usado iniciando con el siguiente mensaje, sin embargo el mensaje change cipher spec no está protegido. Después del change cipher spec viene el mensaje finished (terminado), el cual contiene un MAC de todos los mensajes del protocolo handshake cifrados por la llave maestra (por razones de no seguridad, los mensajes CCS y el de alerta no son autenticados en el mensaje finished). La llave secreta de 48 bytes nunca es revelada; en vez de eso, las llaves de sesión son generadas desde ésta. Asegura que aún si las llaves de sesión son recuperadas, la llave maestra guardará el secreto, así que los mensajes del protocolo handshake seguramente serán autenticados.

b) Dejando Caer El Mensaje CCS: En el protocolo de intercambio de llaves el mensaje CCS, no es protegido por el mensaje de autenticación en el mensaje finished. Permite al criptoanalista realizar un ataque. El flujo normal de SSL es:

```
→ {CCS}
→ {finished}
→ 'CCS'
→ {finished}
→ m
```

Donde $\{\}_K$ representa la transformación criptográfica de codificación usada para la capa de registro, m denota un mensaje de texto plano enviado después de que el intercambio de llaves es terminado, y a representa el código de autenticación del mensaje finished, el cual es obtenido computando un MAC simétrico en los mensajes handshake anteriores (excluyendo CCS). Antes de recibir un mensaje CCS, la actual suite de cifrado no ofrece algoritmos de cifrado y autenticación, las suites pendientes incluyen la suite de cifrado negociada, al recibir un mensaje CCS, las implementaciones son supuestas para copiar la suite de cifrado pendiente a la actual y habilitan protección criptográfica en la capa de registro.

Existe un ataque que toma ventaja de la falta de protección de los mensajes CCS. Nosotros asumimos el caso especial donde la suite de cifrado negociada incluye sólo la protección del mensaje de autenticación y el no cifrado. El atacante activo intercepta y borra los mensajes CCS, así que las partes nunca actualizarón su actual suite de cifrado; en particular, las partes nunca habilitaron la autenticación de mensajes o cifrado en la capa de registro para paquetes de entrada. Ahora el atacante permite que el resto de la interacción proceda, despojando de la capa de registro los campos de autenticación desde mensajes finished y datos de sesión. En este punto no hay protección de la autenticación para datos de sesión, y el atacante activo puede modificar según su voluntad los datos de sesión transmitidos. El impacto es que, cuando una autenticación es negociada, un atacante activo puede derrotar la protección de la autenticación en los datos de sesión, transparentemente provocando a ambas partes aceptar los datos de sesión de entrada sin ninguna protección de integridad criptográfica. Ataque:

C → M	[CCS]
C → M	{finished:} $\{a\}_K$
M → S	{finished:} a
S → M	[CCS]
S → M	{finished:} $\{a\}_K$
M → C	{finished:} a
C → M	$\{m\}_K$
M → S	m

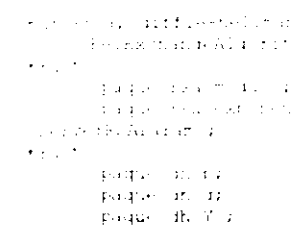
$\{m\}_K$ denota la transformación de un mensaje m junto con un campo de autenticación del mensaje cifrado por k, dando $\{m\}_K$ es fácil dejar el campo de MAC y recuperar {m}, sino es usada la encripción aqui. El atacante puede remplazar fácilmente los datos de sesión sin protección m por datos falsificados de su elección.

Vale la pena que pase cuando la suite de cifrado negociada incluye encripción. Entonces el mensaje finished del cliente es enviado cifrado, pero el servidor espera recibirlo sin cifrar, no basta dejar el campo de MAC – envez de eso, el atacante debe recuperar la llave de cifrado k y descifrar $\{a\}_K$ para obtener a. Por lo tanto el ataque será frustado cuando la suite de cifrado negociada incluya una encripción fuerte. En el caso intermedio donde la encripción usada sea débil (modo exportable de 40 bits), el atacante quizá sea capaz de realizar este ataque, si es posible ejecutar una búsqueda de llaves online eshaustiva para recuperar la corta llave de encripción. En tiempo real esta búsqueda de cifrados de 40 bits, actualmente está fuera del alcance de muchos atacantes, aunque en un futuro será posible.

El arreglo más simple que requiere es una implementación que reciba un mensaje CCS antes del mensaje finished. Un arreglo más radical incluye el mensaje CCS dentro del cálculo del mensaje de autenticación del mensaje finished. Ambos arreglos requerirían cambios en las especificacions de SSL, pero haria el protocolo más robusto.

c) Algoritmo Rollback De Intercambio De Llaves: El protocolo handshake de SSL 3.0 contiene fallas en el diseño. Un servidor puede enviar parámetros de llave pública de corta vida, firmando bajo un gran término de llave de firma certificada, en el mensaje de intercambio de llave del servidor. Muchos algoritmos de intercambio de llaves son soportados (RSA, Diffie-Hellman). Desafortunadamente, la firma en los parámetros de vida corta no protegen el campo que especifica el tipo de algoritmo de intercambio de llaves que se usa.

Estructuras de datos del mensaje de intercambio de llave del servidor:



```
struct {
      select (KeyExchangeAlgorithm) {
            case diffie-hellman:
                  ServerDHParams params;
                  Signature singed_params
            case rsa:
                  ServerRSAParams params;
                  Signature singed_params

} ServerKeyExchange;
```

Los campos de signed_params contienen la firma del servidor en un hash del campo ServerParams, pero la firma no cubre el valor del KeyExchangeAlgorithm. Por lo tanto, para modificar el campo (sin protección) KeyExchangeAlgorithm, podemos abusar de la legitimidad de la firma del servidor en un conjunto de parámetros Diffie-Hellman y hacer pensar al cliente que el servidor firmó un conjunto de parámetros RSA.

Ejecutando un ataque rollback de una suite de cifrado coacciona al servidor usando un algoritmo de intercambio de llaves Diffie-Hellman. Modificar el mensaje de intercambio de llaves del servidor, cambiando el campo KeyExchangeAlgorithm para seleccionar intercambio de llaves RSA pero abandonado el campo de ServerParams y sin tocar la firma del servidor. El servidor Diffie-Hellman módulo primo p (dh_p) y el generador g (dh_g) probablemente serán interpretados por el cliente como una firma de corta vida RSA k^9 modulo p (rsa_modulus) con exponente g (rsa_exponent). El cliente encripta el PreMasterSecret con los falso valores RSA. Intercepta los valores de encripción RSA k^9 modulo p, recuperando k, el PKCS codifica el PreMasterSecret tomando g-th rutas, que pueden hacerse eficazmente desde p primo. Ahora que es comprometido el PreMasterSecret, es fácil engañar al resto del intercambio de llaves, incluyendo al mensaje finished falsificado, para ambos. Por lo tanto uno puede decriptar todos lo datos sensitivos de la aplicación transmitidos o datos falsificados en la conexión SSL; toda la protección criptográfica ha sido totalmente derrotada. El ataque es:

```
[Client hello:]
C → M          SSL_RSA...
M → S          SSL_DHE_RSA...
[Server hello:]
S → M          SSL_DHE_RSA...
M → C          SSL_RSA...
[Server key exchange:]
S → M          {p,g,y}   , diffie-hellman
M → C          {p,g,y}   , rsa
[Client key exchange:]
C → M          k^9 mod p
M → S          g  mod p
```

Al final del intercambio de llaves, el valor del PreMasterSecret del cliente es k, mientras que el valor del servidor es g^{xy} mod p donde x fue escogido por el atacante M; ambos son conocidos por el atacante, y todos lo secretos son derivados desde esos valores, todas las transformaciones criptográficas subsecuentes que no ofrecen protección contra M.

d) Ataques De Repetición Con Intercambio De Llaves Anónimo. El algoritmo estándar de intercambio de llaves de firma une a la firma en los parámetros criptográficos de corta vida a la conexión aplicando hash con los nonces del servidor y el cliente, pero debido a alguna vigilancia, el intercambio anónimo de llaves no ejecuta esta unión. Por lo tanto, si se puede convencer a un servidor de ejecutar un intercambio de llaves anónimo, entonces será capaz de engañar al servidor en todas las sesiones futuras que usen intercambio de llaves. Algún cliente que acepte intercambio de llaves, es vulnerable a tal engaño. Para detener este ataque la firma del servidor en el parámetro de intercambio de llave anónima debería indicar que el servidor está dispuesto a aceptar intercambio de llaves anónimo y ser vulnerable a ataques de hombre y medio, y esta firma sería el límite de la sesión actual. Este requiere unir la firma a los nonces aleatorios de conexiones específicas.

```
        Digitally-signed struct {
              select (SignatureAlgorithm){
                    case anonymous: struct {};
                    case rsa:
                          opaque md5_hash[16];
                          ...
              }
        } Signature;
md5_hash=MD5(ClientHello.Random+ServerHello.Random+ ServerParams);
```

En el caso de intercambio anónimo, la firma está sobre una estructura vacía, la firma no incluye el ClientHello.Random o ServerHello.Random y por lo tanto no limita la sesión actual. Por lo tanto, una vez que una atacante haya recolectado una estructura de Signature anónima desde un servidor, podrá engañar al servidor en futuras sesiones y repetir la vieja estructura Signature sin detección.

En ataque rollback al algoritmo de intercambio de llaves y en el ataque de repetición, SSL es sólo tan seguro como el más débil de los algoritmos de intercambio de llaves o suites de cifrado.

e) Ataques Rollback Version: Las implementaciones de SSL 3.0 probablemente sean lo bastante flexibles para aceptar conexiones SSL 2.0. Este engaño es creado por este ataque, donde un intruso modifica el client hello para que se parezca al mensaje hello de SSL 2.0 y proceda a explotar las vulnerabilidades de SSL 2.0.

Paul Kocher diseña una estrategia para detectar estos ataques en SSL 3.0. Las implementaciones del cliente soportan el SSL 3.0 montado en algún arreglo en los bytes de relleno RSA PKCS para indicar que soportan SSL 3.0. Los servidores que soportan SSL 3.0 refutaran la aceptación del intercambio de llaves cifrado con RSA sobre conexiones compatibles con SSL 2.0 si la encripción RSA incluye esos distintivos bytes de relleno no aleatorios. Este se asegura que el cliente y el servidor que soportan SSL 3.0 son capaces de detectar estos ataques, los cuales tratan de coaccionarlo usando SSL 2.0. Algunos clientes viejos SSL 2.0 usarán rellenos PKCS aleatorios, así que ellos trabajaran con servidores que soporten SSL 2.0.

El objetivo es detectar cuando ambos soporten SSL 3.0 para descubrir los ataques activos

```
[Client hello:]
C → M        v3.0 SSL_RSA...
M → S        v2.0 SSL_DHE...
[Server hello:]
S → C        v2.0 SSL_DHE...
[Server key exchange:]
S → C        {p,g,y}, diffie-hellman
[Client key exchange:]
C → S        {p,g,x}, diffie-hellman
```

Aquí ambos soportan SSL 3.0 y 2.0 para ser forzados a revertir el protocolo SSL 2.0. Sea evitado el intercambio de llaves RSA del SSL 3.0, ahora el atacante activo podrá explotar alguno de sus ataques en SSL 2.0, tal como el ataque rollback de suites de cifrado, tomando ventaja de la débil autenticación del mensaje en SSL 2.0.

Una vulnerabilidad resulta de mezclar versiones a través de sesiones resumidas. La especificación no prohíbe o desalienta SSL 2.0 para ser compatibles con los servidores SSL desde aceptar una petición de client hello SSL 2.0 para resumir una sesión la cual originalmente fue iniciada en SSL 3.0. Si la sesión original de SSL 3.0 incluyera la autenticación del cliente, esto permitiría a un atacante engañar al cliente, como en el ataque rollback que recupera los bits de la llave a través de fuerza bruta, y toma ventaja de las debilidades de SSL 2.0, las llaves MAC son de 40 bits de longitud en modos debilitados de exportación de datos falsificados y engañar el cliente víctima al servidor

```
[Client hello:]
C → S        v4.0, crear una nueva sesión
[Server hello:]
```

```
C → S          v3.0, creada
[Client hello:]
M → S          v2.0, resumir una previa sesión
[Server hello:]
S → M          v2.0, resumida
```

Si reemplazamos la parte donde M actúa por una ataque rollback de suite de cifrado en SSL 2.0 tenemos:

```
[Client hello:]
M → S v2.0, resumir una previa sesión, SSL_RC4_128_EXPORT40_WITH_MD5
[Server hello:]
S → M v2.0, resumida, SSL_RC4_128_EXPORT40_WITH_MD5
[M recupera un MAC de 40bits y k llaves RC4]
M → S          {m},
S → M          {m'},
```

Aquí m representa una sesión falsa de datos escogidos por M; utilizando SSL 2.0 que usa llaves MAC de 40 bits en modos debilitados de exportación, así que una simple búsqueda exhaustiva de 40 bits recupera todas las llaves del protocolo de registro y permite a M falsificar la autenticación y la encripción. El servidor acepta la falsificada $\{m\}_K$ como un mensaje válido. El servidor quizá también envíe de regreso una respuesta confidencial $\{m'\}_K$, y M podrá decriptarla y recuperar el texto plano m'. Por lo tanto todas las protecciones criptográficas han sido comprometidas en este escenario.

f) Salvaguardando El Mastersecret. El masterSecret es importante para SSL, ya que todas las llaves son generadas desde él, y la protección contra intrusos en el protocolo handshake SSL confía grandemente en el secreto del MasterSecret. El MasterSecret es usado en:

Mensaje	Uso
Certificate verify	Hash = adhoc-MAC (MasterSecret, HandShake Messages)
Finished	Hash = adhoc-MAC (MasterSecret, HandShake Messages+Sender)
Change cipher spec (CCS)	KeyBlock = ExpandKeys (MasterSecret, ServerHello.Random+ ClientHello.Random,...]

Un enemigo puede recolectar ilimitada cantidad de texto plano conocido de la transformación MAC de MasterSecret codificada encontrada en el mensaje finished. El atacante abre muchas conexiones simultaneas vía los mensajes client hello requeridos en la reanudación de la sesión objetivo. Para cada conexión el servidor recoge un nonce aleatorio, calcula un MAC con el MasterSecret, y lo envía de regreso cifrado en un mensaje finished. El adversario inteligente debería abandonar esas conexiones abiertas sin responder al mensaje finished del servidor: enviando datos incorrectos de alguna conexión causara una alerta fatal la cual hara la sesión irresumible. En este camnio, el oponente puede coleccionar una gran cantidad de texto plano escogido aplicándole hash con la MasterSecret. Si algún criptoanalista descubre un ataque en adhoc_MAC() usará mucho texto plano conocido para recuperar la llave secreta, el actual protocolo SSL podría no ser guardado. Un protocolo handshake robusto probablemente limitará la cantidad de texto plano conocido que esta disponible para los criptoanalistas

La protección del PreMasterSecret es menos importante. Un atacante quizá adquiera más texto escogido aplicándole hash con la PreMasterSecret repitiendo el texto de cifrado original cifrado con RSA el cual contiene el PreMasterSecret. El atacante no será capaz de completar el protocolo HandShake con esta repetición del texto cifrado RSA, pero quizá sea posible conseguir el servidor para enviar el mensaje finished conteniendo algún texto claro conocido al que se le aplica hash con el PreMasterSecret. Esto sólo será posible si el servidor es suficiente tubería para enviar un mensaje finished después de recibir el mensaje de intercambio de llaves del cliente pero antes recibiendo un mensaje finished del cliente.

c) El Protocolo Alerta

SSL incluye una pequeña provisión para enviar un mensaje de alerta Mucho de éstos indican condiciones fatales de errores y da instrucciones al recipiente inmediatamente al terminar la sesión. Previenen los ataques de truncación.

En general SSL 3.0 provee excelente seguridad contra las intromisiones y otros ataques pasivos. Aunque los modos de debilidad exportados ofrecen mínima protección de confidencialidad. SSL no puede hacer nada contra ese hecho. Un cambio referente a la protección contra ataques pasivos es obtener las longitudes de las peticiones en el Análisis de tráfico.

Se tienen diversos ataques activos, pero quizá todas las implementaciones no sean vulnerables. El ataque más importante es el Disminuir CCS, falsificando el Algoritmo de Intercambio de llaves y el Rollback versión. Estas fallas pueden ser arregladas para prevenir estos ataques. Hay muchos caminos para mejorar la robustez del protocolo.

SSL 2.0 sufrió pocos ataques activos en el protocolo de registro y en el de intercambio de llaves. SSL 3.0 tapa esos agujeros de SSL 2.0 y por lo tanto es considerablemente más seguro contra ataques activos SSL 3.0 provee mucha mejor protección de integridad en modos debilitados de exportación. SSL 3.0 mejora aspectos de no seguridad de SSL, como un soporte flexible de una extensa variedad de algoritmos criptográficos.

Se tiende a

- Negociación de llaves
- Mejora de la Administración de Certificados
- Certificados Cadena
- Llaves de RSA más grandes para certificados de servidor
- PKCS #7, PEM formatos de certificados
- Más aplicaciones con implementación de SSL
- Solicitud de entrada desde cuerpos estándar y otros grupos de interés
- Trabajar con otros estándares para establecer estándares de seguridad en común en diferentes aplicaciones y protocolos

4.1.2 S-HTTP Secure HyperText Transfer Protocol

WWW es un sistema distribuido hypermedia. El protocolo nativo y primario que es usado por la mayoría de los browsers entre los clientes WWW y servidores es HTTP (HyperText Transfer Protocol / Protocolo de Transferencia de Hipertexto). El fácil uso del Web ha despertado un gran interés en el uso de arquitecturas cliente / servidor para muchas aplicaciones, que requieren que exista una autenticación entre ambas partes y en el intercambio sensitivo de información confidencial. HTTP sólo soporta modestos mecanismos criptográficos apropiados para sus transacciones.

Secure HTTP (S-HTTP) provee mecanismos de comunicación segura entre un cliente y servidor HTTP para transacciones comerciales. Es un protocolo flexible que soporta múltiples modos de operación, mecanismos de administración de llaves, modelos de confianza, algoritmos criptográficos, y formatos de encapsulación a través de opciones de negociación entre las partes para cada transacción

Características

- Protocolo de comunicaciones seguras diseñadas en conjunto con HTTP. Este diseño coexiste con el modelo de mensajes HTTP y es fácilmente integrado en aplicaciones HTTP.
- Provee una variedad de mecanismos de seguridad con los clientes y servidores HTTP, proveen las opciones de servicio de seguridad apropiadas con el gran rango del potencial de usuarios finales para WWW
- Provee capacidades simétricas para el cliente y el servidor (a ambos se les da el mismo trato en solicitud y respuesta, al igual como las preferencias de ambas partes) mientras preserve el modelo de transacción y las características de implementación de HTTP.

S-HTTP soporta sólo modos de operación de llave simétrica. Las transacciones privadas pueden ocurrir sin requerir que un usuario haya establecido su llave pública.

S-HTTP provee completa flexibilidad de algoritmos criptográficos, modos y parámetros. La opción de negociación es usada para permitir a los clientes y servidores estar de acuerdo con los modos de transacción, algoritmos criptográficos (RSA vs. DSA para firmar, DES vs. RC2 para encriptar, etc.); y el certificado de selección

Preparación de Mensajes

La creación de un mensaje S-HTTP puede ser pensada como una función con tres entradas:

1. Mensajes en texto claro. Mensaje HTTP o algún otro objeto de datos.
2. Preferencias criptográficas del receptor y el material de codificación
3. Preferencias criptográficas del emisor y el material de codificación. La entrada a la función puede ser pensada como implícita desde que existe sólo en la memoria del emisor.

Para crear un mensaje S-HTTP, el emisor integra sus preferencias con las preferencias del receptor. El resultado de esto es una lista de mejoras criptográficas para ser aplicadas y el material clave para ser aplicado Usando estos datos, el emisor aplica las mejoras al texto en claro del mensaje para crear el mensaje S-HTTP

Los pasos de procesamiento requieren transformar el texto en claro dentro del mensaje S-HTTP. estos requieren anexar las preferencias del emisor y receptor

Recuperación del mensaje

La recuperación de un mensaje S-HTTP puede pensarse de como una función de cuatro entradas distintas

1. Mensaje S-HTTP.
2. Preferencias criptográficas declaradas anteriormente por el receptor y el material de codificación.
3. Preferencias criptográficas actuales del receptor y el material de codificación.
4. Opciones criptográficas previamente declaradas por el emisor.

Para recuperar un mensaje S-HTTP, el receptor necesita leer los encabezados para descubrir que transformaciones criptográficas fueron aplicadas al mensaje, entonces quita las transformaciones que usan algunas combinaciones de material de codificación de emisores y receptores, mientras se verifica que mejoras se aplicaron.

El receptor también puede verificar que las mejoras aplicadas sean iguales a las mejoras que el emisor declaró y que el receptor solicito, al igual que las preferencias actuales para ver si el mensaje S-HTTP fue transformado apropiadamente. Este proceso puede requerir interacción con el usuario para verificar que las mejoras son aceptadas por el usuario.

Modos de Operación

La protección del mensaje puede proporcionarse en tres ejes: firmas, autenticación, y encripción, se puede dar cualquier combinación de éstos (incluyendo la no protección).

Soportan múltiples mecanismos de administración de llaves, incluyen passwords (secretos compartidos manualmente), intercambio de llave pública y la distribución del ticket de Kerberos. En particular, la provisión ha constituido de antemano las llaves simétricas de sesión para enviar los mensajes confidenciales que no tienen algún par de llaves públicas.

Adicionalmente, un mecanismo challenge-response ("nonce") se provee para permitir que las partes se aseguren de lo reciente de la transacción.

a) La Firma: Si se aplica la mejora de la firma digital, un certificado apropiado quizá puede ser unido al mensaje (posiblemente con una cadena certificada) o el emisor puede esperar que el destinatario obtenga el certificado requerido (cadena) independientemente.

b) Intercambio de Llaves y Encripción: Define dos mecanismos de transferencia de llaves, uno usando llave pública para cubrir el intercambio de llaves y otro con arreglo de llaves externas.

En el caso anterior, el parámetro del criptosistema de llave simétrica se pasa encriptado bajo la llave pública del receptor.

En el último modo, se encripta el contenido usando la llave de sesión previamente acordada, con la información de identificación de la llave especificada en una de las líneas del encabezado. También pueden extraerse la llave de los tickets de Kerberos

C) Integridad del Mensaje y Autenticación del Emisor: Proporciona medios para verificar la integridad del mensaje y la autenticidad del receptor de un mensaje computando un Código de Autenticación de Mensajes (MAC- Message Authentication Code), el cómputo es como una codificación hash del documento que usa un secreto compartido (llave previamente acordada o Kerberos). Esta técnica no requiere el uso de criptografía de llave pública ni de encripción.

Este mecanismo también es útil para los casos donde es apropiado permitir a las partes identificarse confiablemente en una transacción sin proporcionar (tercera parte) no-repudiación para sus transacciones. La provisión de este mecanismo se motiva por la acción de "firmar" una transacción que debe ser explícita y consciente para el usuario, considerando que muchos que necesitan autenticación (control de accesos) pueden reunirse con un mecanismo que retiene las ventajas de escalabilidad, y de criptografía de llave pública para el intercambio de la llave.

Formato del Mensaje

La sintaxis de S-HTTP es casi idéntica a la sintaxis de HTTP, para facilitar la integración con sistemas que procesan HTTP. Además, se promueven ciertos encabezados HTTP para ser encabezados S-HTTP porque ellos proporcionan funcionalidad útil que tiene implicaciones de seguridad.

Un mensaje S-HTTP consiste en una solicitud o estado en línea (como en HTTP) seguido por una serie de estilos de encabezados RFC-822 y por el contenido encapsulado. Una vez que el contenido se ha recuperado, éste debería ser otro mensaje S-HTTP, un mensaje HTTP, o simples datos. Para los propósitos de compatibilidad con implementaciones HTTP existentes, distinguimos las solicitudes y las respuestas de la transacción de S-HTTP como un protocolo distinto(' Secure-HTTP/1.2 ').

Solicitud en Línea

El formato de las solicitudes en línea S-HTTP es similar al de HTTP. Sin embargo, todas las solicitudes S-HTTP usan el método, ' Secure'. Todas las solicitudes S-HTTP (usando esta versión del protocolo) debe leer:

```
Secure * Secure-HTTP/1.2
```

Todas las variaciones del caso deben ser aceptadas. El asterisco mostrado es un placeholder y debe ser ignorado por servidores, clientes proxy-aware deben substituir la URL (y debe proporcionar por lo menos el puerto del host) de la solicitud cuando la comunicación es vía proxy, como es la convención actual de HTTP; los proxys deberían remover la cantidad apropiada de esta información para minimizar la amenaza de análisis de tráfico.

El Estado de Línea

Para las respuestas del servidor, la primera línea debería ser:

```
Secure-HTTP/1.2 200 OK
```

si la solicitud tuvo éxito o falló. Esto provee análisis de éxito o fracaso para cualquier solicitud, para la cual el destinatario correcto puede determinarse desde los datos encapsulados. Todas las variaciones del caso deben ser aceptadas.

Líneas de Encabezado S-HTTP

Las líneas descritas en esta sección van en el encabezado de un mensaje S-HTTP. Todos excepto 'Content-Type' y 'Content-Privacy-Domain' son opcionales. El cuerpo del mensaje se separará del bloque del encabezado por dos sucesivos CRLFs.

Content-Privacy-Domain: ' MOSS' se refiere al formato de mejora de la privacidad definido en [RFC-1847] y [RFC - 1848] y ' PKCS-7 '.

Content-Transfer-Encoding: El formato del mensaje PKCS-7 se diseño para un canal claro de 8 bits, pero puede pasarse sobre otros canales que usan codificación base-64.

Para ' Content-Transfer-Encoding: PKCS-7 ', los valores aceptados para este campo son ' BASE64 ', ' 8BIT ', o ' BINARIOS'. A menos que semejante línea sea incluida, se asume que el resto del mensaje es ' BINARIO'.

Para 'Content-Privacy-Domain: MOSS' todo el contenido codificado transfiendo es permitido.

Content-Type para PKCS7: Bajo condiciones normales, la terminal encapsula el contenido (después de todas las de privacidad que han sido removidas) que sería un mensaje HTTP. En este caso, habrá una lectura de Content-Type en línea:

```
Content-Type:  aplicación/HTTP
```

Si el mensaje interno es un mensaje S-HTTP, entonces el Content-Type sería 'aplicación/S-HTTP'.

El contenido de la terminal puede ser de algún otro tipo con tal de que el tipo sea indicado propiamente por el uso de una apropiada línea de encabezado Content-Type. En este caso, los campos del encabezado para la encapsulación del contenido de la terminal aplica el contenido de la terminal ('encabezado final'). Pero en ningún caso, los encabezados finales deberían ser encapsulados siempre con S-HTTP.

La encapsulación S-HTTP de los datos que no son de http, es un mecanismo útil para pasar datos reforzados (sobre todo datos prefirmados) sin requerir que los encabezados de HTTP sean pre-mejorados.

Content-Type para MOSS: Será un tipo de contenido MIME aceptable que describe el proceso criptográfico aplicado. El tipo de contenido se describe en la línea del tipo contenido que corresponde al contenido interno, y para los mensajes HTTP que serán ' aplicación/HTTP '.

Prearranged-Key-Info: Esta línea del encabezado lleva información sobre una llave que se ha colocado fuera del formato criptográfico interno. El uso de esto es permitir comunicación en banda de llaves de sesión para regresar encripción en el caso donde una de las partes no tiene un par de llaves. Sin embargo, esto también debería ser útil en el evento en que las partes escogen usar algún otro mecanismo, por ejemplo, una lista de llaves de una sola vez.

Esta especificación define tres métodos para intercambiar llaves nombradas, Inband, Kerberos y Outband. Inband y Kerberos indican que la llave de sesión fue intercambiada previamente y usa un encabezado de asignación de llaves del método correspondiente. Los arreglos Outband implican que agentes que tienen acceso externo para las llaves de codificación que corresponden a un nombre dado, probablemente vía acceso de la base de datos o quizás proporcionada inmediatamente por un usuario desde el teclado. La sintaxis para la línea del encabezado es:

```
Prearranged-Key-Info: <Hdr-Cipher>','<CoveredDEK>','<CoverKey-ID>
<CoverKey-ID> := <method>':'<key-name>
<CoveredDEK> := <hex-digits>
<method> := 'inband' | 'krb-'<kv> | 'outband'
<kv> := '4' | '5'
```

Mientras la cadena de cifrados requiere un Vector de Inicialización (IV) para empezar fuera de la cadena, esa información no se lleva en este campo. Más bien, debe pasarse al interior del formato criptográfico que se está usando. Igualmente, el cifrado de bloque usado. Debería ser el nombre del cifrado en bloque usado para encriptar la llave de la sesión, que es la llave protegida de encripción de datos bajo la cual el mensaje encapsulado fue encriptado. Debería ser apropiadamente (aleatorio) generado por el agente emisor, entonces es encriptado con la llave negociada (llave de sesión) usando el cifrado del encabezado indicado, y después convertido en hex. Para evitar colisiones de nombre, tapa los namespaces de las llaves que deben ser separados por el host y el puerto.

Hay que notar que algunos Content-Privacy-Domains, podrán soportar la administración de llaves simétricas. El campo Prearranged-Key-Info necesita no ser usado en tales circunstancias, se prefiere la sintaxis nativa. El intercambio de llaves con Key-Assign, quizá sea usado en esta situación.

MAC-Info: Este encabezado se usa para proporcionar Verificación de la Autenticidad del Mensaje, y proporciona autenticación e integridad del mensaje, computado desde el texto del mensaje, el tiempo (opcional/puede prevenir ataques de repetición), y un secreto compartido entre el cliente y el servidor. El MAC debe computarse en el contenido encapsulado del mensaje S-HTTP S-HTTP/1.1 definió que los MAC's deben ser computados usando el siguiente algoritmo ('||' concatenación).

```
MAC = hex(H(Message||[<time>]||<shared key>))
```

El tiempo debe representarse como una cantidad de 32 bits sin firmar, representando segundos desde las 00:00:00 GMT del 1 de enero de 1970, en orden de byte de red. El formato de llave compartida es un problema local.

Se utiliza una construcción HMAC como la siguiente:

```
HMAC = hex(H(K' ^ pad2 || H(K' ^ pad1 ||[<time>]|| Message)))
pad1   the byte 0x36 repeated enough times to fill out a hash input block. (I.e. 64
times for both MD5 and SHA-1)
pad2 = the byte 0x5c repeated enough times to fill out a hash input block.
K' = H(<shared key>)
```

La construcción HMAC es para el uso de una llave con longitud igual que la longitud de la salida del hash. Aunque es considerada segura para usar una llave de longitud diferente (La fortaleza no puede ser aumentada más allá de la longitud de la función hash, pero puede ser reducida usando una llave más corta.) En la construcción que utiliza S-HTTP se aplica hash a la llave original para permitir el uso de llaves compartidas más largas que la longitud del hash. Esta técnica no incrementa la fortaleza de las llaves cortas.

El formato de la línea de MAC-Info es:

```
MAC-Info: [hex <time>],<hash-alg>, hex-<hash data>,<key-spec>
<time> :- "unsigned seconds since Unix epoch"
<hash-alg> :- "hash algorithms from section 3.2.4.8"
<hash-data> :- "computation as described above"
<Key-Spec> :- 'null' | 'dek' | <Key-ID>
```

Key-Ids pueden referirse al límite de la línea de encabezado Key-Assign o a aquéllos límites en el mismo modo como el método Outband. El uso de un 'Null' key-spec implica que una llave de longitud cero fue usada, y por consiguiente que el MAC representa un hash del texto del mensaje y (opcionalmente) el tiempo. El especial key-spec 'DEK' se refiere a la Llave de Intercambio de Datos usada para encriptar el cuerpo del mensaje siguiente (éste es un error para usar DEK key-spec en situaciones donde el cuerpo del mensaje siguiente está sin encriptar).

Si el tiempo se omite de la línea de MAC-Info, simplemente no debe ser incluido en el hash.

Esta línea puede usarse para proporcionar el modo de autenticación básico de HTTP en el cual el usuario puede pedir se le proporcione un nombre de usuario y una contraseña. Sin embargo, la contraseña permanece privada y la integridad del mensaje puede asegurarse. Esto puede lograrse sin encripción de cualquier tipo.

Además, MAC-Info permite la rápida comprobación de la integridad (en la pérdida de no-repudio) para los mensajes, con tal de que los participantes compartan una llave (posiblemente pasó usando Key-Assign en un mensaje previo).

Content

El contenido del mensaje es dependiente de los valores en los campos Content-Privacy-Domain y Content-Transfer-Encoding.

Para un mensaje PKCS-7, con Content-Transfer-Encoding de '8BIT's', el contenido debería ser el propio mensaje PKCS-7.

Si el Content-Transfer-Encoding es ' BASE64 ', el contenido debería ser precedido por la siguiente línea:

```
-- -BEGIN PRIVACY ENHANCED MESSAGE-
```

y seguido por la linea:

```
-----END PRIVACY-ENHANCED MESSAGE-----
```

el contenido simplemente representa base-64 del contenido original. Si el contenido interior (protegido) es el mismo mensaje PKCS-7, entonces el Content-Type del contenido de salida debería ser colocado apropiadamente; sino, el ContentType debe representarse como ' Data'.

Si el Content-Privacy-Domain es MOSS, el contenido debe consistir de Multiparte de Seguridad MOSS.

Se espera que una vez las mejoras a la privacidad hayan sido removidas, el resultado del contenido (posiblemente protegido) será una solicitud HTTP normal. Alternadamente, el contenido quizá sea otro mensaje S-HTTP, en el que los casos de carencia de privacidad deberían ser desenvueltos hasta aclarar el contenido que es obtenido o que la carencia de privacidad no pueda ser removida. Con tal de que todas las carencias puedan ser removidas, el contenido final de la carencia debería ser una solicitud válida HTTP (o respuesta) al menos que por otra parte sea especificado por la línea Content-Type.

La encapsulación recursiva de mensajes potencialmente permite que los logros de seguridad sean aplicados (o removidos) para el beneficio de intermediarios quienes son parte de una transacción entre un cliente y el servidor (ej., un proxy que requiere autenticación del cliente).

Opciones del Formato de Encapsulación

a) Content-Privacy-Domain: PKCS-7

Content-Privacy-Domain: PKCS-7 sigue la forma PKCS-7 estándar.

La protección del mensaje puedes proceder en dos ejes: firma y encripción. Cualquier mensaje puede ser firmado, encriptado, ambos, o ninguno. El modo de protección 'auth' de S-HTTP se proporciona independientemente del código de PKCS-7 vía el encabezado MAC-Info, desde que PKCS-7 no apoya un tipo 'KeyDigestedData', aunque soporte el tipo 'DigestedData'.

Signature: Usa el tipo de PKCS-7 ' SignedData' (o ' SignedAndEnvelopedData'). Cuando se usan firmas digitales, un certificado apropiado quizá sea unido al mensaje (posiblemente a lo largo de la cadena del certificado) como se especifica en PKCS-7 o el emisor puede esperar que el destinatario obtenga su certificado (y/o cadena) independientemente.

Encripción:

- Encripción – normal de Llave Pública: Un mensaje encriptado en este modo, firmado o de otra manera, es PKCS-7
- Prearreglo de Llaves: Usa el tipo 'EncriptedData' de PKCS-7. En este modo, se encripta el contenido usando un DEK encriptado bajo un prearreglo de llave de sesión, con información de identificación de la llave especifica en una de las líneas del encabezado. Los IV están en el tipo EncriptedContentInfo del elemento de EncriptedData. Para generar el firmado, datos encriptados, es necesario generar 'SignedData' y entonces encriptarlo.

b) Content-Privacy-Domain: MOSS

El cuerpo del mensaje debe ser un mensaje MIME con tipo de contenido igual que la línea Content-Type en los encabezados S-HTTP. Los mensajes encriptados deben usar encriptado multipartes. Firmar mensajes debe usar un firmado multiparte. Sin embargo, desde que la firma de multipartes no comunica el material de codificación, es aceptable usar una mezcla de multipartes donde la primera parte es una aplicación/mosskey-datos y la segunda parte es un mezclado multiparte para llevar certificados para el uso de la verificación de la firma.

Cuando el mismo agente aplica la encripción y la firma, la firma debe ir antes de la encripción.

c) Encabezados HTTP importados

Algunas facilidades de HTTP, particularmente aquéllas que se involucran con almacenamiento y proxys, requieren consideración especial cuando el procesamiento S-HTTP ha sido aplicado. S-HTTP hace adaptaciones especiales para esas características copiando las líneas de encabezado HTTP relevantes dentro de la sintaxis del encabezado de S-HTTP

Connection: Keep-Alive: Este encabezado se diseña para permitir conexiones persistentes entre los pares cliente/proxy y proxy/servidor. Un cliente o proxy que desea conexiones persistentes debe enviar el encabezado 'Connection: Keep-Alive'. Un servidor que está de acuerdo debe responder con 'Connection: Keep-Alive'.

La conexión persistente acaba cuando cualquiera de las partes cierra la conexión o después de que el destinatario de una respuesta crece la palabra clave "Keep-Alive". El servidor puede cerrar la conexión inmediatamente después de responder a una solicitud sin la palabra clave "Keep-Alive". Un cliente puede decir si la conexión será cerrada buscando un "Keep-Alive" en la respuesta.

Los proxys y los gateway deben quitar el encabezado "Keep-Alive", pensando, que pueden regenerarlo opcionalmente si desean una conexión persistente con la próxima conexión. Los clientes HTTP que no usan gateways y desean una conexión persistente con el servidor no deben usar este mecanismo, sino que deben usar cualquier mecanismo que proporcione HTTP.

If-Modified-Since: Esto puede ser usado por el proxy para indicar que el documento puede estar almacenado y que ha preparado el documento para dárselo al solicitante actual. Los servidores reciben este encabezado y no deciden reenviar el documento, deben responder usando el código de la respuesta 320.

Este encabezado sólo debe ponerse en encabezados S-HTTP para proxys. Los clientes que quieren usar If-Modified-Since deben ponerlo en el encabezado HTTP del contenido interno.

Content-MD5: Los servidores pueden generar un encabezado Content-MD5 para permitirles a los proxys descubrir cuando han ocurrido hits del cache válidos. Nota que el encabezado Content-MD5 proporciona la posibilidad del análisis de tráfico. Los servidores usados deben tener presente ese riesgo.

Los Content-MD5 se computan en el contenido interno en lugar de en el texto cifrado

Parámetros Criptográficos

a) Opciones de Encabezados

Cada solicitud S-HTTP es (por lo menos conceptualmente) preacondicionada por las opciones de negociación proporcionadas por el receptor potencial. Las dos locaciones primarias para estas opciones son:

1. En los encabezados de una Solicitud/Respuesta HTTP
2. En el HTML que contiene la liga que es de referenciada

Hay dos tipos de opciones criptográficas que pueden proporcionarse: Opciones de negociación, transporta un mensaje potencial de las preferencias criptográficas de los mensajes del destinatario. Opciones de codificación, proporciona el material de codificación qué puede ser de uso al emisor al reforzar un mensaje

- **Opciones de Negociación**

Ambas partes pueden expresar sus requisitos y preferencias con respecto a qué mejoras criptográficas permitiran/requeriran a la otra parte para proporcionarlos. La elección de la opción apropiada depende de las

capacidades de aplicación y los requisitos de aplicaciones particulares. Un encabezado de la negociación es una secuencia de especificaciones que conforman un esquema detallado en cuatro partes:

1. Propiedad: la opción será negociada, como contenido del algoritmo de encripción.
2. Valor: el valor será discutido para la propiedad, tal como DES-CBC.
3. Dirección: la dirección que será afectada, a saber: durante la recepción u origen (desde la perspectiva del creador).
4. Fuerza: la fuerza de preferencia, a saber: requerido, opcional, rechazado.

Como un ejemplo, la línea del encabezado:

```
SHTTP-Symmetric-Content-Algorithms: recv-optional=DES-CBC,RC2
```

podría pensarse que dice: "Usted es libre de usar DES-CBC o RC2 para encripción de contenido para la encripción de mensajes."

Se definen nuevos encabezados (para ser usado en el encabezado HTTP encapsulado, no en el encabezado de S-HTTP) para permitir la negociación.

El formato general para las opciones de la negociación es:

```
<Option> := <Field> ':' <Key-val>{';'<Key-val>}*
<Key-val> := <Key> '=' <Value>{','<Value>}*
<Key> := <Mode>'-'<Action>
<Mode> := 'orig'|'recv'
<Action> := 'optional'|'required'|'refused'
```

El valor indica que si se refiere a las acciones del agente que están por encima de mensajes con privacidad mejorada como opuesto a recibirlos. Para cualquier par de mode-action dado, la interpretación será colocada en la lista de mejoras:

- 'recv-optativo:' El agente procesará la mejora si la otra parte lo usa, pero también procesará los mensajes sin el perfeccionamiento.
- 'recv-requirió:' El agente no procesará mensajes sin la mejora.
- 'recv-refused:' El agente no procesará mensajes con la mejora.
- 'orig-optative:' Al encontrar a un agente que se niega a la mejora, el agente no lo proporcionará, y cuando encuentre a un agente que lo requiere, si lo proporcionara.
- 'orig-required:' El agente siempre generará la mejora.
- 'orig-refused:' El agente nunca generará la mejora.

La conducta de agentes que descubren que se están comunicando con un agente incompatible está en la discreción de los agentes. Es impropio para persistir ciegamente en una conducta que se conoce como inaceptable para la otra parte. Las respuestas creíbles simplemente incluyen terminando la conexión, o, en el caso de una respuesta del servidor, regresa 'Not implemented 501'.

Se considera que los valores opcionales son listados en orden decreciente de preferencia. Los agentes son libres de escoger cualquier miembro de la intersección de las listas opcionales (o ninguna).

Si cualquiera queda indefinido, debe asumirse que se tomará un valor por default. Cualquier llave que es especificada por un agente derogará cualquier apariencia de esa llave en algún default para ese campo.

Parametrización para la Llave de los Cifrado de Longitud Variable

Para los cifrados con llaves de longitudes variables, los valores pueden ser parametrizados usando la sintaxis

```
<cipher>'['<length>']'
```

Por ejemplo, ' RSA[1024] ' representa una llave de 1024 bits para RSA. Estos rangos puede representarse como

```
<cipher>'['<bound1>' '<bound2>']'
```

Para los propósitos de preferencias, esta anotación debe tratarse como si lo leyera (asumiendo que x y y son enteros)

```
<cipher>[x], <cipher>[x+1],...<cipher>[y] (if x<y)
```

y

```
<cipher>[x], <cipher>[x-1],...<cipher>[y] (if x>y)
```

El valor especial 'inf' puede usarse para denotar longitud infinita.

Simplemente usado para tal cifrado será leído como un gran rango posible para el cifrado dado.

Sintaxis de la Negociación

SHTTP-Privacy-Domains: Este encabezado se refiere al tipo Content-Privacy-Domain. Los valores aceptables son, por ejemplo:

```
SHTTP-Privacy-Domains: orig-required pkcs-7; recv-optional pkcs-7,MOSS
```

indica que el agente siempre genera mensajes PKCS-7, pero puede leer PKCS-7 o MOSS.

SHTTP-Certificate-Types: Indica que clase de certificados de llave pública aceptará el agente ('X.509' y 'X.509v3')

SHTTP-Key-Exchange-Algorithms: Este encabezado indica que algoritmos pueden usarse para el intercambio de llaves ('RSA', 'Outband', 'Inband', y 'Krb -)'. <kv> RSA se refiere a la envoltura RSA. Outband se refiere a alguna clase de acuerdo de llave externa. Inband y Kerberos se refieren a protocolos.

La configuración común esperada de clientes que no tienen ningún certificado y servidores que tienen certificados se parece a (en un mensaje enviado por el servidor):

```
SHTTP-Key-Exchange-Algorithms:    orig-optional Inband, RSA;
                                  recv-required-RSA
```

SHTTP-Signature-Algorithms: Este encabezado indica que algoritmos de Firmas Digitales pueden usarse ('RSA' [PKCS-1] y 'NIST-DSS' [FIPS-186]) Desde que NIST-DSS y RSA usan módulos de longitud variable. Nota que la longitud de la especificación de la llave puede interactuar con la aceptabilidad de un certificado dado, desde que las llaves (y sus longitudes) especifican certificados de llave pública.

SHTTP-Message-Digest-Algorithms: Indica que algoritmos Message Digest pueden usarse ('RSA-MD2' y 'RSA-MD5')

SHTTP-Symmetric-Content-Algorithms: Este encabezado especifica la llave del cifrado bulk simétrico usada para encriptar el contenido del mensaje. Los valores definidos son:

```
DES-CBC -- DES in Cipher Block Chaining (CBC) mode (FIPS-81)
DES-EDE-CBC -- 2 Key 3DES using Encrypt-Decrypt-Encrypt in outer CBC mode
DES-EDE3-CBC -- 3 Key 3DES using Encrypt-Decrypt-Encrypt in outer CBC mode
RSA-CBC -- RSA's RC2 in CBC mode
IDEA-CBC -- IDEA in CBC mode (XXXX)
RC2-CBC -- RSA's RC2 in CBC mode
MME-CBC -- IBM's MIME workalike key, DES in CBC mode
```

SHTTP-Symmetric-Header-Algorithms: Este encabezado especifica la llave del cifrado simétrico usado para encriptar los encabezados.

```
DES-ECB -- DES in Electronic Codebook (ECB) mode [FIPS-81]
DES-EDE-ECB -  2 Key 3DES using Encrypt-Decrypt-Encrypt in ECB mode
DES-EDE3-ECB    3 Key 3DES using Encrypt-Decrypt-Encrypt in ECB mode
DESX-ECB -- RSA's DESX in ECB mode
IDEA-ECB -- IDEA
RC2-ECB -- RSA's RC2 in ECB mode
CDMF-ECB -- IBM's CDMF in ECB mode
```

SHTTP-MAC-Algorithms: Este encabezado indica que algoritmos son aceptables para proporcionar una llave simétrica MAC ('RSA-MD2', 'RSA-MD5' y 'NIST-SHS' persisten desde S-HTTP/1.1 que usa la vieja construcción MAC). Los tokens 'RSA-MD2-HMAC', 'RSA-MD5-HMAC' y 'NIST-SHS-HMAC' indican la nueva construcción de HMAC con los algoritmos MD2, MD5, y SHA-1 respectivamente.

SHTTP-Privacy-Enhancements: Este encabezado indica mejoras de seguridad a aplicar ('sign', 'encrypt' y 'auth'), que indican si los mensajes se firmaron, encriptaron, o autenticaron, respectivamente.

Your-Key-Pattern: Este es una sintaxis generalizada de un modelo que describe identificadores para un gran número de material de codificación. La sintaxis general es:

```
Your-Key-Pattern : <key-use>','<pattern-info>
<key-use> :: 'cover-key' | 'auth-key'   'signing-key'   'krbIV-'<kv>
```

Este encabezado especifica valores deseados para nombres de llaves usados en la encripción de llaves de la transacción que se usan en la sintaxis del Prearranged-Key-Info. La sintaxis consiste en una serie de expresiones regulares separadas por coma. Las comas deben escaparse con backslashes si ellos aparecen en el regexps.

Los modelos Auth-Keys especifican nombres de formas deseadas para el uso de autenticadores MAC. La sintaxis pattern-info consiste en una serie de expresiones regulares separadas por una coma. Las comas deben escaparse con backslashes si ellos aparecen en el regexps

Este parámetro describe un modelo o modelos para que las llaves sean aceptables para firmar por la mejora de la firma digital. La sintaxis pattern-info para singning-key es:

```
<pattern-info> :: <name-domain>','<pattern data>
```

El único nombre de dominio definido actualmente es ' DN-1485 '. Este parámetro especifica los valores deseados para los campos de Nombres Distinguidos

El Pattern-data es una cadena modificada, con expresiones regulares permitidas como valores de campos. El modelo ha realizado consideración de campos, los campos no especificados se igualan a algún valor (Modelo completamente no especificado permite cualquier DN) Las cadenas del certificado también puede igualarse (para permitir certificados sin la subordinación del nombre) Se considera que las cadenas DN son ordenadas de izquierda-a-derecha con el certificado dado del emisor en su derecho inmediato, aunque los emisores necesitan no ser especificados. Un rastro '. ' indica que la sucesión de DNs es absoluta.

La sintaxis para los valores del modelo es,

```
<Value> :: <DN spec>  ','<Dn-spec> | '.'
<Dn spec> :  '/'<Field-spec>*'/'
<Field-spec> :  <Attr> '='<Pattern>
<Attr> :  'CN' | 'L' | 'OU' | 'O' | 'C' | "or any appropriate"
<Pattern> :  "POSIX 1003.2 regular expression"
```

Por ejemplo, para pedir que el otro agente firme con un certificado por la autoridad certificadora RSA se usa la expresión de abajo.

```
Your-Key-Pattern: DN-1485,
                  /OU=Persona Certificate, O="RSA Data Security, Inc\."/
```

Ejemplo de encabezados para un servidor:

```
SHTTP-Privacy-Domains: recv-optional MOSS, PKCS-7;
      orig-required=PKCS-7
SHTTP-Certificate-Types: recv-optional X.509;
      orig-required=X.509
STTP-Key-Exchange-Algorithms: recv-required=RSA;
      orig-optional=Inband,RSA
SHTTP-Signature-Algorithms: orig-required RSA;
      recv-required=RSA
SHTTP-Privacy-Enhancements: orig-required sign
      orig-optional=encrypt
```

Defaults: Los parámetros de negociaciones explícitas toman precedencia sobre valores default. Los valores default son:

```
SHTTP-Privacy-Domains: orig-optional PKCS-7, MOSS;
      recv-optional=PKCS 7, MOSS
SHTTP-Certificate-Types: orig-optional X.509;
      recv-optional X.509
SHTTP-Key-Exchange Algorithms: orig-optional=RSA,Inband;
      recv-optional RSA,Inband
SHTTP-Signature-Algorithms: orig-optional RSA;
      recv-optional=RSA
SHTTP-Message-Digest Algorithms: orig-optional=RSA-MD5;
      recv-optional=RSA-MD5
SHTTP-Symmetric-Content-Algorithms: orig-optional=DES-CBC;
      recv-optional=DES-CBC
SHTTP-Symmetric-Header-Algorithms: orig-optional=DES-ECB;
      recv-optional=DES-ECB
SHTTP-Privacy-Enhancements: orig-optional sign,encrypt, auth;
      recv-required=encrypt;
      recv-optional sign, auth
```

➢ Encabezados de No Negociación

Hay varias opciones que se usan para comunicar o identificar al destinatario potencial del material de codificación.

Encription-Identity: Este encabezado identifica al principal potencial para quien el mensaje descrito por estas opciones podria ser encriptado; note que éste explícitamente permite el regreso de la encripción bajo la llave pública sin que el otro agente firme primero (o bajo una llave diferente a la de la firma). O, en el caso de Kerberos, proporciona información como la identidad del agente Kerberos. La sintaxis de la línea Encription-Identity es:

```
Encryption-Identity: name-class,key-info, name-arg: name-class:
"DN-1485" ...
```

El nombre de la clase es una cadena ASCII que representa el dominio dentro del cual el nombre será interpretado, en los nuevos proyectos MOSS. Además de los nombres de formas MOSS, se agrega el nombre de la forma DN-1485 para representar una forma más conveniente de nombre distinguido.

Nota: Los nombres de formas Kerberos de proyectos anteriores son empujados por las cadenas e-mail de la forma MOSS.

Certificate-Info: Para permitir operaciones de llave pública en un DNs especificado por los encabezados de Encription-Identity sin el certificado explícito buscado por el receptor, el emisor puede incluir información de la certificación en la opción Certificate-Info. El formato de esta opción es:

```
Certificate-Info: <Cert-Fmt>','<Cert-Group>
```

Los valores definidos son ' PEM' y ' PKCS-7 '. Los grupos de certificados PKCS-7 son proporcionados como un mensaje PKCS-7 SignedData codificado en base-64 conteniendo secuencias de certificados con o sin el campo de SignerInfo. Un grupo de certificados con formato PEM es una lista de certificados PEM separados en codificaciones base64-encoded PEM. Pueden ser definidas muchas líneas Certificate-Info.

Key-Assign: Esta opción sirve para indicar que el agente desea ligar una llave a un nombre simbólico para (probablemente) una referencia posterior. La sintaxis general del encabezado Key-Assign es:

```
Key-Assign: <Method>,<Key-Name>,<Lifetime>,<Ciphers>;<Method-arg:>
<Key-name> := <string>
<Lifetime> := 'this' | 'reply' | ''
<Method> : 'inband' | 'krb '<kv>
<Ciphers> :  'null'   <Cipher>+
<Cipher> :  "Header cipher from section 4.2.4."
<kv> := '4' | '5'
```

El Key-Name es el nombre simbólico de la llave, de una lista de cifrados. La keyword 'null' debería usarse para indicar que es impropio para usar algún cifrado Esto es potencialmente útil para intercambiar llaves por el cómputo de MAC.

El tiempo de vida es una representación del período más largo, durante el cual el destinatario de este mensaje puede esperar a que el emisor acepte esa llave ' this' indica que es probable que sólo sea válida la transacción para lectura. 'reply' indica que es útil para contestar este mensaje. Si un Key-Assign con la respuesta del tiempo de vida aparece en un bloque CRYPTOPTS, indica que es bueno para al menos una referencia (pero quizás sólo uno) de esta liga. El tiempo de vida no especificado implica que esta llave puede reusarse para un número infinito de transacciones.

El método debe ser uno de varios tipos de intercambios de llave. Los valores actualmente definidos son 'inband', ' krb-4 ' y ' krb-5 ', refiriéndose respectivamente a las llaves Inband (es decir, asignación directa) y Kerberos versiones 4 y 5 respectivamente. Method-args dependerá de métodos.

Esta línea quizá aparezca en un encabezado sin encapsular o en un mensaje encapsulado, aunque cuando una llave descubierta está siendo asignada directamente, sólo puede aparecer en un contenido encapsulado encriptado.

Las llaves definidas por este encabezado son referenciadas como Key-IDs, que tienen la sintaxis

```
<Key-ID> :  <method>':'<key-name>
```

también puede usarse como una línea del encabezado en los encabezados S-HTTP si los datos que está llevando no necesita seguridad, ej. con Kerberos

Asignación de la Llave Inband

Esto se refiere a la asignación directa de una llave descubierta para un nombre simbólico. Method-args debe ser justo la llave de sesión deseada codificada en hexadecimal como en:

```
Key-Assign: inband, <key>,reply,DES-EDE3-CBC,0123456789abcdef
```

Deben derivarse llaves cortas de las llaves largas leyendo para lectura de bits de izquierda a derecha

Esta asignación es especialmente importante para permitir la confidencialidad de la comunicación espontánea entre agentes donde uno (pero no ambos) de los agentes tienen su par de llaves Sin embargo, este mecanismo también es útil para permitir cambios de llaves sin cómputos de llave pública. La información de la llave se lleva en esta linea del encabezado debe estar en la solicitud interna S-HTTP, por consiguiente el uso de mensajes sin encriptar no está permitido.

Asignación de Llave Kerberos

Esto permite el ocultamiento del secreto compartido derivado de un par ticket/autenticador Kerberos para un nombre de llave simbólico. En este caso, method-args debería ser el par ticket/autenticador (cada uno en codificación base64), separado por una coma. Por ejemplo:

```
Key-Assign: krb-4,akerbkey,reply,DES-ECB;<krb-ticket>,<krb-auth>
```

Nonces: Son ocultos, pasajeros, identificadores orientados a sesión que pueden ser usados para proporcionar demostraciones de novedad. Los valores de Nonce son un material local, aunque ellos están quizá sean simplemente números del azar generados por el creador. El valor se proporciona para ser simplemente regresado por el destinatario.

Nonce

Este encabezado es usado por un creador para especificar qué valor es regresado en la respuesta. El campo puede ser algún valor. Múltiples Nonce pueden proporcionarse, cada uno será repetido independientemente

El Nonce debe volverse una linea de encabezado de Nonce-Echo.

Agrupando Encabezados Con SHTTP-Cryptopts

Para que los servidores liguen un grupo de encabezados a una liga HTML, es posible combinar varios encabezados en una sola linea S-HTTP Cryptopts. Los nombres de las ligas a las cuales estos encabezados aplican se indica con el parámetro 'scope'.

SHTTP-Cryptopts. Esta opción proporciona un juego de cryptopts y una lista de referencias a las cuales aplican (Para HTML, estas referencias se nombran usando la etiqueta NAME). Los nombres son proporcionados en el alcance del atributo como una coma que separa la lista y separa de la próxima línea del encabezado por un punto y coma. El formato para la linea SHTTP-Cryptopts es:

```
SHTTP-Cryptopts: <scope>';'<cryptopt-list>
<scope> :  'scope '<tag-spec>
<tag-spec> := <tag>{','<tag>}*   <null>
<cryptopt list> :  <cryptopt>{';'<cryptopt>}*
<cryptopt> :  "S-HTTP cryptopt lines described below"
<tag> :  "value used in HTML anchor NAME attribute"
```

Por ejemplo:

```
SHTTP-Cryptopts: scope 'all,tag:;
        SHTTP-Privacy-Domains:
        orig-required pkcs-7; recv-options: pkcs-7,MOSS
```

Si un mensaje contiene encabezados de negociación S-HTTP y encabezados agrupados en línea(s) SHTTP-Cryptopts, los otros encabezados se tomarán para aplicar a todas las ligas no limitadas en la línea(s) de SHTTP-Cryptopts. Nota que esto es una proposición todo-o-nada. Es decir, si un encabezado SHTTP-Cryptopts liga opciones a una referencia, entonces ninguna de estas opciones globales aplican, aún cuando algunos de los encabezados de opciones hacen que no aparezca las opciones limitadas.

Nuevas Líneas de Encabezado para HTTP

Security-Scheme: Todos los agentes obedientes de S-HTTP deben generar el encabezado Security-Scheme en los encabezados de todos los mensajes HTTP que ellos generan. Este encabezado permite a otros agentes detectar que ellos se están comunicando con un agente obediente S-HTTP y genera los encabezados de opciones criptográficas apropiadas. Para las implementaciones obedientes con esta especificación, el valor debe ser ' S-HTTP/1.2 '.

Nonce-Echo: El encabezado se usa para regresar el valor proporcionado en un Nonce previamente recibido: campo. Esto tiene que ir en los encabezados encapsulados para que sea criptográficamente protegido.

Reportes de el Estado de Error de los Servidores

Proceso especial apropiado para los reintentos del cliente ante servidores que regresan un estado de error.

a) Reintento para la Opción de (Re)Negociación

Un servidor puede responder a una solicitud del cliente con un código de error, que indica que la solicitud no ha fallado completamente sino que el cliente puede lograr satisfacción posiblemente a través de otra solicitud. HTTP ya tiene este concepto con los códigos 3XX de redirección

En el caso de S-HTTP, es concebible (y de hecho probablemente) que el servidor espere a que el cliente reintente su solicitud usando otro juego de opciones criptográficas. Ej., el documento que contiene la liga, que el cliente está referenciado es viejo y no requirió firma digital para la solicitud en cuestión, pero el servidor tiene ahora una política de requisición de firma para la referencia del URL. Estas opciones deben llevarse en el encabezado del mensaje HTTP encapsulado, precisamente como las opciones del cliente son llevadas.

La idea general es que el cliente realice el reintento en el manera indicada, para la combinación de la solicitud original y la naturaleza precisa del error y los perfeccionamientos criptográficos dependiendo de las opciones contenidas en la respuesta del servidor.

El principio guiado en la respuesta del cliente a estos errores debe ser proporcionarle al usuario el mismo orden de opción informada con respecto a la referencia de estas ligas referenciadas como liga normal. Para el caso, debería ser impropio para que el cliente firme la solicitud sin pedir permiso para la acción

b) Conducta del Reintento Específico

Desautorizado 401, PagoRequerido402: Los errores HTTP 'Desautorizado 401', 'PagoRequeido 402' representan fallas del estilo de autenticación HTTP y esquemas de pago. Mientras S-HTTP no tiene apoyo explícito para esos mecanismos, ellos pueden ser ejecutados bajo S-HTTP mientras se aprovechan de los servicios de privacidad ofrecidos por S-HTTP.

420 ReintentoSeguridad La respuesta del estado del servidor se proporciona para que el servidor pueda informar al cliente que aunque la solicitud actual sea rechazada, un reintentó de la solicitud con mejoras criptográficas diferentes vale la pena intentarlo. Este encabezado también se usará en el caso donde una solicitud HTTP se ha hecho, pero una solicitud S-HTTP debería haber sido hecha. Obviamente, esto no sirve a ningún otro propósito útil que señalar un error si la solicitud original debería haber sido encriptada, pero en otras situaciones (control de acceso) puede ser usual.

- S-HTTP : En el caso de una solicitud que se hizo como una solicitud SHTTP, indica que por alguna razón las mejoras criptográficas aplicadas a la solicitud fueron poco satisfactorias, y que debe ser repetida con las opciones encontradas en el encabezado de la respuesta. Nota que esto puede usarse como una manera de forzar una nueva negociación de llave pública, si la llave de sesión en uso ha expirado o para proporcionar un único nonce para los propósitos de asegurar lo nuevo de la solicitud

- HTTP: Si el código 420 ha devuelto en respuesta una solicitud HTTP, ésta indica que la solicitud debería ser reintentada usando S-HTTP y las opciones criptográficas indicadas en el encabezado de la respuesta.

421 EncabezadoBogus: Este código de error indica que algo sobre la solicitud S-HTTP era malo. El código de error será seguido por una explicación apropiada, ej.:

```
421 BogusHeader Content-Privacy-Domain debe ser especificado
```

422 SHTTP Autenticación Proxy Requerida: Esta respuesta es análoga a la respuesta 420 sólo que las opciones en el mensaje se refieren a perfeccionamientos que el cliente debe ejecutar para satisfacer al proxy.

320 SHTTP No Modificado: Este código es específicamente para el uso con la interacción de un servidor proxy, donde el proxy ha puesto el encabezado If-Modified-Since en el encabezado S-HTTP de su solicitud. Esta respuesta indica que el siguiente mensaje S-HTTP contiene material de codificación suficiente para el proxy para remitir el documento almacenado para el nuevo solicitador.

En general, esto toma la forma de un mensaje S-HTTP donde el contenido real reforzado está perdido, pero todos los encabezados y el material de codificación es retenido. (Es decir el contenido opcional del mensaje PKCS7 ha sido removida.) Así que, si la respuesta original fue encriptada, la respuesta contiene el DEK original recubierto para el nuevo destinatario.

Redirección 3XX. Estos encabezados son de HTTP, pero pueden contener opciones de negociación S-HTTP de importancia para S-HTTP. La solicitud debería ser remitida en sentido de HTTP, con precauciones criptográficas apropiadas que se observan.

c) Limitaciones En Reintentos Automáticos

Permitiendo reintentos automáticos del cliente en respuesta al orden de las respuestas del servidor permite varias formas de ataque. Considere para el caso de tarjeta de crédito:

El usuario ve un documento que requiere su tarjeta de crédito. El usuario verifica que el DN del destinatario proporcionado sea aceptable y que la solicitud sea encriptada y dé referencia a la liga. El atacante intercepta la respuesta del servidor y responde con un mensaje encriptado con la llave pública del cliente que contiene el encabezado Moved 301. Si el cliente estaba ejecutando automáticamente éste redirecciónandolo comprometiendo la tarjeta de crédito del usuario.

- Recuperación de Encripción Automática

Muestra un posible peligro de reintentos automáticos - compromiso potencial de información encriptada. Mientras es imposible considerar todos los posibles casos, los clientes nunca deben reencriptar automáticamente los datos al menos de que el servidor que pide el reintento demuestre que él ya tiene los datos. Así que, las situaciones en las que sería aceptable la reincripción son si:

1. La respuesta del reintento fue reencriptada bajo una llave inband generada recientemente para la solicitud original.
2. La respuesta del reintento fue firmada por el destinatario propuesto en la solicitud original.
3. La solicitud original usó una llave outband y la respuesta es encriptada bajo esa llave.

Nota que un comportamiento apropiado en casos donde la reencripción automático no es apropiada se debe pedir permiso al usuario.

- Recuperación Automática de la Firma

Desde que se descorazona el firmado automático (sin la confirmación del usuario) incluso en casos usuales, y dado los peligros descritos, está prohibido para recuperar la firma automáticamente.

- Recuperación de la Autenticación MAC Automática

Asumiendo que todas las condiciones se siguieron, es permisible para recuperar automáticamente la Autenticación MAC.

Otros Problemas

Compatibilidad de Servidores con Clientes Viejos: Los servidores que reciben solicitudes en claro los cuales deberían asegurarse regresar 'SecurityRetry 420' con líneas del encabezado colocadas para indicar que se requieren mejoras a la privacidad

Tipo de Protocolo URL: Se designa un nuevo protocolo URL, 'S-HTTP'. El uso de este designador como parte de una liga URL implica que el servidor designado S-HTTP sea capaz, y que una dereferencia de esta URL deba sufrir procesamiento S-HTTP.

Note que los agentes inconsistentes de S-HTTP no deben estar dispuestos para la dereferencia en un URL con un especificador del protocolo desconocido, y por lo tanto estos datos sensitivos no serán accidentalmente enviados en claro por usuarios de clientes no seguros.

Convenciones del Servidor:

- Solicitud de Certificado: Se define la convención que emite una solicitud normal HTTP:

```
GET /SERVER-CERTIFICATE-<B64-DN> <http version>
```

Que causaría que el servidor regrese el certificado correspondiente. <B64-DN> es la codificación base-64 (para proteger los espacios en blanco) de la forma ASCII canónica completamente-especificada para el DN del certificado solicitado. Sino se especifica ningún DN, entonces el servidor escogerá cualquier certificado que juzgue que es el más apropiado. El servidor debe firmar la respuesta con la llave que corresponde al DN proporcionado.

- Solicitud de Políticas y Solicitudes CRL: Los servidores deben (pero no deben) almacenar las políticas de las Autoridades de Políticas de Certificación, los CRLs del PCA correspondiente para sus certificados. La convención para recuperar tales políticas y los CRLs vía HTTP son las solicitudes:

```
GET /POLICY-<B64-DN> <http-version>
GET /CRL-<B64 DN> <http version>
```

Nuevamente, <B64-DN> es el DN del certificado que corresponde a la política y al CRL solicitado. Se recomienda que este documento sea (pre) firmado por el PCA.

Presentación del Browser:

- Estado de Seguridad de la Transacción: Mientras se prepara un mensaje seguro, el browser debe proporcionar una indicación visual de la seguridad de la transacción, así como una indicación de la parte que podrá leer el mensaje. Mientras lee un mensaje firmado y/o envuelto, el browser debe indicar esto y (si aplica) la identidad del firmante. Los certificados firmados deben diferenciarse claramente de aquellos validados por una jerarquía de certificación.

- Reportando la Falla: Fracaso para autenticar o decriptar un mensaje de S-HTTP que debe ser presentado diferentemente de un fracaso para recuperar el documento. Los clientes inconformes quizá en su opción desplieguen documentos sin verificación pero debe indicar claramente que ellos fueron en cierto modo inverificables de distinta manera en la que ellos despliegan los documentos que no poseen ninguna firma digital o documentos con firmas verificables.

- Manejo del Certificado: Los clientes mantendrán un método para determinar las solicitudes HTTP que están para ser firmadas y para determinar que certificado será usado para la firma. Se sugiere que los

usuarios se presenten con alguna orden en la lista de selección del cual ellos pueden escoger un valor por default. Ninguna firma debe realizarse sin alguna clase de explícita de una interfaz de usuario, aunque tal acción puede tomar la forma de un escena persistente vía un mecanismo de preferencias de usuario.

- Anchor Dereference: Los clientes proporcionarán un método para desplegar el DN y la cadena de certificado asociada con un anchor dado para ser referenciado para que los usuarios puedan determinar si sus datos están siendo encriptados. Este debe ser distinto del método para desplegar quién ha firmado el documento conteniendo el anchor desde las piezas de encripción de información.

Datos de Preafinados

Motivación: Las dos motivaciones primarias para los documentos preafinados son seguridad y desempeño. Estas ventajas incrementan el número de firmas pero pueden también bajo circunstancias especiales aplicar confidencialidad o autenticación repudiable (basado en MAC).

Considere el caso de un servidor que repetidamente envía el mismo contenido a múltiples clientes. Un ejemplo sería un servidor el cual tenga catálogos o listas de precios. A los clientes les gustaría, ser capaces de verificar los precios actuales. Sin embargo, desde que los precios son los mismos para todas las personas que llegan, la confidencialidad no es un problema.

Por consiguiente, el servidor podría desear firmar el documento una vez y simplemente mandar el documento firmado que está almacenado cuando un cliente hace una nueva solicitud, evitando el uso de una operación de llave privada cada vez. Note eso concebible, el documento firmado se podría haber generado por una tercera parte y colocado en el almacén del servidor. El servidor quizá no tenga la llave de firma. Esto ilustra el beneficio de seguridad de prefirmar: Los servidores no confiables pueden sacar datos autenticados sin riesgo aún cuando el servidor este comprometido.

Respuestas/Solicitudes Prefirmadas: La más simple implementación es tomar una sola solicitud/respuesta, almacenarla, y enviarla en situaciones donde un mensaje nuevo se generarara por otra parte.

Documentos Prefirmados: También es posible usar S-HTTP para firmar los datos subyacentes y enviarlos como un mensaje S-HTTP. Para hacer esto, uno tomaría el documento firmado (un mensaje PKCS-7 o MOSS) y une los encabezados S-HTTP (ej. Línea de solicitud/respuesta S-HTTP, el Content-Privacy- Domain) y los encabezados HTTP necesarios (incluso un Content-type refleja el contenido interno).

```
SECURE * Secure HTTP/1.2
   Content Type: text/html
   Content-Privacy-Domain: PKCS-7
   Content-Transfer-Encoding: base64

   -----BEGIN PRIVACY-ENHANCED MESSAGE-----
   Random signed message here...
   -----END PRIVACY-ENHANCED MESSAGE-----
```

Este mensaje no puede enviarse, pero necesita ser recursivamente encapsulado.

Encapsulación Recursiva: El resultado de las necesidades del encapsulado para proteger los encabezados HTTP, es cuando la confidencialidad es requerida, pero el autoperfeccionamiento o incluso la transformación null podría aplicarse en cambio. Es decir, el mensaje mostrado puede ser usado como el contenido interno de un nuevo mensaje S-HTTP, como este:

```
SECURE * Secure-HTTP ...
Content Type: application/x-http
Content-Privacy-Domain: PKCS-7
Content-Transfer-Encoding: base64
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Encrypted version of the message above...
-----END PRIVACY-ENHANCED MESSAGE-----
```

Para desplegar esto, el receptor descifraría el mensaje S-HTTP exterior, reingresa el ciclo parsing (S-)HTTP para procesar el nuevo mensaje, vea que también era S-HTTP, descifre esp, y recupere el contenido interno.

Este acercamiento puede usarse también para proporcionar actualidad a la actividad del servidor (aunque no del propio documento) mientras todavía provee no repudiación de los datos del documento si un NONCE incluido en la solicitud.

- Los Mensajes Preencriptados. Aunque las premejoras trabajan mejor con firma, también pueden ser usadas con encripción bajo ciertas condiciones. Considere la situación donde el mismo documento confidencial será enviado varias veces. El tiempo gastado para encriptar puede ser ahorrado almacenando el texto cifrado y generando un nuevo bloque de intercambio de llaves para cada destinatario.

Sumario de la Sintaxis del Protocolo

Encabezados S-HTTP (Sin encapsular):

```
Content-Privacy-Domain: ('PKCS-7' | 'MOSS')
Content-Transfer-Encoding: ('8BIT' | '7BIT'   'BASE64')
Prearranged-Key-Info: <Hdr-Cipher>,<Key>,<Key ID>
Content-Type: 'application/http'
MAC-Info: [hex(timeofday)','']<hash-alg>','hex(<hash-data>)',' <key-spec>
```

Opciones de no negociación HTTP (Encapsuladas)

```
Key-Assign: <Method>','<Key-Name>','<Lifetime>','<Cipher>';'<Method args>
Encryption-Identity: <name-class>','<key-sel>','<name-args>
Certificate-Info: <Cert-Fmt>','<Cert Group>
Nonce: <string>
Nonce-Echo: <string>
```

Opciones de negociación Encapsuladas:

```
SHTTP-Cryptopts: <scope>';'<string>[,<string>]*
SHTTP-Privacy-Domains: ('PKCS-7' | 'MOSS')
SHTTP-Certificate-Types: ('X.509')
SHTTP-Key-Exchange-Algorithms: ('RSA' | 'KRB-'<kv>)
SHTTP-Signature-Algorithms: ('RSA'   'NIST-DSS')
SHTTP-Message-Digest-Algorithms: ('RSA-MD2' | 'RSA-MD5' | 'NIST-SHS'
       'RSA-MD2-HMAC', 'RSA-MD5-HMAC', 'NIST-SHS-HMAC')
SHTTP-Symmetric-Content-Algorithms: ('DES-CBC' | 'DES-EDE-CBC' |
       'DES-EDE3-CBC' | 'DESX-CBC' | 'CDMF-CBC' | 'IDEA-CBC' |
       'RC2-CBC' |
SHTTP-Symmetric-Header-Algorithms: ('DES-ECB' | 'DES-EDE-ECB'
       'DES-EDE3-EBC' | 'DESX-ECB' | 'CDMF-ECB' |
       'IDEA-ECB' | 'RC2-ECB')
SHTTP-Privacy-Enhancements: ('sign' | 'encrypt' | 'auth')
Your-Key-Pattern: <key-use>','<pattern-info>
```

Métodos HTTP:

```
Secure * Secure HTTP/1.2
```

Reporte de Estatus del Servidor:

```
Secure HTTP/1.2 200 OK
SecurityRetry 4
BogusHeader 421 <reason>
```

Convenciones del Servidor

```
GET SERVER-CERTificATE-Hel LO> <http version>
GET POLICY-<Hel LO> <http version>
GET CRL-<B64-LO> http-version>
```

4.1.3 PCT

El protocolo de Tecnología de Comunicaciones Privadas (PCT – Private Communication Technology) es diseñado para proporcionar privacidad entre aplicaciones cliente/servidor, autenticar al servidor y al cliente (opcional). Se asume que es un protocolo de transporte independiente confiable para transmisión y recepción de datos.

Protocolo de aplicación de alto nivel (HTTP, FTP, TELNET, etc.) que puede actuar transparentemente. Este protocolo inicia con una fase de saludo en la que negocia el algoritmo de encripción y las llaves de sesión (simétricas) tan bien como autentica el servidor al cliente (y viceversa opcionalmente), basado en certificados de llave pública. Cuando inicia la transmisión de datos, todos los datos son encriptados usando la llave de sesión.

No especifica detalles acerca de la verificación de certificados con respecto a las autoridades certificadoras, listas de revocación, entre otros. Más bien se asume que su implementación tiene acceso a una caja negra la cual es capaz de regular los certificados válidos que son recibidos de manera satisfactoria a la implementación del usuario. Esta regulación implica la consulta remota con un servicio de confianza, o con el usuario actual a través de una interfaz gráfica o de texto.

Verifica la integridad de mensajes usando una función hash basada en el código de autenticación de mensajes (MAC).

El formato del protocolo de registro PCT es compatible con el de SSL. La diferencia en PCT es que el bit más significativo del número de la versión del protocolo es colocado en uno. Este protocolo difiere de SSL en el diseño de su fase de saludo, en los siguientes aspectos:

- La vuelta y la estructura de mensajes son considerablemente más cortos y simples: una sesión reconectada sin autenticación del cliente requiere sólo un mensaje en cada dirección, y no otro tipo de conexión requiere más de dos mensajes en cada dirección.
- La negociación para la elección de algoritmos criptográficos y formatos para usar en la sesión ha sido extendida a cubrir más características del protocolo y permitir diferentes características para ser negociadas independientemente. La negociación del cliente PCT y el servidor, agregan un tipo de cifrado y de certificado del servidor, una función hash y un tipo de intercambio de llaves. Si la autenticación del cliente es solicitada, un certificado del cliente y una firma son negociadas también.
- La autenticación del mensaje ha sido adaptada así que ahora usa diferentes llaves que las llaves de encripción. Por lo tanto, las llaves de autenticación de mensajes quizá sean mucho más grandes y seguras que las llaves de encripción, las cuales son más débiles o no existen.
- Un hoyo de seguridad en la autenticación del cliente SSL ha sido reparada, el challenge-response de la autenticación del cliente PCT ahora depende del tipo de cifrado negociado en la sesión. La autenticación del cliente SSL es independiente de la fortaleza del cifrado usado en la sesión y también si la autenticación es ejecutada para una reconexión de una vieja sesión o para una nueva. Como resultado, un atacante de hombre y medio quien ha obtenido la llave de sesión para una sesión usando criptografía débil puede usar ésta para romper la sesión para autenticarse como el cliente en una sesión usando criptografía fuerte.
- Un campo "verify-prelude" ha sido agregado a la fase del saludo, con el cual el cliente y el servidor pueden verificar el tipo de cifrado y otras negociaciones cargadas en claro que no han sido alteradas.

Formato del Encabezado del Registro PCT

PCT usa el mismo formato de registro que SSL, todos los datos enviados se encapsulan en un registro, el cual está compuesto de un encabezado y alguna cantidad de datos non-zero. Cada encabezado de registro contiene una longitud de 2 o 3 bytes de código. Si el bit más significativo es colocado en el primer byte del encabezado de la longitud del código de registro entonces el registro no ha sido rellenado y el total de la longitud del encabezado es de dos bytes, de otra manera el registro ha sido rellenado y la longitud total del encabezado es de tres bytes. El encabezado de registro es transmitido antes de la porción de datos del registro.

Nota que en el caso de encabezados grandes (3 bytes), el segundo bit más significativo en el primer byte tienen un significado especial. Cuando es cero, el registro es enviado en un registro de datos, y cuando es uno, el registro es enviado como un escape de seguridad, y el primer byte del registro es un ESCAPE_TYPE_CODE que indica el tipo de escape ("out-of-band data" escape y "redo handshake" escape.) En cualquier caso, la longitud del código describe cuantos datos son transmitidos en el registro; éste quizá sea más grande que la cantidad de datos después de la desencripción, particularmente si se uso relleno.

El encabezado de registro define un valor llamado PADDING_LENGTH, que especifica cuantos bytes de datos fueron agregados al registro original por el emisor. Los datos de relleno son usados para hacer la longitud de registro un múltiplo del tamaño del cifrado de bloque que es usado para encripción.

El emisor de un registro relleno agrega los datos de relleno al final de los datos normales y entonces encripta la cantidad total. El valor actual de los datos de relleno no importa, pero la forma encriptada debe ser transmitida al receptor para decriptar el registro. Una vez que la cantidad total de datos está siendo transmitida es conocido que el encabezado pudo ser construido con un valor de relleno. El receptor agrega relleno al registro usando el valor de PADDING_LENGTH desee el encabezado cuando determine la longitud de ACTUAL_DATA en el registro de datos.

Formato de los Datos del Registro PCT

El formato de los datos encriptados del registro PCT difiere con la de SSL. El primer mensaje del saludo enviado en cada dirección es enviado en claro, y contiene el campo del número de la versión en ambos protocolos, pero este campo es el que los diferencia. El registro está compuesto de:

```
ENCRYPTED_DATA[N+PADDING_LENGTH]
MAC_DATA[MAC_LENGTH]
```

El campo ENCRYPTED_DATA contiene la encripción de la concatenación del ACTUAL_DATA y PADDING_DATA. El campo MAC_DATA contiene el Código de Autenticación de Mensajes (MAC).

Los registros de saludo son enviados en claro, y el MAC no es usado. Consecuentemente el PADDING_LENGTH será cero y la MAC_LENGTH será cero. Para los registros de datos que no son del saludo, el emisor agrega campos PADDING_DATA que contienen datos arbitrarios, así que N + PADDING_LENGTH es la longitud apropiada para el cifrado usado para encriptar los datos.

MAC_DATA es computado

```
MAC_DATA := Hash( MAC_KEY, Hash( ACTUAL_DATA, PADDING_DATA, SEQUENCE_NUMBER , ) )
```

Si el cliente está enviando el registro, entonces el MAC_KEY es el CLIENT_MAC_KEY; si el servidor está enviando el registro, entonces el MAC_KEY es el SERVER_MAC_KEY. Los parámetros de la invocación interna de la función hash son la entrada de la función hash en el siguiente orden, el SEQUENCE_NUMBER representado en el orden del byte de red o el orden "big endian". Si la longitud de MAC_KEY no es un múltiplo exacto de 8 bits, entonces es considerada para los propósitos de la computación MAC, para tener cero bits (menos de 8) agregados a ésta, para crear una cadena de un número de bytes integrales para la entrada dentro de la función hash MAC

El SEQUENCE_NUMBER es un contador el cual es incrementado por el emisor y el receptor. Por cada dirección de transmisión, un par de contadores es guardado (uno por el emisor y el otro por el receptor). Antes del primer registro (saludo) es enviado o recibido en una conexión PCT todas las secuencias de números inicializadas a cero (excepto en reiniciar la conexión con un token basado en intercambio, en el cual el estado del cifrado es preservado). La secuencia de números del emisor que envía al receptor es incrementada después del envío de cada registro. La secuencia de números con de cantidades sin firmar de 32 bits, y quizá no incremente pasados los 0xFFFFFFFF.

El receptor de un registro primero usa la WRITE_KEY del emisor para decriptar los campos concatenados ACTUAL_DATA y PADDING_DATA, entonces usa la MAC_KEY del emisor, el ACTUAL_DATA, el PADDING_DATA, y el valor esperado de la secuencia de números como entrada en la función MAC_DATA. El MAC_DATA computado debe acordar bit por bit con el MAC_DATA transmitido. Si los dos no son idénticos, entonces ocurre un error INTEGRITY_CHECK_FAILED y es recomendado que el registro sea tratado como sino contuviera datos. Este mismo error ocurre si N + PADDING_LENGTH no es correcto para el bloque de cifrado usado.

La capa de registro PCT es usada para todas las comunicaciones PCT, incluyendo el mensaje de saludo, los escapes de seguridad y la transferencia de datos de aplicación. Para los encabezados de dos bytes, la longitud máxima del registro es de 32767 bytes; y para encabezados de tres bytes, la longitud máxima del registro es de 16383 bytes.

Escapes de Seguridad

a) Out-Of-Band Data

Soporta la transmisión y recepción de datos fuera de banda como SSL, esto es definido en el nivel del protocolo TCP/IP, pero a PCT le es difícil soportarlo. Para enviar los datos fuera de banda, el emisor envía un registro escape en el que su cuerpo sólo contiene un byte de datos y es el valor del ESCAPE_TYPE_CODE PCT_ET_OOB_DATA. El registro siguiente del registro de escape será interpretado como datos fuera de banda y sólo será disponible para el receptor a través de un mecanismo sin especificar que es diferente desde el método normal de recepción de datos del receptor. El registro de escape y el registro de datos transmitidos son transmitidos normalmente (encripción, cómputos MAC, y el resto es el relleno del cifrado de bloque). El registro de escape y el registro de datos asociados son enviados usando los mecanismo de envío TCP, no usando los mecanismos fuera de banda. El escape "Redo Handshake" asociado a los mensajes de saludo quizá se interpongan entre un registro de escape fuera de banda y su registro asociado. En tal caso, el primer registro de no escape, no saludo seguido de un registro de escape fuera de banda será tratado como fuera de banda.

b) Redo Handshake

Permite al cliente o al servidor solicitar, tiempo después de que la fase de saludo ha sido completada por una conexión, otra fase de saludo será ejecutada para esa conexión. Por tal razón se recomienda que la implementación forcé un límite en la duración de ambas conexiones y sesiones, con respecto al número de bytes totales enviados, al número de registros enviados, el tiempo actual transcurrido desde el inicio de la conexión o la sesión, y en el caso de sesiones, el número de las reconexiones hechas. Ese límite sirve para asegurar que las llaves no son usadas más que esta vez y quizá, la discreción del implementador, incluya indicaciones desde la aplicación como la sensitividad de los datos que están siendo transmitidos o recibidos.

La solicitud de una nueva fase de saludo para esta conexión, el emisor (cliente o servidor) envía un registro escape el cual contiene en su cuerpo un solo byte de datos que es el valor del ESCAPE_TYPE_CODE PCT_ET_REDO_CONN. El registro de escape es transmitido normalmente (encripción, cómputos MAC, y el resto es el relleno del cifrado de bloque).

Hay muchos casos para considerar la seguridad de que el mensaje ha sido descargado y permitir que los mensajes de saludo sean distinguidos desde los registros de datos. Las siguientes reglas aseguran que el primer mensaje en el saludo rehecho son siempre precedido inmediatamente por un mensaje de escape "Redo Handshake".

Si el cliente inicia el "Redo Handshake", envía este mensaje inmediatamente seguido por un mensaje normal CLIENT_HELLO. el servidor, al recibir este mensaje "Redo Handshake", quizá sea en uno de dos estados. Si el mensaje fue un "Redo Handshake", entonces simplemente espera el mensaje CLIENT_HELLO; de otra manera, envía el mensaje "Redo Handshake" en respuesta, y espera el mensaje CLIENT_HELLO.

Si el servidor inicia el "Redo Handshake", entonces el servidor envía el mensaje "Redo Handshake" y espera un mensaje "Redo Handshake" en respuesta, este "Redo Handshake" debería ser seguido de un mensaje normal

CLIENT_HELLO. El cliente, al recibir el mensaje "Redo Handshake" del servidor, quizá sea uno de dos estados. Si el último de los dos mensajes enviados fuera un mensaje "Redo Handshake" seguido por un mensaje CLIENT_HELLO, entonces simplemente espera un mensaje del servidor SERVER_HELLO; de esta manera, envía un mensaje "Redo Handshake" en respuesta, seguido por un mensaje CLIENT_HELLO , y entonces espera para un mensaje SERVER_HELLO.

En todos los casos, el emisor del mensaje "Redo Handshake" continúa para procesar los mensajes de entrada, pero quizá no envía algún mensaje que no se de un saludo hasta que el nuevo saludo se completa.

La fase de saludo que sigue al mensaje "Redo Handshake" es algo normal; el cliente quizá solicite la reconexión de una sesión vieja, o solicite que una nueva sesión sea iniciada, y el servidor, al recibir una solicitud de reconexión, pueda aceptar la reconexión o demandar que una nueva sesión sea iniciada. Si la nueva sesión es establecida, entonces el servidor debe solicitar la autenticación del cliente si y solo si la autenticación del cliente fue solicitada en una sesión previa. De otra manera, la autenticación del cliente es opcional. Ambas partes deben verificar que las especificaciones negociadas previamente en la sesión, tan bien como algunos certificados intercambiados, sean idénticas a las encontradas en la nueva fase de saludos. Un resultado. Un desajuste en un SPECS_MISMATCH o un error BAD_CERTIFICATE aseguran que las propiedades de la seguridad del canal de comunicación no cambian.

Flujo del Protocolo de Saludo PCT

El protocolo de saludo es usado para negociar las mejoras de seguridad para los datos enviados usando el protocolo de registro PCT. Estas mejoras consisten de autenticación, encripción simétrica e integridad de mensajes. La encripción simétrica se da usando un algoritmo de intercambio de llaves como RSA, Diffie-Hellman y Fortezza. Consiste de cuatro mensajes, enviados respectivamente por el cliente, servidor, cliente y servidor (algunas veces los últimos dos mensajes pueden ser omitidos). Los mensajes son, en orden, CLIENT_HELLO, SERVER_HELLO, CLIENT_MASTER_KEY, y SERVER_VERIFY.

El contenido general de los mensajes depende de dos criterios: si la conexión que se realiza es una reconexión o una nueva sesión y si el cliente será autenticado. El primer criterio es determinado por el cliente y el servidor; el CLIENT_HELLO tendrá diferentes contenidos dependiendo si una nueva sesión es iniciada o una vieja continúa, y el mensaje SERVER_HELLO también confirmara una continuación de la solicitud de una vieja sesión, o requiere que una nueva sesión sea iniciada. El segundo criterio es determinado por el servidor, el SERVER_HELLO quizá contenga un demanda para autenticación del cliente. Si el servidor no requiere la autenticación del cliente, y la reconexión de una vieja sesión es solicitada por el cliente y aceptada por el servidor, entonces los mensajes CLIENT_MASTER_KEY y SERVER_VERIFY no son necesarios, y son omitidos.

El mensaje CLIENT_HELLO contiene un challenge de autenticación aleatoria para el servidor y solicita uno para el tipo y nivel de criptografía y certificación usada para la sesión. Si el cliente intenta continuar la vieja sesión, entonces es también suplido el ID de sesión.

En el caso de una nueva sesión el mensaje SERVER_HELLO contiene un certificado y un identificador de conexión aleatoria, este identificador dobla como un challenge de autenticación para el cliente si el servidor desde autenticar al cliente. El mensaje CLIENT_MASTER_KEY enviado por el cliente en respuesta incluye la llave maestra para la sesión, encriptada usando la llave pública del certificado del servidor, tan bien como un certificado y una respuesta al challenge de autenticación del servidor, si es solicitado. Para asegurar que los mensajes previos sin encriptar no fueron alterados, su hash que tiene llaves es incluida con el mensaje CLIENT_MASTER_KEY. Finalmente, el servidor envía un mensaje SERVER_VERIFY que incluye una respuesta el challenge del cliente y un id de sesión aleatoria para la sesión.

Si el servidor acepta el id de la sesión vieja, entonces el mensaje SERVER_HELLO contiene una respuesta al challenge del cliente, y un identificador de conexión aleatoria el cual nuevamente se duplica como un challenge aleatorio para el cliente, si el servidor requiere la autenticación del cliente. Si la autenticación del cliente no es solicitada, el saludo termina (aunque una autenticación del cliente es implícita en el MAC incluido con el primer

mensaje de datos del cliente). De otra manera, el mensaje CLIENT_MASTER_KEY subsecuente contiene la respuesta del cliente, y el mensaje SERVER_VERIFY simplemente señala al cliente continuar.

Para una nueva sesión, la fase de saludo tiene la siguiente forma (lo que esta en corchetes es si se requiere la autenticación del cliente):

Cliente	**Servidor**
CLIENT_HELLO: client challenge; client's cipher, hash, server-certificate, and key-exchange specification lists	
	SERVER_HELLO: Connection id/server challenge; server's cipher, hash, server-certificate, and key-exchange specification choices; server certificate [; server's signature-type and client-certificate specification lists]
CLIENT_MASTER_KEY: master key, encrypted with server's public key; authentication of previous two messages [; client's signature-type and client-certificate specification choices; client's certificate; client's challenge response]	
	SERVER_VERIFY: session id; server's challenge response

Para una reconexión de una vieja sesión, la fase de saludo tiene la siguiente forma (lo que está en corchetes es si se requiere la autenticación del cliente):

Cliente	**Servidor**
CLIENT_HELLO: client challenge; session id; client's cipher, hash, server-certificate, and key-exchange specification choices	
	SERVER_HELLO: Connection id/server challenge; old session's cipher, hash, server-certificate, and key-exchange specification choices; server's challenge response [; server's signature-type and client-certificate specification lists]
CLIENT_MASTER_KEY: client's certificate; client's challenge response]	
	SERVER_VERIFY]

Nota que el protocolo es asimétrico entre el cliente y el servidor. El cliente autentica al servidor porque sólo el servidor puede decriptar la llave maestra la cual es encriptada con la llave pública del servidor, y la respuesta challenge del servidor depende en el conocimiento de la llave maestra. El servidor autentica al cliente porque el cliente firma su challenge response con su llave pública. La razón para la asimetría es que cuando no hay autenticación del cliente, no hay llave pública, así que el cliente debe escoger la llave maestra y encriptarla con la llave pública del servidor para esconderla de todos excepto del servidor.

Usualmente el cliente puede seguramente enviar datos en el transporte implícito inmediatamente seguido por el mensaje CLIENT_MASTER_KEY sin esperar el SERVER_VERIFY; a esto lo llamamos datos iniciales. El envío de los datos iniciales es bueno porque significa que PCT agrega sólo un viaje; éste no es posible de mejorar sin la exposición del servidor a un ataque de repetición. Sin embargo, este es imprudente para enviar los datos iniciales si por alguna razón éste es importante para el cliente asegurarse de estar en contacto con el servidor correcto antes de enviar algún dato.

Mensajes del Protocolo de Saludo PCT

Estos mensajes son enviados usando el protocolo de Registro PCT y consiste de un mensaje de un solo byte de código, seguido de algunos datos. El intercambio de mensajes del cliente y del servidor se da enviándose de uno a dos mensajes uno a otro. Una vez que el saludo ha sido completado exitosamente, el cliente envía primero su ACTUAL_DATA.

Los mensajes del protocolo de saludo son enviados en claro, con la excepción de los campos de intercambio de llaves que se incluyen en el mensaje CLIENT_MASTER_KEY , ya que algunos tienen encripción de llave pública.

La siguiente notación es usada para los mensajes PCT:

```
MSG_EXAMPLE
FIELD1
FIELD2
THING_LENGTH_MSB
THING_LENGTH_LSB
THING_DATA[(MSB<<8) LSB];
```

El orden de la notación describe el orden de cómo son enviados los datos.

Para la entrada "THING_DATA", los valores MSB y LSB son actualmente THING_LENGTH_MSB y THING_LENGTH_LSB y definen el número de bytes de datos actualmente presentados en el mensaje.

Los códigos de longitud son valores sin firmar, y siempre vienen en bytes.

CLIENT_HELLO (enviado en claro)

```
CH_MSG_CLIENT_HELLO
CH_CLIENT_VERSION_MSB
CH_CLIENT_VERSION_LSB
CH_PAD
CH_SESSION_ID_DATA[32]
CH_CHALLENGE_DATA[32]
CH_OFFSET_MSB
CH_OFFSET_LSB
CH_CIPHER_SPECS_LENGTH_MSB
CH_CIPHER_SPECS_LENGTH_LSB
CH_HASH_SPECS_LENGTH_MSB
CH_HASH_SPECS_LENGTH_LSB
CH_CERT_SPECS_LENGTH_MSB
CH_CERT_SPECS_LENGTH_LSB
CH_EXCH_SPECS_LENGTH_MSB
CH_EXCH_SPECS_LENGTH_LSB
```

```
CH_KEY_ARG_LENGTH_MSB
CH_KEY_ARG_LENGTH_LSB
CH_CIPHER_SPECS_DATA[(MSB<<8)|LSB]
CH_HASH_SPECS_DATA[(MSB<<8)|LSB]
CH_CERT_SPECS_DATA[(MSB<<8)|LSB]
CH_EXCH_SPECS_DATA[(MSB<<8)|LSB]
CH_KEY_ARG_DATA[MSB<<8|LSB]
```

Cuando un cliente primero se conecta a un servidor es requerido que envíe el mensaje CLIENT_HELLO. El servidor está esperando este mensaje desde el cliente como su primer mensaje. Este es un error ILLEGAL_MESSAGE para un cliente enviar alguna cosa más como primer mensaje. El mensaje CLIENT_HELLO inicia con el número de la versión de PCT, y dos campos de longitud arreglados seguidos por un conjunto de datos de longitud variable. El campo CH_OFFSET contiene número de bytes usado por varios campos que siguen el campo OFFSET y precede a los campos de longitud variable. Para la versión 1 de PCT, el valor OFFSET es siempre PCT_CH_OFFSET_V1. El campo CH_PAD quizá contenga algún valor.

El mensaje CLIENT_HELLO incluye una cadena de bytes aleatorios usado como datos challenge desde el cliente. También, si el cliente encuentra un identificador de sesión en la memoria cache para el servidor , entonces los datos de identificación de la sesión son enviados. De otra manera, el valor especial PCT_SESSION_ID_NONE es usado. En cualquiera de los casos, el cliente especifica CIPHER_SPECS_DATA, HASH_SPECS_DATA, CERT_SPECS_DATA, y EXCH_SPECS_DATA sus opciones de cifrados simétrico, longitud de llaves, funciones hash, certificados, y algoritmos de intercambio de llaves asimétricas. Sin embargo, si el identificador de la sesión es enviado, entonces las opciones elegidas son relevantes en el caso donde el servidor no reconozca el identificador de sesión, y una nueva sesión de ser iniciada. Si el servidor reconoce la sesión, entonces esos campos son ignorados por el servidor.

El campo CHALLENGE_DATA contiene 32 bytes de bits aleatorios, para ser usados en la autenticación del servidor, este debería ser criptográficamente aleatorio.

El campo CIPHER_SPECS_DATA contiene una lista de posibles cifrados simétricos soportados por el cliente, en orden de preferencia. Cada elemento de la lista es de campos de 4 bytes, de los cuales los primeros dos bytes contienen un código representando el tipo de cifrado, el tercer byte contiene la longitud de las llaves de encripción en bits (0-255), y el cuarto byte contiene la longitud de la llave MAC en bits, menos 64 (valores 0-255, representando longitudes de 64-319, esta codificación aplica los requerimientos que la longitud de la llave MAC debe ser de al menos 64 bits). La longitud de la lista entera en bytes (cuatro veces el número de los elemento) es colocada en el campo CIPHER_SPECS_LENGTH.

El campo HASH_SPECS_DATA contiene una lista de posibles funciones hash soportadas por el cliente, en orden de preferencia. El servidor escogerá uno de esos para ser usado computando los MACs y derivando llaves. Cada elemento en la lista es de campos de dos bytes conteniendo un código representando a la opción de función hash elegida. La longitud de la lista (dos veces el número de elementos) es colocada en el campo HASH_SPECS_LENGTH.

El campo CERT_SPECS_DATA contiene una lista de posibles formatos de certificados soportados por el cliente, en orden de preferencia. Cada elemento en la lista es de campos de dos bytes contiene una lista de posibles formatos de certificados soportados por el cliente, en orden de preferencia.

El campo EXCH_SPECS_DATA contiene una lista de posibles algoritmos de intercambio de llaves asimétricos soportados por el cliente, en orden de preferencia. Cada elemento en la lista es de campos de dos bytes conteniendo un código representando el tipo de algoritmo. La longitud de la lista (dos veces el número de elementos) es colocada en el campo EXCH_SPECS_LENGTH.

El campo KEY_ARG_DATA contiene un vector de inicialización usado para reconectar la sesión cuando el tipo de cifrado es un cifrado de bloque (excepto con PCT_CIPHER_RC4, y en intercambio de llaves excepto con PCT_EXCH_RSA_PKCS1_TOKEN_RC4). Si una nueva sesión es solicitada, entonces el campo KEY_ARG_LENGTH debe ser cero.

El mensaje CLIENT_HELLO debe ser el primer mensaje enviado por el cliente al servidor. Después de que el mensaje es enviado al cliente espera el mensaje SERVER_HELLO. Algún otro mensaje regresado por el servidor genera el error PCT_ERR_ILLEGAL_MESSAGE.

El servidor, recibe el mensaje CLIENT_HELLO, verifica el número de la versión y el campo OFFSET para determinar donde inician los campos de los datos de longitud variable. El servidor entonces verifica si el campo SESSION_ID no es un nulo, y si lo es, si reconoce el id. En ese caso, el servidor responde con el mensaje SERVER_HELLO conteniendo un campo diferente de cero RESTART_SESSION_OK, y el valor apropiado en los campos RESPONSE y CONNECTION_ID. De otra manera, verifica si las listas CIPHER_SPECS, HASH_SPECS, CERT_SPECS y EXCH_SPECS en el mensaje CLIENT_HELLO contiene al menos un tipo de cada uno soportado por el servidor. Si así es, entonces el servidor envía el mensaje SERVER_HELLO al cliente, de otra manera, el servidor envía el mensaje de error SPECS_MISMATCH.

SERVER_HELLO (Enviado en claro)

```
SH_MSG_SERVER_HELLO
SH_PAD
SH_SERVER_VERSION_MSB
SH_SERVER_VERSION_LSB
SH_RESTART_SESSION_OK
SH_CLIENT_AUTH_REQ
SH_CIPHER_SPECS_DATA[4]
SH_HASH_SPECS_DATA[2]
SH_CERT_SPECS_DATA[2]
SH_EXCH_SPECS_DATA[2]
SH_CONNECTION_ID_DATA[32]
SH_CERTIFICATE_LENGTH_MSB
SH_CERTIFICATE_LENGTH_LSB
SH_CLIENT_CERT_SPECS_LENGTH_MSB
SH_CLIENT_CERT_SPECS_LENGTH_LSB
SH_CLIENT_SIG_SPECS_LENGTH_MSB
SH_CLIENT_SIG_SPECS_LENGTH_LSB
SH_RESPONSE_LENGTH_MSB
SH_RESPONSE_LENGTH_LSB
SH_CERTIFICATE_DATA[MSB<<8|LSB]
SH_CLIENT_CERT_SPECS_DATA[MSB<<8|LSB]
SH_CLIENT_SIG_SPECS_DATA[MSB<<8|LSB]
SH_RESPONSE_DATA[MSB<<8|LSB]
```

El servidor envía este mensaje después de recibir el mensaje CLIENT_HELLO. El número de la versión PCT en SH_SERVER_VERSION es siempre la versión de protocolo máximo que el servidor soporta, el resto del mensaje y todos los mensajes subsecuentes se conformaran al formato especificado por la versión del protocolo correspodiente a la mínima versión del protocolo del cliente y del servidor. A menos que haya un error, si el servidor siempre regresa un valor aleatorio de 32 bytes en la longitud del campo CONNECTION_ID. Este valor duplica al data challenge si el servidor solicita la autenticación del cliente, y debería por lo tanto ser un aleatorio en el challenge data en el mensaje CLIENT_HELLO. El campo SH_PAD quizá contenga algún valor.

Hay dos casos para RESTART_SESSION_OK. En el primer caso, el servidor regresa una bandera cero de RESTART_SESSION_OK porque el mensaje CLIENT_HELLO no contiene ningún id de sesión o porque el que lo contiene no es reconocido por el servidor. En este caso, el servidor debe comportarse como sigue

El servidor selecciona alguna opción la cual es compatible, desde cada lista CH_CIPHER_SPECS, CH_HASH_SPECS, CH_CERT_SPECS y CH_EXCH_SPECS proporcionadas en el mensaje CLIENT_HELLO El certificado es especificado en SH_CERT_SPECS_DATA y SH_EXCH_SPECS_DATA que son colocados en el campo CERTIFICATE_DATA field. El campo SH_RESPONSE_DATA está vacío, y su longitud es cero. En el segundo caso, el servidor regresa un valor diferente de cero para la bandera RESTART_SESSION_OK por el mensaje CLIENT_HELLO contiene un identificador de sesión diferente al que conoce el servidor. En este caso el servidor se comporta como sigue:

El servidor omite el campo CERTIFICATE_DATA (con CERTIFICATE_LENGTH en cero), y pone los valores a CIPHER_SPECS_DATA, HASH_SPECS_DATA, CERT_SPECS_DATA y EXCH_SPECS_DATA para los valores almacenados junto con el identificador de sesión. Hay dos subcasos: (1) Si el SH_EXCH_SPECS_DATA no hace referencia a un tipo TOKEN, entonces las llaves CLIENT_MAC, SERVER_MAC, CLIENT_WRITE, y SERVER_WRITE son rederivadas usando la MASTER_KEY de la vieja sesión, tan bien como los valores de CONNECTION_ID y CH_CHALLENGE desde los mensajes SERVER_HELLO y CLIENT_HELLO, respectivamente, para esta conexión. (2) Si el SH_EXCH_SPECS_DATA se refiere a un tipo TOKEN, entonces las llaves desde la sesión que continúa son reusados. En orden para obtener material de codificación reciente o cambiar el número de la secuencia, las implementaciones TOKEN deben usar un mecanismo REDO_HANDSHAKE. Cuando este mecanismo es usado con un tiempo de intercambio TOKEN, el cliente debe enviar PCT_SESSION_ID_NONE en el campo CH_SESSION_ID_DATA del mensaje subsecuente CLIENT_HELLO.

El RESPONSE_DATA es construido computando la función :

```
Hash( SERVER_MAC_KEY, Hash( "SR", CH_CHALLENGE_DATA,
SH_CONNECTION_ID_DATA, CH_SESSION_ID_DATA ) ).
```

Los valores CH_CHALLENGE_DATA y CH_SESSION_ID_DATA son encontrados en el mensaje CLIENT_HELLO para esta conexión. El valor SH_CONNECTION_ID_DATA es el del mensaje SERVER_HELLO. El SERVER_MAC_KEY es rederivado de esta conexión. Si la longitud de SERVER_MAC_KEY no es un múltiplo exacto de ocho bits, entonces es considerada, para propósitos de la computación del MAC, para agregarle los bits faltantes, para crear una cadena de un número integral de bytes como entrada de la función hash MAC. Esta función hash es determinada en el campo SH_HASH_SPECS_DATA en el mensaje SERVER_HELLO.

En ambos casos de reconexión, si el servidor requiere la autenticación del cliente, el campo CLIENT_AUTH_REQ es colocado un valor diferente de cero. También, una lista de tipos de certificados (cliente) aceptables para el servidor, en orden de preferencia, es colocado en el campo CLIENT_CERT_SPECS_DATA, y una lista de algoritmos de firma soportados por el servidor, en orden de preferencia es colocado en el campo CLIENT_SIG_SPECS_DATA. Los valores de los certificados en la lista deben ser de dos bytes usados para la lista CERT_SPECS que aparece en el mensaje CLIENT_HELLO y el algoritmo de firma también es de dos bytes de longitud. Las longitudes de la lista en bytes (duplica el número de elementos) son colocadas en los campos CLIENT_CERT_SPECS_LENGTH y CLIENT_SIG_SPECS_LENGTH. Sino es requerida la autenticación del cliente, entonces la longitud de esos campos y el campo CLIENT_AUTH_REQ, son colocadas en cero, y los campos de datos correspondientes vacíos.

Cuando el cliente recibe el mensaje SERVER_HELLO, verifica si el servidor ha aceptado la reconexión de una vieja sesión o si establece una nueva sesión. Si se inicia una nueva sesión, y se solicita la autenticación del cliente, entonces el cliente verifica si es compatible con alguno de los certificados y firmas listados en las listas CLIENT_CERT_SPECS y CLIENT_SIG_SPECS. Si el cliente puede proveer un certificado compatible, entonces envía un mensaje CLIENT_MASTER_KEY, de otra manera genera un error SPECS_MISMATCH.

Si la sesión es una vieja, entonces el cliente establece los nuevos CLIENT_WRITE_KEY, SERVER_WRITE_KEY, CLIENT_MAC_KEY y SERVER_MAC_KEY de acuerdo a las reglas de CIPHER_SPEC acordadas. El cliente verifica el contenido del campo RESPONSE_DATA en el mensaje SERVER_HELLO para ver si es correcto. Si la respuesta es igual al valor calculado por el cliente, entonces el saludo es terminado, y el cliente empieza a enviar datos, de otra manera ocurre un error SERVER_AUTH_FAILED.

CLIENT_MASTER_KEY (enviado en claro excepto las llaves)

```
CMF_MSG_CLIENT_MASTER_KEY
CMF_PAD
CMF_CLIENT_CERT_SPE[...]ATA[?]
CMF_CLIENT_SIG_SPE[...]ATA[?]
CMF_CLEAR_KEY_LENGTH_MSB
CMF_CLEAR_KEY_LENGTH_LSB
```

```
CMK_ENCRYPTED_KEY_LENGTH_MSB
CMK_ENCRYPTED_KEY_LENGTH_LSB
CMK_KEY_ARG_LENGTH_MSB
CMK_KEY_ARG_LENGTH_LSB
CMK_VERIFY_PRELUDE_LENGTH_MSB
CMK_VERIFY_PRELUDE_LENGTH_LSB
CMK_CLIENT_CERT_LENGTH_MSB
CMK_CLIENT_CERT_LENGTH_LSB
CMK_RESPONSE_LENGTH_MSB
CMK_RESPONSE_LENGTH_LSB
CMK_CLEAR_KEY_DATA[MSB<<8|LSB]
CMK_ENCRYPTED_KEY_DATA[MSB<<8|LSB]
CMK_KEY_ARG_DATA[MSB<<8|LSB]
CMK_VERIFY_PRELUDE_DATA[MSB<<8|LSB]
CMK_CLIENT_CERT_DATA[MSB<<8|LSB]
CMK_RESPONSE_DATA[MSB<<8|LSB]
```

El cliente envía este mensaje después de recibir el mensaje SERVER_HELLO desde el servidor si una nueva sesión es iniciada o si la autenticación del cliente ha sido requerida. Sino ha sido requerida la autenticación y la vieja sesión está reconectada, entonces el mensaje CLIENT_MASTER_KEY no es enviado.

Para tipos de intercambio TOKEN, ambos cliente y servidor ponen la secuencia de números acero cuando este mensaje es enviado/recibido

El contenido de los campos CLEAR_KEY_DATA, ENCRYPTED_KEY_DATA, y KEY_ARG_DATA dependen del contenido de los campos SH_CIPHER_SPECS_DATA y SH_EXCH_SPECS_DATA en el mensaje SERVER_HELLO presente. El campo CMK_PAD quizá contenga algún valor

El campo CMK_VERIFY_PRELUDE_DATA contiene el valor Hash(CLIENT_MAC_KEY, Hash("cvp", CLIENT_HELLO, SERVER_HELLO)).

Si la longitud de CLIENT_MAC_KEY no es un múltiplo exacto de 8 bits, entonces es considerada, para los propósitos de la computación MAC, agregándole los faltantes bits en cero, para crear una cadena de un número integral de bytes para entrada dentro de la función hash MAC. Esta función está especificada en SH_HASH_SPECS_DATA. Nota que el cliente necesito sólo guardar una corrida del hash de todos los valores pasados en los primeros dos mensajes, entonces el resultado usando CLIENT_MAC_KEY cuando genera, el valor computado VERIFY_PRELUDE.

Si SH_CLIENT_AUTH_REQ es cero, entonces CMK_CLIENT_CERT_SPECS_DATA y CMK_CLIENT_SIG_SPECS_DATA son cero, y los campos CMK_CLIENT_CERT y CMK_RESPONSE_DATA están vacíos. Por otra parte, el campo CMK_RESPONSE_DATA contiene la respuesta de la autenticación del cliente, y los campos CMK_CLIENT_CERT_SPECS_DATA y campos de CMK_CLIENT_SIG_SPECS_DATA contienen las opciones del cliente del SH_CLIENT_CERT_SPECS_DATA y SH_CLIENT_SIG_SPECS_DATA lista, respectivamente. El campo de CMK_CLIENT_CERT_DATA contiene el certificado del cliente que debe emparejar el tipo del certificado especificado en el campo de CMK_CLIENT_CERT_SPECS_DATA. También, la llave pública en el certificado debe ser una llave de la firma del tipo especificada en CMK_CLIENT_SIG_SPECS_DATA que a su vez debe emparejar uno de los tipos en la lista de SH_CLIENT_SIG_SPECS_DATA.

CMK_RESPONSE_DATA simplemente es una firma digital y usa la llave privada asociada con la llave pública en el certificado del cliente, de valor en el campo CMK_VERIFY_PRELUDE_DATA. El algoritmo de la firma es determinado por el campo CMK_CLIENT_SIG_SPECS_DATA.

Al recibir un mensaje de CLIENT_MASTER_KEY, el servidor realiza las funciones descritas en el CIPHER_SPECS para establecer los nuevos CLIENT_WRITE_KEY, SERVER_WRITE_KEY, CLIENT_MAC_KEY y SERVER_MAC_KEY. El servidor entonces verifica los valores VERIFY_PRELUDE_DATA, el certificado del cliente, y la contestación del cliente para la exactitud y validez. La verificación de VERIFY_PRELUDE_DATA y RESPONSE_DATA son realizadas recomputando su valor

correcto, y comparándolos con los valores recibidos. El certificado es verificado usando un mecanismo que ha sido implementado para validar certificados, y la firma en el campo RESPONSE_DATA es verificada usando el algoritmo de verificación asociado con el esquema de la firma usada. Si todos estos valores pasan su verificación, entonces el servidor envía el mensaje SERVER_VERIFY; de otra manera, un error ocurre

SERVER_VERIFY (Enviado en claro)

```
SV_MSG_SERVER_VERIFY
SV_PAD
SV_SESSION_ID_DATA[32]
SV_RESPONSE_LENGTH_MSB
SV_RESPONSE_LENGTH_LSB
SV_RESPONSE_DATA[MSB<<8|LSB]
```

El servidor envía este mensaje al recibir un mensaje válido CLIENT_MASTER_KEY del cliente. El campo SV_PAD puede contener algún valor. Si una sesión vieja está reconectándose, entonces el campo de RESPONSE_DATA está vacío, su longitud es cero, y el campo SESSION_ID_DATA puede contener algún valor. Por otra parte, el campo SV_SESSION_ID_DATA contiene un valor de 32 bytes de longitud que debe generarse aleatoriamente. El valor PCT_SESSION_ID_NONE no debe usarse como un valor SV_SESSION_ID_DATA. Los contenidos del campo SV_RESPONSE_DATA son construidos computando la función

```
Hash( SERVER_MAC_KEY, Hash( "sr", CH_CHALLENGE_DATA,
SH_CONNECTION_ID_DATA, SV_SESSION_ID_DATA ) ).
```

Los valores CH_CHALLENGE_DATA y SH_CONNECTION_ID_DATA, la opción de función hash usada, y el valor SERVER_MAC_KEY es determinado por los mensajes CLIENT_HELLO, SERVER_HELLO y CLIENT_MASTER_KEY, respectivamente, precediendo el mensaje SERVER_VERIFY. Los valores son entrada en la invocación interior de la función hash en el orden especificado. Si la longitud de SERVER_MAC_KEY no es un múltiplo exacto de ocho bits, entonces SERVER_MAC_KEY es considerado, para los propósitos del cómputo de MAC, para tener (menos que ocho) bits ceros añadidos a él, y crear una cadena de un número integro de bytes para la entrada en la función hash MAC.

Cuando el cliente recibe este mensaje, verifica la exactitud de los datos de respuesta, computando el valor hash y comparándolo con el recibido. Si es correcto, entonces el cliente procede con los primeros registros de transmisión de datos; de otra manera, un error SERVER_AUTH_FAILED ocurre. Una aplicación puede escoger enviar datos iniciales inmediatamente después del mensaje CLIENT_MASTER_KEY, sin esperar a que llegue el mensaje SERVER_VERIFY, si verifica la identidad del servidor antes de enviarle cualquier dato

Algoritmos de intercambio de llaves

```
PCT_EXCH_RSA_PKCS1
PCT_EXCH_RSA_PKCS1_TOKEN_DES
PCT_EXCH_RSA_PKCS1_TOKEN_DES3
PCT_EXCH_RSA_PKCS1_TOKEN_RC2
PCT_EXCH_RSA_PKCS1_TOKEN_RC4
PCT_EXCH_DH_PKCS3
PCT_EXCH_DH_PKCS3_TOKEN_DES
PCT_EXCH_DH_PKCS3_TOKEN_DES3
PCT_EXCH_FORTEZZA_TOKEN
```

Nota que los tipos de intercambio de llaves especifican cifrado también, si uno de éstos es escogido, entonces su opción de cifrado aparece en el campo de SH_CIPHER_SPECS_DATA del mensaje de SERVER_HELLO.

Para el intercambio de llaves PCT_EXCH_RSA_PKCS1, un valor MASTER_KEY debería ser generado por el cliente aleatoriamente en el siguiente sentido: los atacantes no deben poder predecir cualquiera de los bits de MASTER_KEY. Se recomienda que los bits usados sean generados aleatoria y uniformemente o generados usando un generador criptográfico seguro de números pseudo aleatorios, con el cual se alimenta aleatoria y uniformemente generando la semilla. El valor MASTER_KEY es encriptado usando la llave pública de

encripción del servidor, obtenida del certificado del servidor en el campo SH_CERTIFICATE_DATA del mensaje SERVER_HELLO. La encripción debe seguir el formato estándar RSA PKCS#1. Esta encripción se envía al servidor en el campo CMK_ENCRYPTED_KEY_DATA del mensaje CLIENT_MASTER_KEY, y es decriptada por el servidor para obtener MASTER_KEY.

Para el intercambio de llaves PCT_EXCH_DH_PKCS3, un valor privado aleatoriamente "x" y el valor público correspondiente "y" son generados por el cliente siguiendo el formato estándar RSA PKCS#3. El valor "y" es entonces enviado al servidor en el campo CMK_ENCRYPTED_KEY_DATA del mensaje CLIENT_MASTER_KEY. El valor privado del cliente x, junto con el valor público "y" incluido en el certificado del servidor en el campo SH_CERTIFICATE_DATA del mensaje SERVER_HELLO, es usado para generar MASTER_KEY. El servidor usa su valor privado, "x' ", junto con el valor de "y" enviado por el cliente, para obtener el mismo valor de MASTER_KEY.

Para los varios tipos de TOKEN de intercambio de llaves, todo el material de codificación está contenido en el campo CMK_ENCRYPTED_KEY_DATA, pero el formato de los datos es definido por la implementación del token.

La longitud de MASTER_KEY depende del tipo de intercambio de llaves. Para los intercambios PCT_EXCH_RSA_PKCS1 y PCT_EXCH_DH_PKCS3, MASTER_KEY es de valor de 128-bits. El CLIENT_WRITE_KEY y SERVER_WRITE_KEY se computan como sigue:

```
CLIENT_WRITE_KEY_i  = Hash( i, "cw", MASTER_KEY, "cw"^i,
SH_CONNECTION_ID_DATA, "cw"^i, SH_CERTIFICATE_DATA,"cw"^i,
CH_CHALLENGE_DATA, "cw"^i )

SERVER_WRITE_KEY_i = Hash( i, "svw", MASTER_KEY, "svw"^i,
SH_CONNECTION_ID_DATA, "svw"^i, CH_CHALLENGE_DATA, "svw"^i )
```

Donde x"^i denota i copias de i de la cadena concatenada "x".

CLIENT_MAC_KEY y SERVER_MAC_KEY son computadas como sigue:

```
CLIENT_MAC_KEY_i = Hash( i, MASTER_KEY, "cmac"^i,
SH_CONNECTION_ID_DATA, "cmac"^i, SH_CERTIFICATE_DATA, "cmac"^i,
CH_CHALLENGE_DATA, "cmac"^i )

SERVER_MAC_KEY_i = Hash( i, MASTER_KEY, "svmac"^i,
SH_CONNECTION_ID_DATA, "svmac"^i, CH_CHALLENGE_DATA, "svmac"^i )
```

Donde x"^i denota i copias de i de la cadena concatenada "x".

Tipos de Cifrados

```
PCT_CIPHER_DES
PCT_CIPHER_IDEA
PCT_CIPHER_RC2
PCT_CIPHER_RC4
PCT_CIPHER_DES_112
PCT_CIPHER_DES_168
```

Cada uno de estos tipos es denotado por código de dos-bytes, y es seguido en campos CIPHER_SPECS_DATA por dos especificaciones de longitud de un-byte. Una especificación de longitud de encripción cero asociada con cualquier cifrado denota la opción de no encripción; un intercambio de llaves es realizado solamente para compartir las llaves para el cómputo de MAC. La longitud de la llave MAC debe ser por lo menos de 64 bits.

El campo CLEAR_KEY_DATA sólo se usa que cuando las llaves de encripción de longitud es menor que la longitud estándar especificada por el cifrado usado, de otra manera, el campo está vacío. Cuando la longitud de una llave especificada es menos que la longitud estándar de la llave para el cifrado especificado, entonces las llaves de longitud especificada normalmente se derivan como se describió anteriormente, y entonces se "expande" para derivar las llaves de longitud estándar. La expansión procede como sigue:

1. Asigna el resultado de dividir la longitud estándar de la llave por el cifrado, en bits, por la longitud de salida de la función hash, en bits, redondeando al entero más cercano.
2. Divide CLEAR_KEY_DATA secuencialmente en d subsegmentos iguales. (Nota que la longitud del campo CLEAR_KEY_DATA debe ser por consiguiente un múltiplo de d bytes, y que ninguno de los dos iguala d partes, cuando es dividido, puede ser idéntico) Denote estos subsegmentos CLEAR_KEY_DATA_1 a través de CLEAR_KEY_DATA_d.

3. Computa los valores hash.

```
STANDARD_LENGTH_KEY_i :  Hash( i, "s1"^i, WRITE_KEY, "s1"^i,
CLEAR_KEY_DATA_i ).
```

Donde x"^i denota i copias de i de la cadena concatenada "x".

4. Concatenta los STANDARD_LENGTH_KEY_1 a través de STANDARD_LENGTH_KEY_d, y entonces los trunca como sea necesario(removiendo bits del final) para producir STANDARD_LENGTH_KEY que actualmente es usado para encripción.

El campo de KEY_ARG_DATA contiene un valor de 8 bytes aleatorios usados como un vector de inicialización (IV) para el primer mensaje encriptado cuando un cifrado de bloque (excepto con RC4) es usado. El IV para los primeros bloques encriptados en cualquier mensaje subsecuente encriptado, es simplemente el último bloque encriptado para el mensaje anterior. El campo KEY_ARG_DATA está vacío cuando el tipo de cifrado PCT_CIPHER_RC4 (o PCT_EXCH_RSA_PKCS1_TOKEN_RC4) es usado.

PCT_CIPHER_DES denota DES. La longitud de su llave estándar es de 56 bits. PCT_CIPHER_DES_112 y PCT_CIPHER_DES_168 denotan cifrados en los que la entrada es primero encriptada bajo DES con una primera llave, entonces decriptada bajo DES una segunda llave, y finalmente encriptada bajo DES una tercera llave. Para PCT_CIPHER_DES_112, la primera y tercera llave son la misma, y corresponde a los 56 bits iniciales de los 112bits de WRITE_KEY. La segunda llave corresponde a los 56 bits finales de WRITE_KEY. Para PCT_CIPHER_DES_168, las tres llaves son distintas, y corresponden al primero, al segundo, y al tercer subsegmento de 56-bits de WRITE_KEY. Los tres tipos de cifrados basados en DES tienen bloques de datos de 64-bits y se usa con el modo CBC.

Las longitudes estándar de las llaves para PCT_CIPHER_DES_112 y PCT_CIPHER_DES_168 son de 112 y 168 bits, respectivamente. Si se especifica una longitud de llave menor de la longitud estándar por uno de estos cifrados (o PCT_CIPHER_DES), entonces se extiende la longitud estándar de WRITE_KEY.

Note que antes de usar, cada llave de 56-bits de DES debe estar ajustada para agregar ocho bits de paridad para formar una llave DES de ocho bytes DES. Si la longitud de WRITE_KEY especificada es menor de su longitud estándar correspondiente, entonces cada WRITE_KEY se extiende a la longitud normal usando CLEAR_KEY_DATA, para producir una, dos, o tres llaves de 56 bits cada una, las cuales son ajustadas para agregar bits de paridad para formar una llave de ocho bytes.

PCT_CIPHER_IDEA denota el cifrado de bloques IDEA, con bloques de 64 bits de datos y CBC. Este cifrado tiene una longitud de llave estándar de 128 bits.

PCT_CIPHER_RC2 denotan el cifrado de bloque RC2, con bloques de 64 bits y CBC. Como IDEA este cifrado tiene una longitud de llave estándar de 128 bits.

PCT_CIPHER_RC4 denotan el cifrado de flujo RC4. Como los cifrados IDEA y RC2, este cifrado tiene una longitud de llave estándar de 128 bits.

Tipos de Funciones Hash

```
PCT_HASH_MD5
PCT_HASH_MD5_TRUNC_64
PCT_HASH_SHA
PCT_HASH_SHA_TRUNC_80
PCT_HASH_DES_DM
```

PCT_CIPHER_MD5 denota la función hash MD5, con 128-bit de salida.
PCT_CIPHER_MD5_TRUNC_64 denota la función hash MD5, con 128-bit de salida truncada a 64 bits.
PCT_HASH_SHA denota el Algoritmo Hash Seguro (SHA), con 160 bits de salida.
PCT_HASH_SHA_TRUNC_80 denota el Algoritmo Hash Seguro (SHA), con 160 bits de salida truncado a 80 bits.
PCT_HASH_DES_DM denota el algoritmo hash DES-basado en los Davies-Meyer, con 64 bits de salida.

Tipos de Certificados

```
PCT_CERT_NONE
PCT_CERT_X509
PCT_CERT_PKCS7
```

Estos tipos aplican igualmente a los certificados del cliente y servidor. PCT_CERT_NONE denota que ningún certificado es necesario; este tipo puede ser incluido por, el servidor como una opción, haciendo autenticación opcional por el cliente. PCT_CERT_X509 denota un certificado con formato estándar CCITT X PCT_CERT_PKCS7 denota un certificado con formato estándar RSA PKCS#7.

Tipos de Firmas

```
PCT_SIG_NONE
PCT_SIG_RSA_MD5
PCT_SIG_RSA_SHA
PCT_SIG_DSA_SHA
```

PCT_SIG_NONE denota que ninguna firma es necesaria; este tipo puede ser incluido por el servidor como una opción y puede hacerse autenticación opcional para el cliente. PCT_SIG_RSA_MD5 denota el esquema de firma que consiste en aplicar una función hash a los datos a ser firmados usando MD5, y realizando una firma con la llave privada de RSA en el resultado. La firma debe con un tipo de bloque 1 RSA PKCS#1. PCT_SIG_RSA_SHA, denota el mismo esquema de firma con SHA sustituyendo MD5. PCT_SIG_DSA_SHA denota el esquema de firma que consiste en aplicar un hash a los datos para ser firmados con el algoritmo SHA y computa una firma del valor resultante usando el Algoritmo de Firma Digital (DSA).

Errores

El manejo de errores en el protocolo PCT es simple. Cuando un error es detectado durante la fase de saludo, la parte que lo detecta envía un mensaje a la otra parte indicando el error, así que ambas partes lo conocen, y entonces se cierra la conexión. Si una parte detecta un error después éste lo tiene que enviar en el último mensaje del saludo, la parte detectora simplemente cierra la conexión sin enviar un mensaje de error. En el segundo caso sólo hay dos posibles errores, y la parte que no detecta el error puede distinguirlos como sigue: si el servidor ve su conexión abortada y el mensaje más reciente enviado al cliente fue el mensaje de saludo, entonces el error fue SERVER_AUTH_FAILED; de otra manera, el error era INTEGRITY_CHECK_FAILED.

Recibiendo un mensaje de error causa que la parte receptora cierre la conexión. Los servidores y clientes no deben hacer uso extenso de cualquier llave, los challenges, identificadores de conexión, o identificadores de la sesión asociadas con la conexión abortada.

Se recomienda que las aplicaciones ejecuten algún tipo de alarma o función logging cuando se generen errores para facilitar la supervisión de varios tipos de ataque en el sistema

El mensaje enviado en caso de un error del saludo tiene la forma siguiente:

```
MSG_ERROR
ERROR_CODE_MSB
ERROR_CODE_LSB
ERROR_INFO_LENGTH_MSB
ERROR_INFO_LENGTH_LSB
ERROR_INFO_DATA[MSB<<8|LSB]
```

El campo ERROR_INFO_LENGTH es cero excepto en el caso del mensaje de error SPECS_MISMATCH que tiene un campo de seis bytes ERROR_INFO_DATA.

El protocolo de saludo define los siguientes errores:

PCT_ERR_BAD_CERTIFICATE: Este error ocurre cuando el cliente recibe un mensaje SERVER_HELLO en el que el certificado es inválido, o porque una o más de las firmas en el certificado es inválida, o porque la identidad o atributos en el certificado están de alguna manera incorrectos.

PCT_ERR_CLIENT_AUTH_FAILED: Este error ocurre cuando el servidor recibe un mensaje CLIENT_MASTER_KEY del cliente en el que la respuesta de la autenticación del cliente es incorrecta. El certificado puede ser inválido, la firma puede ser inválida, o los contenidos de la respuesta firmada pueden ser incorrectos.

PCT_ERR_ILLEGAL_MESSAGE: Este error ocurre bajo un cierto número de circunstancias. Por ejemplo, ocurre cuando un código escape de seguridad no reconocido se recibe, cuando un mensaje de saludo no reconocido se encuentra, o cuando el valor CH_OFFSET es más grande para su mensaje CLIENT_HELLO.

PCT_ERR_INTEGRITY_CHECK_FAILED: Este error ocurre cuando el cliente o el servidor reciben un mensaje en el que el MAC_DATA es incorrecto. También se recomienda que el registro se trate como sino tuviera ningún dato, para asegurar que las aplicaciones no reciben y procesan datos inválidos antes de aprender que ha fallado su verificación de integridad. También ocurre cuando el valor de VERIFY_PRELUDE_DATA enviado por el cliente en el mensaje CLIENT_MASTER_KEY (durante el saludo) es incorrecto. En este caso, un mensaje de error se envía.

PCT_ERR_SERVER_AUTH_FAILED: Este error ocurre cuando el cliente recibe un mensaje SERVER_HELLO o SERVER_VERIFY en los que la respuesta de la autenticación es incorrecta.

PCT_ERR_SPECS_MISMATCH: Este error ocurre cuando un servidor no puede encontrar en un cifrado, una función hash, un tipo de certificado, o el algoritmo de intercambio de llaves que se proveen en las listas proporcionadas por el cliente en el mensaje CLIENT_HELLO. También ocurre cuando el cliente no puede encontrar un certificado o tipo de firma que este en la lista proporcionada por el servidor en un mensaje SERVER_HELLO que solicite la autenticación del cliente. Este error también puede ocurrir como resultado de un error en las especificaciones del cifrado o de la autenticación del cliente solicitada, entre las especificaciones iniciales y el resultado desde una secuencia redo handshake.

El mensaje de error para este error incluye un campo informativo de seis bytes de la siguiente manera:

```
SPECS_MISMATCH_CIPHER
SPECS_MISMATCH_HASH
SPECS_MISMATCH_CERT
SPECS_MISMATCH_EXCH
SPECS_MISMATCH_CLIENT_CERT
SPECS_MISMATCH_CLIENT_SIG
```

A cada campo se pone a un valor no cero si y sólo si la lista correspondiente produjera una desigualdad.

4.2 De la Capa de Transacción

Estos protocolos actúan como un mecanismo para permitir al cliente en Internet contactar a un vendedor en Internet y asegurar la compra de los bienes o servicios usando un existente proceso de tarjeta de crédito.

La operación de este tipo de protocolos consiste en que el cliente contacte al vendedor y le pida ver sus certificados. Una vez que el cliente vea los certificados del vendedor firmados por un banco adquirente, una organización de tarjetas de crédito o una autoridad certificadora, entonces es como él enviará la información de su compra junto con la del pago (certificados del cliente). El vendedor entonces verifica la orden de compra y los certificados del cliente, le envía la información del pago a un gateway que envía la información a la red de procesamiento de pagos. Entonces ejecuta la operación de autorización o captura (pago) dependiendo del protocolo existente.

4.2.1 iKP IBM

Este protocolo fue analizado anteriormente como un esquema de pago electrónico con tarjeta de crédito o como micropago. IKP es una familia de protocolos que es la base para casi todos los protocolos de tarjetas de crédito usados en Internet , permite un incremento en el nivel de autenticidad y seguridad para ser desplegado como infraestructura de llave pública.

4.2.2 NSC Netscape

Netscape propone el Mensajero seguro (Secure Courier) en 1995, como el primer protocolo de plataforma abierta para crear un sobre digital seguro para datos financieros en Internet. Intuir Inc. y MasterCard International anunciaron que soportaran el nuevo protocolo para la seguridad de la tarjeta de crédito online, tarjeta de débito, tarjeta de cargo y transacciones micro financieras.

NSC es un protocolo de transacción asombroso similar a iKP, tiene algunas diferencias de implementación, una de las cuales es que su funcionalidad criptográfica en el nivel de protocolo de transacción no es usada desde que el protocolo se asume que corra sobre SSL. Netscape esperaba liberar el desarrollo de una infraestructura naciente de llave pública pero ha resultado sin éxito de una ausencia en el crecimiento de la infraestructura de llave pública

4.2.3 STT Microsoft

En el verano de 1995 MasterCard y Visa había hablado de la producción en conjunto de una especificación para transacciones con tarjeta de crédito sobre la red Tecnología de Transacciones Seguras (STT/Secure Transaction Technology). El protocolo es muy similar a iKP por lo que se refiere a aspectos técnicos de los protocolos de transacción

4.2.4 SEPP Mastercard

A menos de una semana del anuncio de STT, fue liberada la especificación SEPP por MasterCard, IBM, Netscape, gte, y CyberCash. Este protocolo es parecido al protocolo iKP, y es similar a STT. La similitud puede ser el resultado de dos factores.

1. La involucración con IBM, diseño el protocolo iKP en el cual se basa este protocolo,
2. MasterCard y Visa desarrollaron el protocolo de retiro.

Este protocolo ya fue descrito anteriormente en la parte de sistemas de pago con tarjeta de crédito

Marco Metodológico

IV. MARCO METODOLÓGICO

1. VARIABLES

Independientes:

- Mal establecimiento del procedimiento de compraventa.
- Mala implantación de seguridad en los sistemas de pago digital.
- Incertidumbre al no saber cómo funcionan los sistemas de pago y el comercio electrónico en general.

Dependientes:

- Pérdida de la mercancía.
- Produce desconfianza al cliente en el sistema de pago.
- Fraudes en el comercio electrónico.
- No permite el uso frecuente del comercio electrónico.

Cuya relación detallo en el inciso relativo a la hipótesis.

2. VARIABLES DE CONTROL

Debido a que mi tema de investigación abarca un rango de la población difícilmente definible, no he considerado necesaria la inclusión de variables de control.

3. HIPÓTESIS DEFINITIVA

Al haber realizado el Marco Teórico y el Marco Conceptual, la definición de la hipótesis fue mal redactada en el Marco Problemático, también observe que hay un punto que ya no se está considerando dentro del rango de los efectos de mi hipótesis, y aquí mejorare el nuevo planteamiento de la hipótesis. Uno de los motivos para realizar ésta modificación fue que muchas de las ocasiones los sistemas de pago electrónicos proporcionan mayor seguridad dependiendo la manera en la que se implanten, pero no sólo éste es un factor que influye, existe también la problemática de cómo se haya implantado la red, si los dispositivos fueron instalados adecuadamente previniendo contra ataques externos, y algo importante que no es tomado muy en cuenta es la manera en la que se implantan los procedimientos de cada tienda virtual.

Otro punto que a lo largo de mi investigación fue un efecto a las causas que determine en la hipótesis preliminar, y que se da por, el mal establecimiento del procedimiento de compraventa, de los malos sistemas de seguridad en los sistemas de pago digital, fraudes, incertidumbre al desconocimiento del funcionamiento de los sistemas de pago y al e-commerce en general y la desconfianza que produce al usuario el pensar que su información no viaja por un canal seguro, éste es él de no permitir el crecimiento del comercio electrónico, cosa que al final de las encuestas realizadas y en general de toda la investigación, pude notar que aunque todavía existan una serie de factores por los cuales no se recurre mucho a Internet como un medio de compra, este crecimiento no se detiene, ya que debido a la economía mundial, éste empieza a formar parte de la estructura de dar a conocer los servicios y productos de un negocio en la actualidad, quien no incursione en este tipo de comercio se irá quedando obsoleto. Este punto en la hipótesis definitiva fue suplantado por algo que considere al final de la investigación importante mencionarlo, como un efecto a los problemas que se dan por la inseguridad en las transacciones del comercio electrónico el no permitir el uso frecuente del comercio electrónico. Aunque sea un hecho que el e-commerce no dejará de crecer en un tiempo aún no se hace un uso

constante del mismo, por lo que en mi hipótesis hago referencia a un nuevo efecto de las causas previamente mencionadas y es "No permite el uso frecuente del e-commerce".

Hipótesis Preeliminar

Causa: Mal establecimiento del procedimiento de compraventa.
Efecto: Pérdida de la mercancía.
Produce desconfianza al cliente en el sistema de pago
Fraudes en el comercio electrónico.
No permite el crecimiento del comercio electrónico.

Causa: Malos sistemas de seguridad en los sistemas de pago digital
Efecto: Fraudes en el comercio electrónico.
Produce desconfianza a los usuarios.
No permite el crecimiento del comercio electrónico

Causa: Fraudes en el comercio electrónico.
Efecto: Produce desconfianza a los usuarios.
No permite el crecimiento del comercio electrónico

Causa: Incertidumbre al no saber cómo funcionan los sistemas de pago y el comercio electrónico en general.
Efecto No permite el crecimiento del comercio electrónico

Causa: Falta de confianza de que la información de pago esté viajando por un canal seguro.
Efecto: No permite el crecimiento del comercio electrónico

De las diversas relaciones hipotéticas que anteceden he hecho una selección conceptual que dan origen a la que enseguida se presenta, y es la que determino como mi hipótesis definitiva.

"Es frecuente que haya desconfianza e incertidumbre de las personas a realizar una compra en Internet, principalmente en la segundad del medio por el cual se realiza el pago, en que la mercancía solicitada no llegue a su destino final y que se produzcan fraudes, dando lugar a que no se pueda dar crecimiento en el e-commerce".

Hipótesis Definitiva

Causa: Mal establecimiento del procedimiento de compraventa
Efecto: Pérdida de la mercancía.
Produce desconfianza al cliente en el sistema de pago
Fraudes en el comercio electrónico.
No permite el uso frecuente del comercio electrónico.

Causa: Mala implementación de los sistemas de seguridad en los sistemas de pago digital
Efecto: Fraudes en el comercio electrónico.
Produce desconfianza a los usuarios
No permite el uso frecuente del comercio electrónico

Causa Fraudes en el comercio electrónico.
Efecto: Produce desconfianza a los usuarios.
No permite el uso frecuente del comercio electrónico

Causa: Incertidumbre al no saber cómo funcionan los sistemas de pago y el comercio electrónico en general.
Efecto: No permite el uso frecuente del comercio electrónico

Causa: Falta de confianza de que la información de pago esté viajando por un canal seguro.
Efecto: No permite el uso frecuente del comercio electrónico

De las diversas relaciones hipotéticas que anteceden he hecho una selección conceptual que dan origen a la que enseguida se presenta, y es la que determino como mi hipótesis definitiva.

"Es frecuente que haya desconfianza e incertidumbre de las personas a realizar una compra en Internet, principalmente en la seguridad del medio por el cual se realiza el pago, en que la mercancía solicitada no llegue a su destino final y que se produzcan fraudes, dando lugar al uso moderado de Internet para realizar transacciones de e-commerce."

4. DEFINICIÓN DEL UNIVERSO

El universo en este trabajo es muy complejo y difícil de precisar. Como este trabajo de investigación no va enfocado a hacer pruebas plenas, simplemente se emitirán opiniones aceptables como calificadas que señalen que la hipótesis es válida.

5. DEFINICIÓN DE LA MUESTRA

Aplicaré lo que es una muestra no probabilística denominada de juicio o intencionada, ya que sólo emitiré una opinión en base a los conocimientos adquiridos en este trabajo y ayudado por medio de un cuestionario, aplicado a algunas personas que tengan el conocimiento sobre el tema en empresas del ramo, como muestra significativa.

Daré una breve descripción de los tipos de muestras:

Muestra: Conjunto finito que separamos de un colectivo, entendiéndose por colectivo, población o universo al conjunto del cual se han extraído los números o atributos que forman la serie estadística. En otras palabras, colectivo sería la totalidad de valores posibles de una característica particular de un grupo especificado de objetos al cual se le llama universo.

Muestra probabilística:

Muestra extraída de una población, de tal forma que cada elemento tiene una probabilidad conocida de estar incluido en la muestra.

Entre los métodos de muestreo probabilísticos más utilizados en investigación encontramos:

- Muestra aleatoria simple: Una muestra de tamaño n, extraída de una población de tamaño N, si cada muestra posible de tamaño n tiene la misma probabilidad de ser seleccionada
- Muestra aleatoria estratificada o de Poisson: Cuando la población objeto de estudio se puede dividir en distintas categorías, clases o estratos o, en otras palabras, subpoblaciones, conservando alguna característica homogénea de los elementos que la componen, resulta bastante útil emplear este método, en primer lugar se clasifican los elementos poblacionales en función de alguna característica (subdivisión) de tipo cualitativo o cuantitativo, cada una de las cuales recibe el nombre de estrato; la utilización del método aleatorio simple a cada uno de estos estratos completa el método.

- Muestra aleatoria por conglomerados y áreas o polietápico: Por este método lo que se elige al azar no son unos cuantos elementos sino subgrupos de la población previamente formados. Elegidos estos grupos o conglomerados en un número suficiente, se pasa posteriormente a la elección también al azar de los elementos que se han de observar dentro de cada conglomerado, o bien, según se desee la observación completa de todos los elementos que componen los conglomerados elegidos.

- Muestra sistemática o controlada: Este procedimiento exige, numerar todos los elementos de la población, pero en lugar de extraer n números aleatorios sólo se extrae uno. Se parte de ese número aleatorio i, que es un número elegido al azar, y los elementos que integran la muestra son los que ocupan los lugares i, i+k, i+2k, i+3k,...,i+(n-1)k, es decir se toman los individuos de k en k, siendo k el resultado de dividir el tamaño de la población entre el tamaño de la muestra: k=N/n. El número i que empleamos como punto de partida será un número al azar entre 1 y k.

Muestra no probabilística:

Es el elemento o cada miembro de la población que tiene las mismas probabilidades de ser elegido o de pertenecer a la muestra. Los métodos de muestreo no probabilístico, no garantizan la representatividad de la muestra y por lo tanto no permiten realizar estimaciones inferenciales sobre la población.

- Muestra por cuotas o accidental: se divide a la población en estratos o categorías, y se asigna una cuota para las diferentes categorías y, a juicio del investigador, se selecciona las unidades de muestra. La muestra debe ser proporcional a la población, y en ella deberán tenerse en cuenta las diferentes categorías. La muestra por cuotas se presta a distorsiones, al quedar a criterio del investigador la selección de las categorías.

- Muestra intencionada: también recibe el nombre de sesgada. El investigador selecciona los elementos que a su juicio son representativos, lo que exige un conocimiento previo de la población que se investiga.

- Muestra mixta: se combinan diversos tipos de muestra. Por ejemplo: se pueden seleccionar las unidades de la muestra en forma aleatoria y después aplicar la muestra por cuotas.

- Muestra tipo: la muestra tipo (master simple) es una aplicación combinada y especial de los tipos de muestra existentes. Consiste en seleccionar una muestra "para ser usada" al disponer de tiempo, la muestra se establece empleando procedimientos sofisticados, y una vez establecida, constituirá el módulo general del cual se extraerá la muestra definitiva conforme a la necesidad específica de cada investigación.

- Muestra casual o incidental: Se trata de un proceso en el que el investigador selecciona directa e intencionadamente los individuos de la población. El caso más frecuente de este procedimiento el utilizar como muestra los individuos a los que se tiene fácil acceso (los profesores de universidad emplean con mucha frecuencia a sus propios alumnos). Un caso particular es el de los voluntanos.

- Bola de nieve: Se localiza a algunos individuos, los cuales conducen a otros, y éstos a otros, y así hasta conseguir una muestra suficiente. Este tipo se emplea muy frecuentemente cuando se hacen estudios con poblaciones "marginales", delincuentes, sectas, determinados tipos de enfermos, etc.

6. DEFINICIÓN DEL MÉTODO DE LA INVESTIGACIÓN

El método de investigación seleccionado para la aprobación y comprobación de la hipótesis fue por medio de la aplicación de encuestas. Los resultados de las encuestas aplicadas me ayudarán a analizar la visión, conocimientos y puntos de vista de las personas profesionales en el tema de e-commerce con respecto a la seguridad en los sistemas de pago electrónico en el e-commerce.

7. COSTO DE LA INVESTIGACIÒN

DESCRIPCIÓN	EROGACIÓN	TOTALES
Recursos Humanos		
Investigador	$ 80,000.00	
Total de Recursos Humanos		$ 80,000.00
Equipo de Procesamiento de Datos		
Computadora	$ 8,000.00	
Impresora	$ 3,000.00	
Scanner	$ 3,000.00	
Total de Equipo de Procesamiento de Datos		$ 14,000.00
Software		
Windows 98	$ 1,000.00	
Office 97	$ 900.00	
Power Translator 6.0	$ 500.00	
Antivirus	$ 400.00	
Software del Scanner	$ 400.00	
Total de Software		$ 3,200.00
Accesorios		
Disquete	$ 300.00	
Cartuchos de Impresora	$ 900.00	
Papel (hojas carta)	$ 1,000.00	
Accesorios de Papelería	$ 400.00	
Total de Accesorios		$ 2,600.00
Material de Consulta		
Electronic Payment System	$ 630.00	
E-commerce Security	$ 240.00	
SET	$ 500.00	
Stalling	$ 400.00	
Otros	$ 2,000.00	
Revistas y Copias	$ 1,500.00	
Internet	$ 1,600.00	
Total de Software		$ 7,870.00
Area de Trabajo y Acondicionamiento		
Renta del Local	$ 16,000.00	
Suministro Eléctrico	$ 1,200.00	
Teléfono	$ 1,200.00	
Total del Área de Trabajo y Acondicionamiento		$ 18,400.00
TOTAL DE GASTOS		**$ 126,170.00**

8. CUESTIONARIO

8.1 Construcción del Cuestionario

PREGUNTA	RAZÓN DE SER	RESPUESTA
1. ¿Cuáles son los pasos esenciales para una compra en Internet?	Comprobar si los procedimientos establecidos se siguen de la misma manera, y ver si alguno de ellos proporciona algún punto que ofrezca seguridad, con relación a los otros.	Respuesta cuadro de abajo

- Respuesta esperada

1. Ingresa a Internet.	Comprador	1. Ingresa a Internet. 2. Escribe la dirección de la ubicación de la tienda virtual
2. Selecciona del artículo a adquirir.	Comprador	1. Entra a la tienda virtual 2. Busca el artículo a adquirir 3. Selecciona el artículo 4. Agrega el artículo al carrito de compras dando un click en el carrito o en el botón de agregar la compra. 5. Muestra el artículo seleccionado
3 Solicita dirección e-mail para el alta del cliente.	Comerciante (automático)	1 Se va al botón de nuevo. 2. Pide dirección e-mail.
4. Ingresa dirección e-mail el cliente.	Comprador	1. Ingresa dirección e-mail.
5. Ingreso de datos por el cliente.	Comprador	1. Ingresa nombre, apellidos, dirección y teléfono en el formulario.
6. Verifica que todos los datos hayan sido ingresados.	Comerciante (automático)	1. Checa que los campos tengan datos. 2 Muestra los datos ingresados.
7. Elección de la dirección.	Comprador	1. Tiene que elegir la dirección a la cual se enviará el producto.
8 Muestra datos del cliente y del artículo.	Comerciante (automático)	1. Despliega información del artículo a adquirir y los datos de la dirección de envío.
9 Asigna la cantidad de artículos.	Comprador	1 Asigna una cantidad de compra
10. Señala las formas de envio	Comerciante (automático)	1. Da las diferentes formas de envio y una breve descripción (Nacional/Internacional)
11. Elección de forma de envio	Comprador	1. Elige la opción más adecuada conforme a sus necesidades.

12. Indica las formas de pago.	Comerciante (automático)	1. Pide password y su confirmación. 2. Menciona los procesos de pago.
13. Selección de un método de pago.	Comprador	1. Ingresa password y confirmación. 2. Selecciona el método de pago. 3. Ingresa los datos que se requieren por la forma de pago elegida.
14. Corroboración de datos.	Comerciante (automático)	1. Checa que los datos ingresados sean reales conforme al método de pago elegido.
15. Muestra la orden de compra.	Comerciante (automático)	1. Despliega la información total de la compra. 2. Acepta la compra
16. Aceptación de la orden.	Comerciante (automático)	1. Informa que la orden está lista. 2. Envía un mensaje, para informar el número de la orden.
17. Envío del producto	Comerciante (automático)	1. Checa el depósito de pago 2. Envía el producto.
18. Recepción del producto	Comprador	1. Recibe el producto.

PREGUNTA	RAZÓN DE SER	RESPUESTA
2. ¿Cuáles son los Sistemas de pago electrónicos que ha utilizado?	Esta pregunta se hace con el fin de obtener respuesta de los sistemas de pago que más se han utilizado.	SET, uso de los protocolos SSL, SHTTP, Ecash, Millicent, Mondex, CyberCash.
3. ¿Cuáles son los sistemas de pago que usted cree se usan más comúnmente?	Ver cuáles son los sistemas de uso más común en Internet para así poder determinar, en qué sistemas el usuario confía más, al igual de saber cuáles son los que más comúnmente se aplican en los sitios de comercio electrónico.	Los sistemas de pago más usuales para compradores y vendedores son los relacionados con tarjeta de crédito.
4. ¿Por qué considera que estos sistemas sean los más usados?	Verificar qué es lo que tomó en cuenta, para utilizar estos sistemas de pago.	Debido a que proporciona mayor grado de seguridad y es el sistema más común por el cual la gente adquiere sus productos, desde una compra por medio del teléfono, en los centros comerciales y ahora por Internet.

PREGUNTA	RAZÓN DE SER	RESPUESTA
5. Al momento de elegir un sistema de pago para un sitio de comercio electrónico, ¿En qué se piensa?	Ver cuáles son las razones para elegir un sistema de pago, dependiendo la tienda virtual que se coloque en Internet.	1. Se define el o los artículos que se van a vender. 2. Se elige un sistema de pago dependiendo el artículo a vender acorde con el costo del mismo.
6. ¿La seguridad de una compra en Internet radica en que el sistema de pago sea seguro?	Corroborar si la mayoría de las empresas tienen conocimiento que no sólo la seguridad radica en el sistema de pago, sino que se deben checar más aspectos como la instalación del hardware, software y el establecimiento de buenos procedimientos.	No.
7. ¿Qué aspectos debemos verificar, para proporcionar seguridad en la transacción de compra?	Definir los aspectos que se cuidan principalmente en la seguridad de la transacción de compra	1. La seguridad en la instalación del hardware en el que se encuentra el servidor. 2. La correcta implantación del sistema de pago. 3. Verificar que los procedimientos que se siguen en la transacción de compraventa, proporcionen la seguridad de la entrega del producto al cliente.
8. ¿Es común el uso de los sistemas de pago en los sitios de comercio electrónico en México?	Evaluar cuánto es el uso de los sistemas de pago, y comprobar si el uso se reduce a uno de los sistemas (Pago con tarjeta de crédito).	Actualmente en México la mayoría de los sitios de comercio electrónico no están muy familiarizados con el uso de los sistemas de pago, por lo que recurren a hacer la compra por medio de una llamada telefónica, dando su número de tarjeta, aún el pago no se realiza vía Internet.
9. ¿Existen requerimientos para dar de alta un sitio de comercio electrónico en México?	Obtener información para observar si el poco uso de los sistemas de pago, se debe a que las empresas necesitan cubrir ciertos requerimientos para establecer el sistema de pago.	Si existen diversos organismos como VeriSign que regulan el uso de sistemas de pago con tarjeta de crédito. Poder abstraer otros.
10. ¿Cuáles son los problemas de seguridad que comúnmente se encuentran?	Mostrar que los problemas tienen que ver con la definición de la hipótesis final.	1. Falta de conocimientos en los diversos sistemas de pago y en su implementación. 2. Mal diseño de la tienda virtual. 3. Mala implantación de la seguridad en el equipo en el

		cual se encuentra la tienda. 4. Mal establecimiento de los procedimientos de entrega del producto.
11 ¿Cuáles son los problemas que produce la inseguridad de las transacciones?	Verificar si nuestras variables dependientes son las correctas.	1. No llega la mercancía a su destino. 2. Se cometen fraudes. 3. Desconfianza en las personas. 4. Incertidumbre al no saber de la existencia de los sistemas de pago. 5. No permite el crecimiento del e-commerce.

8.2 Cuestionario Piloto

1. ¿Cuáles son los pasos esenciales para una compra en Internet?

1. Ingresa a Internet. ( )
2. Selecciona del artículo a adquirir. ( )
3. Solicita dirección e-mail para el alta del cliente. ( )
4. Ingresa dirección e-mail el cliente. ( )
5. Ingreso de datos por el cliente. ( )
6. Verifica que todos los datos hayan sido ingresados. ( )
7. Elección de la dirección. ( )
8. Muestra datos del cliente y del artículo. ( )
9. Asigna la cantidad de artículos. ( )
10. Señala las formas de envío. ( )
11. Elección de forma de envío ( )
12. Indica las formas de pago. ( )
13. Selección de un método de pago. ( )
14. Corroboración de datos. ( )
15. Muestra la orden de compra. ( )
16. Aceptación de la orden. ( )
17. Envío del producto. ( )
18. Recepción del producto ( )

2. ¿Cuáles son los sistemas de pago electrónicos que ha utilizado?

FirstVirtual	( )	FSTC	( )	Ecash	( )	Millicent	( )
CARI	( )	NetBill	( )	CAFÉ	( )	SubScrip	( )
IKP	( )	NetCheque	( )	Netcash	( )	PayWord	( )
SEPP	( )			Cybercoin	( )	IKP	( )
SET	( )			Mondex	( )	MicroMint	( )
				EMV Cash Cards	( )		

3. ¿Cuáles son los sistemas de pago que usted cree se usa más comúnmente?

FirstVirtual	( )	FSTC	( )	Ecash	( )	Millicent	( )
CARI	( )	NetBill	( )	CAFÉ	( )	SubScrip	( )
IKP	( )	NetCheque	( )	Netcash	( )	PayWord	( )
SEPP	( )			Cybercoin	( )	IKP	( )
SET	( )			Mondex	( )	MicroMint	( )
				EMV Cash Cards	( )		

4. ¿Por qué considera que estos sistemas sean los más usado?

Por seguro ( )
Por ser el más popular ( )
Depende de la tienda en la que se compre ( )
( )
( )

5. **Al momento de elegir un sistema de pago para en un sitio de comercio electrónico, ¿En qué se piensa?**

6. **¿La seguridad de una compra en Internet radica en que el sistema de pago sea seguro?**

SI **NO**

¿Por qué?

7. **¿Qué aspectos debemos verificar, para proporcionar seguridad en la transacción de compra?**

Conocimiento de la tienda virtual. ( )
La implantación del sistema de pago ( )
Buena elección del sistema de pago. ( )
Implantación de la seguridad del hardware y del SO. ( )
Uso de técnicas criptográficas. ( )
Buen establecimiento del procedimiento de compraventa. ( )
Buen diseño del establecimiento de la tienda virtual. ( )

8. **¿Es común el uso de los sistemas de pago en los sitios de comercio electrónico en México?**

SI **NO**

¿Por qué?

9. **¿Existen requerimientos para dar de alta un sistema de pago electrónico en un sitio de e-commerce en México?**

SI **NO**

¿Cuáles?

10. **¿Cuáles son los problemas de seguridad que comúnmente se encuentran?**

Falta de conocimientos en los diversos sistemas de pago y en su implementación. ( )
Mal diseño de la tienda virtual. ( )
Mala implantación de la seguridad en el equipo en el cual se encuentra la tienda. ( )
Mal establecimiento de los procedimientos de entrega del producto ( )

11. ¿Cuáles son los problemas que produce la inseguridad de las transacciones?

No llega la mercancía a su destino. ( )
Se cometen fraudes. ( )
Desconfianza en las personas. ( )
Incertidumbre al no saber de la existencia de los sistemas de pago. ( )
No permite el crecimiento del e-commerce. ( )

8.3 Cuestionario Definitivo

1. ¿Cuáles son los pasos esenciales para una compra en Internet?

1. Ingresa a Internet. ( )
2. Selecciona del artículo a adquirir. ( )
3. Solicita dirección e-mail para el alta del cliente. ( )
4. Ingresa dirección e-mail el cliente. ( )
5. Ingreso de datos del cliente. ( )
6. Verifica que todos los datos hayan sido ingresados. ( )
7. Elección de la dirección de entrega. ( )
8. Muestra datos del cliente y del artículo. ( )
9. Asigna la cantidad de artículos. ( )
10. Señala las formas de envío. ( )
11. Elección de forma de envío ( )
12. Indica las formas de pago ( )
13. Selección de un método de pago ( )
14. Corroboración de datos. ( )
15. Muestra la orden de compra ( )
16. Aceptación de la orden ( )
17. Envio del producto. ( )
18. Recepción del producto ( )

2. ¿Cuáles son los sistemas de pago electrónicos que ha utilizado?

FirstVirtual	( )	FSTC	( )	Ecash	( )	Millicent	( )
CARI	( )	NetBill	( )	CAFÉ	( )	SubScrip	( )
IKP	( )	NetCheque	( )	Netcash	( )	PayWord	( )
SEPP	( )			Cybercoin	( )	IKP	( )
SET	( )			Mondex	( )	MicroMint	( )
				EMV Cash Cards	( )		

Otros: _____

3. ¿Cuáles son los sistemas de pago que usted cree se usa más comúnmente?

FirstVirtual	( )	FSTC	( )	Ecash	( )	Millicent	( )
CARI	( )	NetBill	( )	CAFÉ	( )	SubScrip	( )
IKP	( )	NetCheque	( )	Netcash	( )	PayWord	( )
SEPP	( )			Cybercoin	( )	IKP	( )
SET	( )			Mondex	( )	MicroMint	( )
				EMV Cash Cards	( )		

4. ¿Por qué considera que estos sistemas sean los más usado?

Por seguro ( )
Por ser el más popular ( )
Costos ( )
Integración con otros sistemas ( )
( )

5. **Al momento de elegir un sistema de pago para en un sitio de comercio electrónico, ¿En qué se piensa?**

6. **¿La seguridad de una compra en Internet radica en que el sistema de pago sea seguro?**

SI **NO**

¿Por qué?

7. **¿Qué aspectos debemos verificar, para proporcionar seguridad en la transacción de compra?**

Conocimiento de la tienda virtual. ( )
La implantación del sistema de pago. ( )
Buena elección del sistema de pago. ( )
Implantación de la seguridad del hardware y del SO. ( )
Uso de técnicas criptográficas. ( )
Buen establecimiento del procedimiento de compra-venta. ( )
Arquitectura HW/ SW ( )

8. **¿Es común el uso de los sistemas de pago en los sitios de comercio electrónico en México?**

SI **NO**

¿Por qué?

9. **¿Existen requerimientos para dar de alta un sistema de pago electrónico en un sitio de e-commerce en México?**

SI **NO**

¿Cuáles?

10. **¿Cuáles son los problemas de seguridad que comúnmente se encuentran?**

Falta de conocimientos en los diversos sistemas de pago y en su implementación. ( )
Mal diseño de la tienda virtual. ( )
Mala implantación de la seguridad en el equipo en el cual se encuentra la tienda ( )
Mal establecimiento de los procedimientos de entrega del producto. ( )

11. ¿Cuáles son los problemas que produce la inseguridad de las transacciones?

No llega la mercancia a su destino. ( )
Se cometen fraudes. ( )
Desconfianza en las personas. ( )
Incertidumbre al no saber de la existencia de los sistemas de pago. ( )
No permite el crecimiento del e-commerce. ( )

8.4 Realización de la Investigación

Las personas que contribuyeron a la realización de mi investigación son conocedoras de la implantación de una tienda virtual en el e-commerce, por lo tanto los resultados que aquí daré serán una muestra significativa de la hipótesis que quiero demostrar.

Personas Entrevistadas

- Carlos Bladinieres
  OpenTec
- Jesús Angél
  SeguriData
- Saúl Sánchez
  Unisys de México, S.A. de C.V
- Ricardo Rivera Román
  Fleishman & Hillar
- Adriana Ayala Martínez
  Dirección General de Presupuestos de la UNAM
- Patricia Macías

9. Captura y Recopilación de datos

En base al cuestionario aplicado, se obtuvieron los siguientes resultados.

Personas entrevistadas	Saúl Sánchez				Carlos Bladinieres				Adriana Ayala				Aida Covarrubias			
	Sí	No	No Sé	No Ne.	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.
1. ¿Cuáles son los pasos esenciales para una compra en Internet?																
1. Ingresa a Internet	x				x				x				x			
2. Selecciona del artículo a adquirir.	x				x				x				x			
3. Solicita dirección e-mail para el alta del cliente.				x	x				x							
4. Ingresa dirección e-mail el cliente.				x	x				x							
5. Ingreso de datos del cliente.	x				x				x				x			
6. Verifica que todos los datos hayan sido ingresados.	x				x				x				x			
7. Elección de la dirección de entrega.	x				x				x							
8. Muestra datos del cliente y del artículo	x				x				x				x			
9. Asigna la cantidad de artículos	x				x				x							
10. Señala las formas de envío.	x				x				x							
11. Elección de forma de envío	x				x				x				x			
12. Indica las formas de pago.	x				x				x							
13. Selección de un método de pago	x				x				x				x			
14. Corroboración de datos.	x				x				x				x			
15. Muestra la orden de compra.	x				x				x				x			
16. Aceptación de la orden	x				x				x				x			
17. Envío del producto				x	x				x				x			
18 Recepción del producto				x	x				x				x			
2. ¿Cuáles son los sistemas de pago electrónicos que ha utilizado?																
FirstVirtual																
CARI																
IKP																
SEPP																
SET					x				x							
FSTC																
NetBill																
NetCheque																
Ecash																
CAFE																
Netcash																
Cybercoin																
Mondex																
EMV Cash Cards																
Millicent																

Personas entrevistadas	Saúl Sánchez				Carlos Bladinieres				Adriana Ayala				Aída Covarrubias			
	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.
2. ¿Cuáles son los sistemas de pago electrónicos que ha utilizado?																
SubScrip																
PayWord																
IKP																
MicroMint																
Otros:	VPOS														x	
3. ¿Cuáles son los sistemas de pago que usted cree se usa más comúnmente?																
FirstVirtual																
CARI																
IKP																
SEPP																
SET					x				x				x			
FSTC																
NetBill																
NetCheque																
Ecash									x				x			
CAFE																
Netcash																
Cybercoin																
Mondex									x				x			
EMV Cash Cards									x							
Millicent																
SubScrip																
PayWord																
IKP																
MicroMint																
Otros:			x						Banksys							
4. ¿Por qué considera que estos sistemas sean los más usado?																
Por seguro	x								x							
Por ser el más popular					x								x			
Costos					x											
Integración con otros sistemas					x				x							

Personas entrevistadas	Saúl Sánchez				Carlos Bladinieres				Adriana Ayala				Aida Covarrubias			
	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.
5. Al momento de elegir un sistema de pago para en un sitio de comercio electrónico, ¿En qué se piensa?																
Seguridad	x				x				x							
Integración con varias plataformas (Compatibilidad)	x				x											
Costos	x				x											
Desempeño	x								x							
Fácil Manejo					x				x							
Interoperabilidad con la tienda virtual									x							
6. ¿La seguridad de una compra en Internet radica en que el sistema de pago sea seguro?		x			x				x							
¿Por qué?																
Verificar Hardware	x															
Verificar Software	x															
Accesos lógicos y físicos a servidores					x											
Seguridad en las conexiones					x											
Por las intercepciones de información (TC)					x											
7. ¿Qué aspectos debemos verificar, para proporcionar seguridad en la transacción de compra?																
Conocimiento de la tienda virtual.					x				x				x			
La implantación del sistema de pago.	x				x				x				x			
Buena elección del sistema de pago.	x				x				x				x			
Implantación de la seguridad del hardware y del SO	x				x				x							
Uso de técnicas criptográficas.					x				x							
Buen establecimiento del procedimiento de compraventa.					x				x							
Arquitectura HW/ SW	x				x				x							
8. ¿Es común el uso de los sistemas de pago en los sitios de comercio electrónico en México?	x				x					x				x		
9. ¿Existen requerimientos para dar de alta un sistema de pago electrónico en un sitio de e-commerce en México?			x		x										x	
¿Cuáles?																

Personas entrevistadas	Saúl Sánchez				Carlos Bladinieres				Adriana Ayala				Aida Covarrubias			
	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.
10. ¿Cuáles son los problemas de seguridad que comúnmente se encuentran?																
Falta de conocimientos en los diversos sistemas de pago y en su implementación.													x			
Mal diseño de la tienda virtual.																
Mala implantación de la seguridad en el equipo en el cual se encuentra la tienda.	x												x			
Mal establecimiento de los procedimientos de entrega del producto																
11. ¿Cuáles son los problemas que produce la inseguridad de las transacciones?																
No llega la mercancía a su destino					x											
Se cometen fraudes.	x				x				x TC				x			
Desconfianza en las personas	x				x								x			
Incertidumbre al no saber de la existencia de los sistemas de pago					x				x				x			
No permite el crecimiento del e-commerce.													x			

Personas entrevistadas	Patricia Macías				Jesús Ángel				Ricardo Rivera Román			
	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.	Si	No	No Sé	No Ne.
1. ¿Cuáles son los pasos esenciales para una compra en Internet?												
1 Ingresa a Internet.	x				x				x			
2 Selecciona del artículo a adquirir	x				x				x			
3 Solicita dirección e-mail para el alta del cliente	x				x				x			
4 Ingresa dirección e-mail el cliente	x				x				x			
5 Ingreso de datos del cliente.	x				x				x			
6 Verifica que todos los datos hayan sido ingresados.	x				x				x			
7 Elección de la dirección de entrega.	x				x				x			
8 Muestra datos del cliente y del artículo.	x				x				x			
9 Asigna la cantidad de artículos	x				x				x			
10 Señala las formas de envío.	x				x				x			
11 Elección de forma de envío	x				x				x			
12 Indica las formas de pago.	x				x				x			
13 Selección de un método de pago	x				x				x			
14 Corroboración de datos.	x				x				x			
15 Muestra la orden de compra.	x				x				x			
16 Aceptación de la orden.	x				x				x			
17 Envío del producto.	x				x				x			
18 Recepción del producto	x				x				x			
2. ¿Cuáles son los sistemas de pago electrónicos que ha utilizado?												
FirstVirtual												
CARI												
IKP												
SEPP												
SET	x								x			
FSTC												
NetBill	x											
NetCheque												
Ecash	x											
CAFE												
Netcash	x											
Cybercoin												
Mondex												
EMV Cash Cards												
Millicent												
SubScrip												
PayWord												

Personas entrevistadas	Patricia Macías				Jesús Ángel				Ricardo Rivera Román			
	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.
2. ¿Cuáles son los sistemas de pago electrónicos que ha utilizado?												
IKP												
MicroMint												
Otros:	SSL				SSL							
3. ¿Cuáles son los sistemas de pago que usted cree se usa más comúnmente?												
FirstVirtual												
CARI												
IKP												
SEPP												
SET	x								x			
FSTC												
NetBill	x											
NetCheque												
Ecash	x											
CAFE												
Netcash	x											
Cybercoin												
Mondex	x											
EMV Cash Cards												
Millicent												
SubScrip												
PayWord												
IKP												
MicroMint												
Otros:					SSL							
4. ¿Por qué considera que estos sistemas sean los más usado?												
Por seguro	x				x				x			
Por ser el más popular												
Costos												
Integración con otros sistemas	x											
5. Al momento de elegir un sistema de pago para en un sitio de comercio electrónico, ¿En qué se piensa?												
Seguridad	x								x			
Integración con varias plataformas (Compatibilidad)												

Personas entrevistadas	Patricia Macías				Jesús Angel				Ricardo Rivera Román			
	Sí	No	No Sé	No Ne	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.
5. Al momento de elegir un sistema de pago para en un sitio de comercio electrónico, ¿En qué se piensa?												
Costos	x											
Desempeño												
Fácil Manejo												
Interoperabilidad con la tienda virtual												
6. ¿La seguridad de una compra en Internet radica en que el sistema de pago sea seguro?	x				x				x			
¿Por qué?												
Verificar Hardware												
Verificar Software												
Accesos lógicos y físicos a servidores												
Seguridad en las conexiones												
Por las intercepciones de información (TC)									x			
7. ¿Qué aspectos debemos verificar, para proporcionar seguridad en la transacción de compra?												
Conocimiento de la tienda virtual	x								x			
La implantación del sistema de pago	x								x			
Buena elección del sistema de pago	x								x			
Implantación de la seguridad del hardware y del SO	x								x			
Uso de técnicas criptográficas	x								x			
Buen establecimiento del procedimiento de compraventa	x								x			
Arquitectura HW/ SW	x								x			
8. ¿Es común el uso de los sistemas de pago en los sitios de comercio electrónico en México?	x								x			
9. ¿Existen requerimientos para dar de alta un sistema de pago electrónico en un sitio de e-commerce en México?	x									x		
¿Cuáles?												

Personas entrevistadas	Patricia Macías				Jesús Angel				Ricardo Rivera Román			
	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.	Sí	No	No Sé	No Ne.
10. ¿Cuáles son los problemas de seguridad que comúnmente se encuentran?												
Falta de conocimientos en los diversos sistemas de pago y en su implementación.	x								x			
Mal diseño de la tienda virtual.	x								x			
Mala implantación de la seguridad en el equipo en el cual se encuentra la tienda.	x								x			
Mal establecimiento de los procedimientos de entrega de producto	x								x			
11. ¿Cuáles son los problemas que produce la inseguridad de las transacciones?												
No llega la mercancía a su destino.	x								x			
Se cometen fraudes	x								x			
Desconfianza en las personas	x								x			
Incertidumbre al no saber de la existencia de los sistemas de pago.									x			
No permite el crecimiento del e-commerce	x								x			

10. ANÁLISIS DE LOS RESULTADOS

En esta sección analizare pregunta por pregunta los resultados obtenidos emitiendo una conclusión por cada una.

1. ¿Cuáles son los pasos esenciales para una compra en Internet?

La mayoria de las personas entrevistadas coinciden conmigo en base a los pasos esenciales de una compra en Internet. Unos me los mencionaron en distinto orden al propuesto, y otros eliminan el paso de dar de alta la cuenta de correo electrónico, y también alguno no considero necesario incluir el envio y recepción del producto. De aqui se desprende, que la mayoría de los sistemas de comercio siguen una serie de pasos ordenados, en la mayoria de ellos radican las debilidades que se mencionaron en el Marco Conceptual, donde hago referencia a debilidades, pero también depende como se implante el sistema de pago electrónico, porque puede proveer seguridad desde el inicio de la compra si hay una buena implantación del sistema de pago junto con un protocolo de seguridad como SSL, PCT o S-HTTP

2. ¿Cuáles son los sistemas de pago electrónicos que ha utilizado?

Los sistemas de pago que más han utilizado las personas entrevistadas se basan en el esquema de tarjetas de crédito, ya que este medio de pago es el más difundido, pero ejerce una gran desconfianza al usuario, porque piensa que su número de tarjeta de crédito puede ser robado para cometer actos ilicitos con ella. De los sistemas de pago el de uso frecuente fue SET, se mencionaron NetBill, Ecash, NetCash, y de protocolos SSL. Se menciono otro sistema de pago que yo no contemplo en este trabajo VPOS La mayoría de las personas entrevistadas no ha utilizado ningún sistema de pago

3. ¿Cuáles son los sistemas de pago que usted cree se usa más comúnmente?

El sistema de pago más común según los entrevistados sigue siendo el sistema de pago que se basa en la tarjeta de crédito, el más mencionado es SET, después le sigue Ecash y Mondex, también hacen referencia al uso de SSL como sistema de pago, cosa que no es solamente es un protocolo que sirve para establecer una comunicación segura entre el servidor y el cliente SSL. Al igual que el punto anterior mencionan NetBill, y NetCash, ahora incluimos también a EMV Cash Cards. Pero la mayoría sigue sin hacer referencia a más sistemas de pago.

4. ¿Por qué considera que estos sistemas sean los más usado?

La mayoría de los entrevistados afirman que los sistemas antes mencionados son utilizados por ser los más seguros, otros hacen referencia a que también es importante la integración con otros sistemas, y los costos que puedan acarrear, solamente una persona hace referencia a su popularidad.

5. Al momento de elegir un sistema de pago para en un sitio de comercio electrónico, ¿En qué se piensa?

En este punto se menciona que lo más importante en lo que se fijan las personas para el establecimiento de un sistema de pago en un sitio de e-commerce, es la seguridad que proveen, el punto que le sigue en importancia es la integración con varias plataformas, y los costos desempeño y fácil manejo se consideran puntos importantes por algunas personas, y el unico punto en el que solamente se hace referencia una vez es el de la interoperabilidad con la tienda virtual

6. ¿La seguridad de una compra en Internet radica en que el sistema de pago sea seguro?

Todo mundo señala que una compra en Internet es segura si el sistema de pago es seguro, la realidad es que una parte de la seguridad de una transacción en Internet si radica en lo antes mencionado, pero no sólo eso se tiene que cuidar para que una compra sea segura, hay que verificar cómo se implanta el hardware a utilizar,

verificar que todo el software incluido en la tienda no tenga hoyos de seguridad, el buen establecimiento del procedimiento de compraventa, etc.

7. ¿Qué aspectos debemos verificar, para proporcionar seguridad en la transacción de compra?

En base a los puntos mostrados en el cuestionario, emitiré las siguientes conclusiones:

- En relación al conocimiento de la tienda virtual, solamente pocos mencionan que en esto no radica la seguridad de una transacción, puede ser que al momento de la realización de ésta no importe en los pasos que ésta involucra, pero si desde un principio no tenemos la confianza de que es una tienda bien establecida, mejor hay que buscar referencias o información para poder estar seguros que no es una tienda fraudulenta.
- Todos mencionan, que la seguridad de una transacción radica en la implantación del sistema de pago, éste es un punto que se debe cuidar, en toda tienda.
- La mayoría también apunta a que la elección de un buen sistema de pago, provee confianza a la transacción.
- También la seguridad de una transacción se basa en que el hardware y el software se hayan implementado bien y con buenas medidas de seguridad.
- Varios no consideran que el uso de técnicas criptográficas tenga que ver con la provisión de seguridad, si el sistema de pago a usar provee un esquema criptográfico robusto, es seguro que también se pueda proveer un alto grado de seguridad, aunque esto también implicaría un costo mayor
- Algunos no consideran importante el buen establecimiento del procedimiento de compraventa, pero están en un error, porque deben asegurar que desde el momento en que el cliente está pagando por ciertos artículos éstos logren llegar a su destino, que sean los artículos pedidos y las cantidades.
- En relación a si la arquitectura HW/SW provee seguridad fue la mayoría que apunto que si, sin embargo varios de ellos en el punto de implantación de medidas de seguridad de HW y SW no lo consideraron importante, siendo que esto va ligado.

8. ¿Es común el uso de los sistemas de pago en los sitios de comercio electrónico en México?

Según la mayoría de las personas entrevistadas si es común el uso del e-commerce en México, cosa en la que no estoy de acuerdo, estas personas se enfocan más al usuario de Internet siendo que ellas son profesionales del tema y tienen contacto con este tipo de personas. Nuestra realidad es que en promedio menos de una tercera parte de la población mexicana, no cuenta con la posibilidad de tener acceso a una computadora y obviamente no existe una cultura para el uso de la misma y mucho menos de Internet, por lo mismo la gente que se dedica a hacer compras en Internet es gente que accesa constantemente a un equipo de cómputo. Un dato en relación con esto es que somos el segundo país en América Latina que más usuarios tenemos en Internet, el primer lugar lo ocupa Argentina.

9. ¿Existen requerimientos para dar de alta un sistema de pago electrónico en un sitio de e-commerce en México?

La mayoría de ellos no conocen ningún método formal para dar de alta un sistema de pago, sin embargo varios de ellos mencionan los estándares que se deben seguir para implantación de equipos y software. En realidad aquí en México se que hay por lo menos una empresa que se dedica a tratar de regular todo lo relativo a seguridad e imaginó que se abocarán en algún tiempo a los sistemas de pago sino es que ya lo hicieron, está empresa es SeguriData.

10. ¿Cuáles son los problemas de seguridad que comúnmente se encuentran?

Haciendo referencia a las posibles respuestas mostradas en el cuestionario, se deriva:

- Al punto de falta de conocimientos en los diversos sistemas de pago y su implementación, la mayoría no lo considera un problema, pero hay que pensar sino se tienen los conocimientos suficientes para la implantación del mismo difícilmente podrán instalar toda la seguridad que pueda proveer, para que este esquema también pueda ser inviolable.

- Solamente pocos creen que es un problema de seguridad el mal diseño de la tienda virtual, cosa que es importante, para saber en que posibles lugares podemos tener desvío de información.
- Algunos si consideran que la mala implantación de la seguridad en un equipo es un problema, sino se cuidan cosas, como por ejemplo cuidar que se tengan equipos que no permitan el ingreso de personas ajenas al dominio de la tienda, si este aspecto no se toma en cuenta puede ocasionar muchos problemas.
- Muy pocos consideraron la entrega del producto como un problema, sino estamos enviando la información por Internet se debe asegurar de algún modo que el producto final no llegue alterado al momento de la entrega, o en una entrega física se debe asegurar que el producto o servicio debe llegar al domicilio solicitado y cuidar mucho que la o las personas que recibirán el producto son las correctas.

11. ¿Cuáles son los problemas que produce la inseguridad de las transacciones?

Los puntos mostrados en el cuestionario como los problemas que producen la inseguridad en las transacciones son:

- Pocos son los que consideran éste como un problema, pero creo que sí es un problema importante, ya que va ligado con el fraude si se comete un abuso en un pago y se altera la dirección de entrega el pedido nunca llegará al destino solicitado, al igual que el procedimiento de entrega del mismo.
- En este punto todos estuvieron de acuerdo ya que los fraudes que se cometen son de distintos tipos, pero más que nada se incurre en el fraude con el número de la tarjeta de crédito, en el cual se altera la información para que se le carguen saldos a la cuenta del usuario de compras que el no realizó, etc.
- Sólo pocas personas consideraron la incertidumbre como un problema, esta incertidumbre se refiere más que nada, al desconocimiento que produce el e-commerce, y obvio sino se sabe como funciona y que existen sistemas de pago electrónicos, no se podrá confiar en la realización de una transacción en Internet.
- No permite el crecimiento del e-commerce, en éste solamente una de las personas entrevistadas estuvo de acuerdo, sin embargo la tendencia es que en todo tipo de negocio tienda al e-commerce debido al giro de la tecnología, de este punto derive otro que este crecimiento no podrá detenerse, pero aún sigue siendo poco su uso.

11.Conclusión

En base a los resultados anteriormente obtenidos, se ve que sigue habiendo todavía problemas de seguridad en el comercio electrónico, por lo que se nota que hay una tendencia a que la difusión del comercio electrónico se está dando aunque no es muy frecuente su uso, y por lo mismo el conocimiento de los sistemas de pago electrónico y su seguridad no son conocidos.

Los sistemas de pago electrónico más usado en Internet son los de Tarjeta de Crédito, el más difundido de ellos es SET. Por lo que se refiere a los demás, el que va a tener una gran difusión junto con el esquema de tarjetas de crédito va a ser el dinero electrónico, ya que en la actualidad muchos países europeos manejan ambos con el uso de un dispositivo físico denominado Smart Card. El que no se ha difundido y se ocupa para compraventa de información de baja denominación son los micropagos, que tiende a ser amplio su crecimiento. En relación al esquema de cheques electrónicos, no es muy frecuente su uso.

Al momento de que un nuevo usuario de e-commerce va a incursionar en él, desconfía de este comercio al momento del pago, porque piensan que la información, por lo general, del pago con tarjeta de crédito será robada o pagará por bienes o servicios que nunca obtendrá, y muchos de ellos no se aseguran que la tienda esté bien establecida y se tengan recomendaciones de la misma. Muchas de las personas al momento de realizar este tipo de compras llegan a ser sujetos de fraudes y robos, por tal motivo muchas de las mismas temen a realizar nuevamente una compra en otra tienda y comentan con otras personas lo sucedido, por lo que transmiten su desconfianza a más personas.

Otro aspecto importante es que personas involucradas en el e-commerce, no cuidan aspectos importantes de la seguridad en una transacción, cosas tan simples como una buen diseño en su tienda virtual no se da, o se descuidan los procedimientos de compraventa o simplemente el de entrega del producto.

Hay que hacer notar que en los países de Latinoamérica tiende ha haber un crecimiento del comercio para el manejo de negocios, aunque muchas personas aún no tengan acceso a Internet, y los problemas de seguridad no se hayan erradicado.

12. Aprobación de la Hipótesis

Al haber obtenido los resultados de los cuestionarios aplicados, y a toda la información que integra está investigación, apoyan las hipótesis que propongo.

"Existencia de desconfianza e incertidumbre de las personas a realizar una compra en Internet, principalmente en la seguridad del medio por el cual se realiza el pago, lo que da lugar al uso moderado de Internet para realizar transacciones de e-commerce."

Los puntos que analicé como causas y efectos de mi hipótesis son:

Variables Independientes:

- Mal establecimiento del procedimiento de compraventa.

Si no se establece bien este procedimiento, pueden darse los problemas mencionados en lo que considero como variables dependientes, cosas que las personas entrevistadas, los creen como problemas derivados de la desconfianza en el e-commerce.

- Mala implantación de seguridad en los sistemas de pago digital.

En este punto la mayoría de las personas entrevistadas coinciden en que sino se implanta bien el sistema de pago se puede alterar la información de pagos y pedidos, e incurrir en el fraude y el robo.

- Incertidumbre al no saber cómo funcionan los sistemas de pago y el comercio electrónico en general.

Aquí la incertidumbre lo estoy manejando como el desconocimiento al funcionamiento de los sistemas de pago y el comercio electrónico, muchos usuarios de Internet al igual personas que lo implantan no tienen conocimientos suficientes para poder determinar posibles hoyos de seguridad, lo que compromete la seguridad de la información

Variables Dependientes:

- Pérdida de la mercancía.

Según algunos artículos leídos, y las respuestas que obtuve del cuestionario, si se produce que el artículo o servicio no lleguen al destino.

- Produce desconfianza al cliente en el sistema de pago.

Este es el más grande de los problemas que existe ya que el usuario desconfía sobremanera en dar sus datos al momento de realizar el pago, y obviamente produce que no sea frecuentemente usado el e-commerce, por lo que el sistema de pago no será muy difundido

- Fraudes en el comercio electrónico.

En el e-commerce se siguen dando un sinnúmero de fraudes, considerados por una gran parte de la población de personas que ocupan Internet. Sobre todo se demuestra en el uso de los esquemas con tarjeta de crédito.

- No permite el uso frecuente del comercio electrónico

Al producirse desconfianza en los usuarios, difícilmente ellos volverán a hacer uso del mismo, hasta que no se les demuestre que el sistema de pago sea seguro.

Marco Instrumental

V. MARCO INSTRUMENTAL

En la actualidad la mayoría de los sitios de comercio electrónico cuentan con varias formas para realizar pagos en Internet, en esta investigación solamente me enfoqué a los sistemas de pago electrónicos que al momento de su realización estaban en funcionamiento, y algunos que pasan a formar parte de la historia de este tipo de pagos. Este tema aún se sigue desarrollando, por lo que es conveniente continuar su estudio e ir difundiendo su progreso, por tal razón, me propongo concluir las siguientes acciones:

5.1 PROPUESTAS DE ACCIÓN

5.1.1 Actividades Realizadas

- He preparado un artículo del funcionamiento y los ataques de Secure Socket Layer.
  He propuesto a la revista Emprendedores que me permita la publicación de mi artículo. Buscaré revistas especializadas en el tema para ver la posibilidad de incluir el artículo en alguna.

- Realización de una exposición de Secure Socket Layer.
  La exposición realizada fue a la clase optativa de Criptografía del grupo 2081, impartida por el profesor Leobardo Hernández Audelo en el semestre 2001-2.

5.1.2 Actividades a Realizar

- Creación de una página Web con información relativa a la presente investigación y que se mantendrá en actualización constante.
  La información de los sistemas de pago el e-commerce y alguna información adicional de criptografía entre otros, será difundida a través de una página Web, que próximamente se encontrará en http://mx.geocities.com/mmrpli/index.html

- Dar ponencias relativas a los sistemas de pago electrónico en el e-commerce en universidades.
  Creare el material necesario para realizar ponencias en universidades, el primer lugar propuesto es la Facultad de Contaduría y Administración de la UNAM y su posgrado. También trataré de participar en más universidades y dar conferencias en algunos eventos relacionados con el tema

- Difusión de la información obtenida en foros de discusión de seguridad y e-commerce.
  Ingresaré a foros de discusión en los cuales difundiré la dirección de la página que crearé, aparte me propongo tratar de sacar discusiones en relaciones al tema e ir transmitiendo el conocimiento previamente adquirido para los participantes de los foros

- Definición de los temas de un módulo de sistemas de pago que se incluiría dentro de una materia de e-commerce.
  Los temas aquí definidos serán como un tema anexo a una materia de comercio electrónico, la cuál incluirá principalmente los puntos desarrollados a lo largo de este trabajo de investigación, pudiendo incrementar el tema con más aspectos de seguridad que no se tocan en la investigación como los aspectos referentes a seguridad física.

Conclusiones

CONCLUSIONES

- Es sabido que en el comercio electrónico aún se siguen dando fraudes, robos y alteración de información referente a las transacciones realizadas en los sitios de comercio. Esos actos ilícitos conllevan al uso moderado del e-commerce, por tal motivo la difusión de los sistemas de pago electrónico es poca, debido a que esta situación de inseguridad al realizar una transacción electrónica produce desconfianza en los usuarios de Internet, por lo cual es difícil que realicen una compra en Internet.

- La mayor parte de las personas aún desconoce como opera el comercio electrónico en general, y más en los países menos desarrollados, ya que no se tiene la posibilidad de ingresar a un equipo de cómputo que permita el ingreso a Internet, sólo una parte mínima de la población, menor al 10% de habitantes en los países de América Latina, pueden hacerlo.

- Aunque casi no se use este tipo de comercio sin fronteras y se siga considerando inseguro, es indiscutible su crecimiento, ya que las tendencias de negocios se enfocan no sólo a dar a conocer su producto o servicio a sólo ciertas localidades o regiones, si no que ahora pretenden globalizarlos de manera que sus productos, lleguen a ser conocidos y demandados de manera mundial.

- Al momento de establecer los sitios de e-commerce muchas veces no se cuenta con los conocimientos suficientes para un establecimiento seguro de las transacciones que se llevan a cabo en los sitios de e-commerce, por lo que dan lugar a que se cometan los problemas antes mencionados, por eso mismo se deben cuidar todos los aspectos que engloban una implantación segura de éstos, desde el diseño de la tienda virtual, qué tipo de hardware y software se va a ocupar y qué medidas de seguridad proveen, en donde puede haber desviación o alteración de la información o de la entrega del producto al momento del establecimiento de todo el proceso de la transacción de compraventa, si el sistema de pago electrónico es el idóneo para el tipo de producto que estamos vendiendo y si proporciona la seguridad requerida

- Muchos de los sitios de e-commerce aún siguen realizando sus pagos con métodos tradicionales, como depósitos a cuentas bancarias de manera física, por medio de proporcionar sus datos vía telefónica, algunas veces solamente se levanta el pedido en el sitio y llegan a cobrar al domicilio indicado. Los otros sitios que realmente ya se enfocan al pago electrónico, por lo general ocupan sistemas de pago basados en tarjeta de crédito, principalmente SET, y ocupan por lo general un protocolo de comunicación segura SSL. Otro medio de pago que es menos difundido que el de tarjeta de crédito, pero que tiende al reemplazo del dinero en efectivo, es el dinero electrónico, éste medio es usado junto con el esquema de tarjetas de crédito y débito y otro tipo de aplicaciones, en un dispositivo denominado Smart Card o Tarjeta Inteligente, el uso de esta tarjeta tiende a crecer en un futuro no muy lejano. Más que nada su uso ya se está dando en países europeos, cubriendo las funcionalidades de monedero electrónico, sistemas de lealtad, telefónicas y de uso en el ingreso al transporte o algún otro tipo de sitio.

- En la actualidad información de e-commerce puede ser encontrada en varios libros, revistas, periódicos, artículos publicados por institutos de investigación, escuelas y algunas empresas dedicadas al e-commerce y a su seguridad, en algunos seminarios y conferencias, pero gran parte de la información se encuentra en páginas de Internet. Para las personas que se interesen en este tipo de información, deberán estar conscientes que la mayor parte de la información que se pretenda buscar será en inglés y haciendo referencia a otros países, y la poca información que se llegue a encontrar en español, muchas veces suele ser pobre y solamente se enfoca a aspectos globales. La información referente a los sistemas de pago electrónico es poca, pudiendo notar que cada vez que un sistema de pago deja de usarse es mucho más difícil hallar información del mismo.

Anexo 1. Smart Cards

ANEXO 1. SMART CARDS (TARJETAS INTELIGENTES)

Las tarjetas inteligentes (tarjetas chip) nacieron en el año 1983. Su filosofía es muy sencilla, se trata de almacenar información con una cierta autonomía. Son los principales contendientes por el título del dinero del futuro, son tarjetas de plástico de tamaño similar al de las tarjetas de crédito normales, pero con un chip integrado por dentro. El chip puede tener dos funciones, ser un microprocesador o actuar como un chip de memoria. Se les llama inteligentes porque, además de tener una capacidad de almacenamiento mucho mayor que la tradicional cinta magnética de las tarjetas ordinarias, la pueden procesar. La ISO ha definido a las tarjetas inteligentes formalmente con el estándar 7816. Existen dos tipos básicos de tarjetas inteligentes: las desechables, y las recargables. Ejemplos de estas tarjetas son: Visa Cash , Visa Distribución, Crédito y Débito en chip, identificación.

El chip proporciona una capacidad de memoria significativamente superior a la banda magnética que utilizan las tarjetas de crédito o débito actuales. Esto permite integrar nuevas aplicaciones a las tarjetas. El chip tiene tres funciones principales:

a) almacenamiento de datos.
b) seguridad en la información.
c) procesamiento de datos.

El microcircuito es capaz de procesar información. Esto permite el manejo de sistemas de seguridad robustos basados en la tarjeta y en la terminal. Esto a su vez, permite que las transacciones se validen "fuera de línea", es decir, sin tener que viajar a los sistemas del banco, lo cual reduce los costos de telecomunicación, agiliza la transacción y mejora el nivel de servicio / aceptación de la tarjeta

La mejora en los sistemas de seguridad y la velocidad de la transacción permiten que las tarjetas tengan el potencial de utilizarse en más lugares como: el metro, el taxi, la máquina que dispensa refrescos, el teléfono público; y además, permiten que la tarjeta accese a nuevos canales de comunicación como: la computadora personal, los teléfonos celulares, la televisión interactiva, entre otros.

El uso de tarjetas inteligentes se ha popularizado principalmente en Europa y Asia, no así en Estados Unidos. Las tarjetas pueden utilizarse en la telefonía, registros médicos y como tarjetas de débito y crédito. La telefonía parecería ser la principal aplicación de las tarjetas, ya que se estima que en 1996 se vendieron 420 millones de tarjetas telefónicas. Sin embargo, el mercado que mayores cambios sufrirá con la llegada de las tarjetas inteligentes es el del dinero. Actualmente más de 90 instituciones bancarias en el mundo tienen funcionando sistemas que las utilizan.

Ya existen los llamados ATMs (autocajeros) personales, que son aparatos del tamaño de una calculadora, con los que uno puede accesar por teléfono las computadoras del banco y trasladar dinero de su cuenta a la tarjeta, desde donde está. Y, por supuesto, una de las aplicaciones principales en el futuro será el comercio electrónico a través de Internet.

Clasificación de las tarjetas:

Por su tecnología:

- Tarjeta inteligente de contacto: Contiene un chip en la superficie de la tarjeta en conformidad con el estándar de ISO 7816.

- Requieren alimentación y reloj externos.
- Necesitan conexiones de e/s con el exterior.
- El lector de tarjetas y la tarjeta completan un circuito cuando entran en contacto.

- Tarjeta inteligente sin contacto: Realizan la conexión por medio de transmisiones de radio frecuencia.

- La alimentación, y la comunicación con el lector se logra mediante acoplamiento electromagnético.
- Aplicaciones: sistemas de peaje, pago en autoservicios.

Por su capacidad:

- Tarjeta con memoria: Almacena y recupera una serie de flujo de datos que son enviados o recibidos del chip de la propia tarjeta.
- Tarjeta con memoria protegida: Esta tarjeta requiere un código secreto (NIP), que es necesario ser introducido antes de poder enviar y recibir datos el chip.
- Tarjeta con microprocesador: Tiene un chip microprocesador, este chip puede contener un microcódigo que define una estructura de comando, una estructura de archivos y una estructura de seguridad en la tarjeta.

Capacidades dadas en Kb

- **1Kb**. Con 1Kb de memoria disponible y un sistema operativo diseñado especialmente para pagos, la tarjeta Payflex de 1K garantiza un gran nivel de seguridad.
- **4Kb**. Los beneficios de esta tarjeta, son que tiene 4Kb de memoria disponible y un poderosos sistema operativo que permite ampliar las aplicaciones y los servicios. La tarjeta es compatible con el nuevo estándar EMV (Europay-Mastercard-Visa).
- **SAM 4K**. Máxima seguridad, compatible con las tarjetas payflex.
- **Cyberflex 8K**. Tarjeta multiaplicaciones. El lenguaje estándar Java, puede ser aplicado a esta tarjeta.

Por su chip:

- Tarjetas microprocesadas: Tienen como principal utilidad el uso de sistemas de contador (tarjetas monedero, tarjetas de telefonía, etc.) y de identificación de alta seguridad. Su gran uso en la banca ha permitido una rebaja constante en su precio. Normalmente no permiten almacenar mucha información, ya que su uso requiere generalmente poca cantidad de datos. Éstas disponen de una zona de memoria "protegida", sólo accesible por el fabricante, que garantiza una identificación única a nivel universal.

- Tarjetas de memoria: Substituyen la complejidad del sistema de seguridad por una mayor capacidad de almacenar datos. Estas tarjetas permiten la lectura y grabación de datos con las funcionalidades que esto comporta. Actualmente se están fabricando tarjetas de hasta 32 Kb. de memoria. Evidentemente, la capacidad de almacenamiento está directamente relacionada con su costo. Al ser gravables en su totalidad, estas tarjetas no garantizan la identificación con absoluta segundad, por lo que se ha de recurrir a sistemas de encriptación propios de la aplicación con la dicha tarjeta ha de operar.

Por sus aplicaciones principales:

- Crédito y Débito en Chip: Hoy, cuando pagas con tu tarjeta de crédito o de débito, la banda magnética se desliza en la terminal y se lee la información necesaria para realizar tu pago. Con la aplicación de crédito y débito en el chip, tu tarjeta en lugar de deslizarse al pagar, se insertará en un lector de la terminal para leer la información requerida para el pago directamente del microcircuito.

  En este esquema la información de pago se almacena en un ambiente más seguro, lo cual permite reducir el potencial de fraude de la tarjeta. Los esquemas de seguridad más sofisticados permiten también reducir los costos de las transacciones y mejoran el nivel de aceptación de tu tarjeta. Gracias a la gran memoria del microcircuito, es posible que con un sólo plástico tengas acceso a diversas cuentas de crédito o de débito o si lo deseas, podrás pagar con tu monedero.

- Monedero electrónico. Forma de pago para esas pequeñas compras rutinarias que te evita la necesidad de llevar el bolsillo lleno de monedas y cambio. Visa Cash es el primer monedero electrónico en México con un avanzado chip que contiene en su memoria un determinado valor prepagado para hacer compras pequeñas día a día, que automáticamente se van descontando del saldo de tu tarjeta.

  La tarjeta plástica viene equipada con un microcircuito que guarda un determinado valor monetario. Cada vez que usted utiliza la tarjeta para abonar una compra, el total de la compra se deduce automáticamente del saldo almacenado en la tarjeta.

  Pasos:
  - Inserte su tarjeta en el lector de chip.
  - Espere el monto de la compra.
  - Si está de acuerdo con el importe, confirme la compra presionando el botón

  Este tipo de tarjetas se cargan a partir de efectivo, o mediante una tarjeta de crédito o débito de banda magnética en terminales situadas en sucursales bancarias, cajeros automáticos, terminales de carga atendidos, etc..

- Lealtad: Esta aplicación está enfocada en hacer más eficientes los programas de lealtad o de "cliente frecuente". Al consumir, los puntos de lealtad recibidos son almacenados directamente en el chip de la tarjeta. Para redimir los puntos, sólo es necesario insertar la tarjeta en la terminal de aceptación.

- Identificación: Esta aplicación posibilita el almacenamiento seguro de información médica, de seguros, historial académico, etc. Estos datos sólo podrán ser accesados en lugares equipados para ello y con esto se facilitará un mejor control y disponibilidad de la información. La aplicación permite también identificarse electrónicamente de manera segura, con lo cual podrá accesar a lugares como su oficina o identificarse frente a un sistema de cómputo u otros.

Beneficios de las Tarjetas Inteligentes

El beneficio primordial que aporta la tarjeta de chip es que una misma tarjeta le dará acceso a más información en más ubicaciones tradicionales y nuevas, lo que aumentará su utilidad y el grado de conveniencia para el usuario.

- Podrá utilizar su tarjeta para pagar en lugares donde hoy no puede como el metro, el teléfono público, la máquina que dispensa refrescos y muchos más.
- Podrá pagar con su tarjeta a través de su teléfono, su computadora o su televisión.
- La tarjeta de microcircuito le evitará cargar diversas tarjetas en su cartera, ya que con un sólo plástico podrá tener acceso a su diversas cuentas de crédito o de débito o si lo desea, podrá pagar con su monedero.
- Su tarjeta le permitirá también identificarse electrónicamente de manera segura, con lo cual podrá accesar a lugares como su oficina o identificarse frente a un sistema de cómputo u otros.
- También posibilitará el almacenamiento seguro de datos no financieros en la tarjeta, como información médica, de seguros, histonal académico, etc. Estos datos sólo podrán ser accedidos en lugares equipados para ello

En general, su institución financiera podrá ofrecerle más servicios, y podrá crear una tarjeta de pago que responda a sus necesidades particulares como usuario de servicios bancarios.

Ventajas de las Tarjetas Inteligentes

- Caída de los costos para empresarios y usuarios
- Estándares técnicos específicos ISO 7810, 7811, 9992 ,10536
- Seguridad de la información
- Tarjetas Inteligentes Multiservicio. Marketing cooperativo

- Ahorros de papel
- Administración y control de pagos más efectivo
- Transacciones Off y Online
- Información organizada
- Creación de ambientes de oficina y ofimáticos controlados
- Información de emergencia médica
- Reducción del fraude
- Altas capacidades de memoria
- Privacidad. Sólo el usuario accede a los datos

Desventajas de las Tarjetas Inteligentes

- Tasas bancarias asociadas con la tarjeta de crédito.
- Molestias para recuperar la información de una Tarjeta Inteligente multipropósito si se pierde o es robada.
- Computer hackers.
- Virus.
- Costos.
- Es necesario un lector para las tarjetas inteligentes
- La tarjeta requiere ser recargada.
- Por su tamaño las tarjetas pueden extraviarse fácilmente
- Depende de la energía eléctrica para su utilización.
- Puede ser dañada si se derrama un líquido sobre ella.

Aplicaciones de las Tarjetas Inteligentes

La realización de software asociado a este nuevo entorno permite diversidad de aplicaciones comerciales. Sin embargo actualmente no existen demasiados equipos de desarrollo que trabajen en esta línea debido a la poca expansión del sistema y a la gran tecnología requerida. Aplicaciones tipo con tarjetas inteligentes son:

- **Control de acceso y de presencia**. Limitan y controlan el acceso a áreas restringidas, edificios, oficinas, clubes, administración, ordenadores, ...

- **Pagos electrónicos**. Ofrece una solución ideal para aplicaciones de tarjeta monedero, tarjetas telefónicas, maquinas expendedoras, clubes de clientes, compras electrónicas, ...

- **Transportes**. Medio de pago seguro y fácil de utilizar para transportes públicos, billetes de avión parquímetros, peajes de autopistas, ...

- **Identificación y seguridad en informática**. Control de acceso computadoras, terminales, redes, aplicaciones de software, bases de datos, directorios, ficheros confidenciales,

- **Sanidad**. Almacenamiento de los datos del paciente, incluyendo su historial médico. Para que los profesionales sanitarios puedan utilizarlos.

- **Procesos industriales**. Control de accesos en procesos de producción, medición de tiempos, seguridad industrial, ...

Seguridad de las Tarjetas Inteligentes

No existe un sistema seguro al 100%, pero el de las Tarjetas Inteligentes es teóricamente el que ofrece un mayor grado de seguridad.

Krueger, J y Schloss, R, en pruebas realizadas en 1996, aseguran que, para poder romper un sistema como el que nos ocupa necesitaríamos una acumulación exorbitante de capital, tiempo y tecnología.

La Tarjeta Inteligente es un mecanismo muy seguro para el almacenamiento de información financiera o transaccional. La Tarjeta Inteligente es un lugar seguro para almacenar información como claves privadas, número de cuenta, password o información personal muy valiosa. Esta capacidad se debe a:

- Encriptación
- Clave Segura (PIN)
- Clave Secundaria de Seguridad (algoritmo criptográfico que dos partes usan para codificar y decodificar información)
- Sistemas de Seguridad Redundante
- Firmas digitales
- A través de Sistemas Biométricos:
  - Huella dactilar
  - Retina

Hay dos tipos de seguridad:

- Seguridad lógica:
  - Ninguna función o combinación de funciones puede tener como resultado la puesta en claro de información sensible.
  - Limitación del número de funciones en un tiempo dado
  - Implementación de algoritmos de encriptación y autenticación
- Seguridad física:
  - Capas de óxido protegen las celdas de memoria
  - EEPROM: las sondas habituales destruyen las celdas

Amenazas contra las tarjetas inteligentes

Las tarjetas inteligentes son vistas por algunos como las "armas mágicas" de la seguridad informática: herramientas con múltiples fines que pueden ser usadas para controlar accesos, comercio electrónico, autenticación, protección de la privacidad y una gran variedad de aplicaciones. Mientras la flexibilidad de las tarjetas inteligentes las hace una opción muy atractiva para muchos negocios, eso también multiplica los peligros de su seguridad en conjunto. Hasta la fecha, ha habido poco análisis sobre estos riesgos en su seguridad.

Debido al gran número de partes involucradas en cualquier sistema basado en tarjetas inteligentes, existen muchas clases de ataques a los cuales son susceptibles. La mayoría de estos ataques no son posibles en sistemas convencionales e independientes porque tienen que tener lugar en la frontera con los sistemas informáticos tradicionales. Pero en el mundo de las tarjetas inteligentes los ataques que se mencionan a continuación tienen un peligro real.

- **Ataques desde el terminal contra el poseedor de la tarjeta o el propietario de los datos**. Es el ataque más fácil de entender. Cuando el dueño de la tarjeta inteligente la coloca en el terminal, confía en el terminal para realizar entradas y salidas correctas desde la tarjeta. Los mecanismos de prevención en la mayoría de los sistemas de tarjetas inteligentes dan por hecho que la terminal sólo tiene acceso a la tarjeta por un corto período. Los mecanismos de protección reales, sin embargo, no tienen nada que ver con la interacción entre tarjeta inteligente y terminal: son sistemas de proceso que monitorizan las tarjetas y la terminal, señalando las conductas sospechosas.

- **Ataques del Poseedor de la Tarjeta contra la Terminal**: Más sutiles son los ataques del Poseedor de la Tarjeta contra la Terminal. Estos precisan el uso de tarjetas falsas o modificadas ejecutando programas especiales, con la intención de engañar al protocolo de comunicación entre la tarjeta y la terminal. Los protocolos bien diseñados reducen el riesgo de este tipo de ataques. La amenaza se reduce aún más cuando la tarjeta posee características físicas difíciles de falsificar (como el holograma de una tarjeta VISA) que pueden ser revisados manualmente por el poseedor de la terminal.

- **Ataques del Poseedor de la Tarjeta contra el propietario de los datos**: En muchos sistemas de comercio basados en tarjetas inteligentes, la información grabada en la tarjeta debe ser protegida del propietario de la misma. En algunos casos, éste no debe conocer esa información. Si la tarjeta guarda un valor y éste puede ser modificado por el dueño, éste puede conseguir dinero extra muy fácilmente. Ha habido muchos ataques con éxito de este tipo, como análisis de fallos, ingeniería inversa y ataques por canales colaterales, como los análisis de tiempo y energía.

- **Ataques del Poseedor de la Tarjeta contra el Emisor**: Hay muchos ataques financieros que parecen ir dirigidos contra el emisor, pero de hecho están atacando a la integridad y autenticidad de la información o programas grabados en la tarjeta. Si los emisores de tarjetas deciden poner bits que autorizan el uso del sistema en una tarjeta, no se deberían sorprender cuando esos bits son atacados. Estos sistemas descansan sobre la cuestionable suposición de que el margen de seguridad de una tarjeta inteligente es suficientemente grande para sus propósitos.

- **Ataques del Poseedor de la tarjeta contra el Fabricante del programa**: Generalmente, en sistemas donde la tarjeta es emitida a un presunto usuario hostil, lo lógico es que la tarjeta no tenga ningún programa nuevo cargado en ella. La presunción fundamental puede ser que la separación entre el dueño de la tarjeta y el propietario del software es imposible de restablecer. Sin embargo, los atacantes han demostrado una habilidad increíble en conseguir que los aparatos necesarios les sean enviados, a veces gratis, para ayudarles a lanzar un ataque.

- **Ataques del Poseedor de la Terminal contra el Emisor**: En algunos sistemas, el propietario de la terminal y el emisor de las tarjetas son partes totalmente distintas. Esta separación introduce muchas nuevas posibilidades de ataque. La terminal controla toda la comunicación entre la tarjeta y el emisor de la misma, y siempre puede siempre falsificar registros o fallar al completar uno o más pasos de la transacción, en un intento de facilitar el fraude o crear dificultades al servicio de atención al cliente del emisor.

- **Ataques del Emisor contra el Poseedor de la Tarjeta**: En general, la mayoría de los sistemas presuponen que los emisores de las tarjetas actúan de buena fe. Pero éste no es precisamente el caso. Estos ataques son generalmente invasiones de la privacidad, de uno u otro tipo. Los sistemas de tarjetas inteligentes que sirven como sustitutos del dinero en efectivo deben ser diseñados muy cuidadosamente para poder mantener las mismas propiedades del dinero en efectivo: anonimato y ausencia de vinculación.

- **Ataques del fabricante contra el propietario de los datos**: Ciertos diseños de los fabricantes pueden tener efectos perjudiciales para los propietarios de los datos en un sistema. Diseñando un sistema operativo que permita (o incluso recomiende) que múltiples usuarios ejecuten programas en la misma tarjeta, aparecen nuevos temas en cuanto a seguridad, como la subversión del sistema operativo, generadores de números aleatorios intencionadamente débiles o una aplicación en una tarjeta inteligente que altere a otra que se ejecute en la misma tarjeta.

Garantizar la seguridad de los sistemas de tarjetas inteligentes significa reconocer estos ataques y diseñarlos en un sistema. En los mejores sistemas, no importa si (por ejemplo) el usuario puede alterar la tarjeta. Es muy simple: trabajan con el modelo de seguridad, no contra él.

Evolución de las Tarjetas Inteligentes

Todas las tarjetas inteligentes, y terminales evolucionan rápidamente para mejorar los servicios en el futuro, como por ejemplo el servicio de los bancos por medio del teléfono, acceso a Internet, servicios en línea etc.

Para el año 2001, cerca de 100 billones de transacciones serán hechas mediante tarjetas inteligentes. La tarjeta será capaz de manejar la vida profesional de las personas, desde ordenar comida, comprar boletos para el teatro, o controlar las finanzas mediante el teléfono, en cualquier lugar del mundo.

En los años siguientes las tarjetas inteligentes podrán tener información vital sobre una persona, esta información podría ser como: actas de nacimiento, historiales académicos o boletas de calificaciones, curriculum vitae, datos médicos, etc

Glosario

GLOSARIO

aclaración / clearing – **R.A.** Acción y efecto de disipar, quitar lo que ofusca la claridad o transparencia de alguna cosa.

adquirente / acquier
- Persona que compra.
- **Inf.** Miembro de una institución financiera que soporte la actividad del vendedor con una relación de cuentas con el vendedor.

aleatorio / random – Tomar valores al azar.

algoritmo / algorithm
- **R.A.** Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.
- **Inf.** Un algoritmo es una serie de pasos, que se ejecutan en un orden determinado, para llegar a la solución de un problema. Estos pasos son finitos, y aseguran que si el problema tiene solución está será encontrada en un tiempo finito.

anonimato – **R.A.** Carácter o condición de ocultar la identidad de una persona.

autenticación / authentication **Inf.** Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje y su integridad.

autoridad certificadora (AC) / certificate authority (CA) – **Inf.** Tercera parte usada para confirmar las relaciones entre negocios y las transacciones en Internet que se están ejecutando, tan bien como las relaciones entre los negocios y sus llaves públicas.

autorización / autorization **Inf.** Permiso, garantizado por una persona o personas propiamente designadas, para ejecutar alguna acción en el comportamiento de la transacción. Este es un proceso, en el cuál se confirma que un pago dado no es más grande de la cuenta de débito del tarjetahabiente sobre el límite de una cuenta de crédito, y reserva la cantidad específica de crédito.

banco / bank
- **R.A.** Establecimiento público de crédito, constituido en sociedad por acciones.
- **Fin.** Institución que realiza operaciones de banca, es decir es prestatario y prestamista de crédito; recibe y concentra en forma de depósitos los capitales captados para ponerlos a disposición de quienes puedan hacerlos fructificar.

banco del emisor / issuing bank **Inf.** Emite el crédito para acreditar a un tarjetahabiente. Cuando una autorización es solicitada, el banco del vendedor, solicita que los fondos sean transferidos desde la compañía de tarjeta de crédito, la cual recibe los fondos desde el banco del emisor.

banco del vendedor / merchant bank – **Inf.** Cuando una autorización de tarjeta de crédito es procesada, lo primero que hace es detenerse en el banco donde la tienda en línea tiene una cuenta con el vendedor.

bit (binary digit)
- **R.A.** Unidad de medida de información equivalentes a la elección entre dos posibilidades igualmente probables.
- **R.A./Inf.** Unidad de medida de la capacidad de memoria, equivalente a la posibilidad de almacenar la selección entre dos posibilidades, especialmente usadas en las computadoras.

	- **Inf.** Unidad mínima de almacenamiento de la información. Su valor puede ser 0 ó 1 ó verdadero o falso.
browser / visualizador, navegador, hojeador	- **Inf.** Corresponde a un programa computacional (software) cliente utilizado para navegar a través de distintos servicios Internet (ejemplo: páginas web). - **Inf.** Aplicación para visualizar todo tipo de información y navegar por el espacio Internet. En su forma más básica son aplicaciones hipertexto que facilitan la navegación por los servidores de información Internet; cuentan con funcionalidades plenamente multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc.
business to business (B2B) / empresa a empresa	- **Inf.** Modalidad de comercio electrónico en el que las operaciones comerciales se realizan entre empresas (por ejemplo, una empresa y sus proveedores) y no con usuarios finales.
business to consumer (B2C) / empresa a consumidor	- **Inf.** Modalidad de comercio electrónico en el que las operaciones comerciales se realizan entre una empresa y sus usuarios finales.
byte	- **Inf.** Octeto; mínima unidad direccionable, carácter. (8 bits).
cargo	- **R.A.** Pago que se hace o debe hacerse con dinero de una cuenta, y apuntamiento que de él se hace. - **Inf.** Acción y efecto de asentar un débito en una cuenta determinada. Sinónimo de "débito". Implica un costo o gasto adjudicado a una cuenta específica
carrito de compras / shopping cart	- **Inf.** Parte del proceso de compra de una "Tienda Virtual", en el que se depositan los productos o servicios seleccionados para su compra y posterior pago.
cartera digital / digital wallet	- **Inf.** Es un software que permanece residente el disco duro de un comprador en línea. Cuando están listos para hacer una compra, la cartera despliega una venta para mostrar las opciones de pago. Algunas carteras soportan tarjetas de crédito con información encriptada. Otras usan monedas digitales.
certificado / certificate, digital certificate, electronic certificate	- **R.A.** Documento en que se certifica. - **Inf.** Un certificado digital es una clase especial de mensajes firmados digitalmente, que contiene información acerca de una llave pública y el propietario de una llave pública. Un certificado emitido y firmado por una autoridad certificadora une la llave pública al número de cuenta. - **Inf.** Llave pública y una identificación de datos firmados por una tercera parte confiable para proveer autenticación e integridad de la llave. - **Inf.** Son ID's digitales usados para representar credenciales online. Estos certificados son emitidos por compañías que actúan como una tercera parte confiable. - **Inf.** Documento digital diseñado para eliminar problemas de seguridad como la autenticación y no repudiación cuando ejecuta transacciones comerciales via Internet. El certificado contiene información acerca de la autoridad certificadora, el propietario del certificado, una llave pública, la validez del periodo del certificado, y el host para el cual fue emitido el certificado. El token es diseñado de tal manera que ningún detalle puede ser cambiado sin invalidar la firma digital. Eventualmente, los certificados digitales podrían ser construidos dentro de Web browsers y carteras virtuales

certificación / certificated
- **R.A.** Acción y efecto de hacer cierta una cosa, por medio de un instrumento público.

cheque / check
- **R.A.** Mandato escrito de pago, para cobrar cantidad determinada de los fondos que quien lo expide tiene disponibles en un banco.
- **Fin.** Cheque, orden o mandato de pago incorporado a un título de crédito, que permite al librador disponer, en favor de una determinada persona o del simple portador del título, de fondos que tenga disponibles en un banco. El cheque deberá contener: la denominación de cheque inserta en el texto del mismo título, al mandato puro y simple de pagar una suma determinada de dinero, el nombre del que debe pagar(al que se denomina librado), que por fuerza ha de ser un banco, el lugar de pago, la fecha y el lugar de la emisión del cheque, la firma del que lo expide, al que se le denomina librador.
- **Fin.** Título de crédito expedido a cargo de una institución de crédito, por quien esté autorizado por ella al efecto, conteniendo la orden incondicional de pagar una suma de dinero a la vista, al portador o a la orden de una persona determinada. Orden de pago dirigida a un banco, contra los fondos poseídos por el girador. La orden de pago puede ser nominativa o al portador.

cifrado / cipher
- **Inf.** Algoritmo de encripción. El cifrado puede ser simétrico o de llave pública, pueden ser transfendos como flujo de datos o dividido en bloques.

cliente / customer
- **R.A.** Persona que compra en un establecimiento o utiliza sus servicios.
  Inf. Corresponde a la denominación de un programa computacional (software) utilizado para contactar y obtener datos desde un software Servidor que se encuentra generalmente en otro computador. En la arquitectura cliente/servidor, existen un software cliente corriendo en un computador y un software servidor corriendo en otro computador que interactúan entre ellos y ejecutan alguna tarea específica.

comercio / commerce
- **R.A.** Negociación que se hace comprando y vendiendo o permutando géneros o mercancías.

comercio electrónico (e-commerce) / electronic commerce
- **Inf.** En inglés denominado "E-Commerce" Es la compraventa e intercambio de bienes y servicios a través de Internet, habitualmente con el soporte de plataformas y protocolos estandarizados. Dicha acción se desarrolla sin existir un contacto presencial entre ambas partes. Actualmente está comenzando a despuntar el Comercio Electrónico.

comprador / buyer
- Persona que adquiere un bien o servicio, con una persona que los vende.

corredor / broker
- **R.A.** Funcionario cuyo oficio es intervenir, con carácter de notario, si está colegiado, en la negociación de letras u otros valores endosables, en los contratos de compraventa de efectos comerciales y en los seguros.
  Fin. Individuo legalmente autorizado para realizar actividades de compraventa de valores realizadas en la bolsa de valores a favor de terceros.

correo electrónico (e-mail) / electronic mail
- **Inf.** Programa que permite mandar y recibir mensajes, intercambiar imágenes, archivos de texto, audio y video, entre usuarios de una o distintas redes computacionales.

crédito / credit
- **R.A.** Cantidad de dinero, o cosa equivalente que alguien debe a una persona o entidad y que el acreedor tiene derecho de exigir y cobrar.
- **Fin.** Crédito, en comercio y finanzas, término utilizado para referirse a las transacciones que implican una transferencia de dinero que debe devolverse

transcurrido cierto tiempo. Por tanto, el que transfiere el dinero se convierte en acreedor y el que lo recibe en deudor; los términos crédito y deuda reflejan pues una misma transacción desde dos puntos de vista contrapuestos. Crédito, Clases de:
Los principales tipos de crédito son los siguientes: créditos comerciales, que son los que unos fabricantes conceden a otros para financiar la producción y distribución de bienes; créditos a la inversión, demandados por las empresas para financiar la adquisición de bienes de equipo, las cuales también pueden financiar estas inversiones emitiendo bonos, pagarés de empresas y otros instrumentos financieros que, por lo tanto, constituyen un crédito que recibe la empresa; créditos bancarios, que son los que concede un banco y entre los que se podrían incluir los préstamos; créditos al consumo o créditos personales, que permiten a los individuos comprar bienes y pagarlos a plazos; créditos hipotecarios, destinados a la compra de bienes inmuebles, garantizando la devolución del crédito con el bien inmueble adquirido; créditos gubernamentales que reciben los gobiernos (centrales, regionales o locales) al emitir deuda pública; y, por último, créditos internacionales, que son los que concede un gobierno a otro, o una institución internacional a un gobierno, como es el caso de los créditos que concede el Banco Internacional para la Reconstrucción y el Desarrollo, o Banco Mundial.
- **Fin.** Cambio de una prestación presente por una contraprestación futura, es decir, se trata de un cambio en el que una de las partes entrega de inmediato un bien o servicio y el pago correspondiente más los intereses devengados los reciben más tarde.

criptografía / criptography
- **R.A.** Arte de escribir con clave secreta o de un modo enigmático.
- **Inf.** Consiste en "ocultar" o cifrar o dificultar por parte del Emisor un mensaje, para que sólo las personas que conozcan la clave o proceso para "descifrarlo", puedan acceder al mismo y leerlo.

criptografía de llave pública
- **Inf.** Un campo de la criptografía inventada en 1976 por Whitfield Diffie y Martin Hellman. La criptografía de llave pública depende de un par de llaves inversas. La información encriptada con una llave puede sólo ser decriptada con la otra. Esta llave pública provee a un usuario la facilidad para encriptar y decriptar datos o texto.

criptografía de llave secreta
- **Inf.** La criptografía de llave secreta usa la misma llave para cifrar y descifrar. DES, IDEA, RC2 y RC4 son ejemplos de este tipo de cifrados.

cuenta / account
- **R.A.** Cuenta corriente en la que el banco o banquero autoriza al titular para disponer, sobre su saldo favorable, de mayor cantidad que suele fijarse, con exigencia de garantía o sin ella.

cyber
- **Inf.** Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.). Su origen es la palabra griega "cibernao", que significa "pilotar una nave".

Cybercash
- **Inf.** Es una compañía que desarrolla uno de los primeros sistemas de pago para Internet. Ellos dan al consumidor una cartera. Los vendedores online usan el software de Cybercash para recibir ordenes desde compradores con la cartera. Las ordenes son enviadas a través del servidos Cybercash a las redes bancarias para la verificación de la tarjeta de crédito.

datos / data
R.A./Inf. Representación de una información de manera adecuada para su tratamiento por una computadora

- **Inf.** Unidad mínima entre las que componen una información. Es una palabra latina que significa "lo que se da".

denegación del servicio (DoS) / denial of service

- **Inf.** En Internet, un DoS o ataque de denegación de servicio (no confundir con DOS, Disk Operating System, con O mayúscula) es un incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red. En los peores casos, por ejemplo, un sitio web accedido por millones de personas puede verse forzado temporalmente a cesar de operar. Un ataque de denegación de servicio puede también destruir programas y ficheros de un sistema informático. Aunque normalmente es realizado de forma intencionada y maliciosa, este tipo de ataques puede también ocurrir de forma accidental algunas veces. Si bien no suele producirse robo de información estos ataques pueden costar mucho tiempo y dinero a la persona u organización afectada.

DES (Data Encriptyon Standard / Estándar de Encripción de Datos)

- **Inf.** Data Encryption Standard / DES (Estándar de Cifrado de Datos): Algoritmo de cifrado de datos estandarizado por la administración de EE.UU.

desencripción / decryption

- **Inf.** Recuperación del contenido real de una información encriptada previamente.

deuda / debit

- **R.A.** Obligación que alguien tiene de pagar, satisfacer o reintegrar a otro una cosa, por lo común dinero.
- **Fin.** Deuda, en derecho, obligación que se puede hacer cumplir mediante una acción legal para el pago de dinero. En la ley modema, el término deuda no tiene un significado fijo y puede considerarse en esencia como lo que una persona le debe legalmente a otra. Sin embargo, en el derecho consuetudinario, una acción por deuda era un proceso que se emprendía con el expreso objetivo de recuperar una determinada cantidad de dinero. Si la cuantía adeudada no podía determinarse con precisión sin un juicio, el acreedor tenía que emprender otro tipo de acciones legales.
- **Fin.** Cantidad de dinero o bienes que una persona, empresa o país debe a otra y que constituyen obligaciones que se deben saldar en un plazo determinado. Por su origen la deuda puede clasificarse en interna y externa; en tanto que por su destino puede ser pública o privada.

debito / debit

- R.A. Deuda.
- **Fin.** Partida que se asienta en el "debe" de una cuenta. Deuda.
- **Fin.** En contabilidad implica cualquier cantidad que al asentarse o registrarse incrementa el saldo de un pasivo o decrementa el saldo de un activo.

dinero / cash

- **R.A.** Medio de cambio de general de aceptación, que puede ser declarado forma legal de pago, constituido por piezas metálicas acuñadas, billetes u otros instrumentos fiduciarios.
- **Fin.** Dinero, Cualquier medio de cambio generalmente aceptado para el pago de bienes y servicios y la amortización de deudas. El dinero también sirve como medida del valor para tasar el valor económico relativo de los distintos bienes y servicios. El número de unidades monetarias requeridas para comprar un bien, se denomina precio del bien.

- **Fin.** Es el equivalente de todos los bienes y servicios de una colectividad. Por su aspecto externo puede ser moneda cuando es de metal, o billete cuando es de papel. Tiene cuatro funciones: como instrumento de cambio, como medida de valor, como instrumento de capitalización y de movilización de valor, y como instrumento de liberación de deudas y obligaciones.

dinero digital / digital cash
- **Inf.** es un número (de alrededor de 100 dígitos) al que se le asocia cierto valor y pude ser usado como cualquier otro tipo de dinero. Este número va acompañado de la firma del dueño o de un banco.

dirección electrónica / electronic address
- **Inf.** Compuesta del nombre o número de usuario y luego el de la computadora donde se tiene cuenta (casilla de correo), según formato DNS.

dominio / domain
- **Inf.** Representa el nombre único que identifica a un sitio web dentro de Internet. El nombre de dominio siempre tiene dos o más partes separadas por puntos. La parte de la izquierda es más especifica y la de la derecha más general. (ejemplo: vía red.cl, identifica a la máquina vía red dentro del dominio cl que es Chile).

E
- **Inf.** Además de ser una letra del abecedario, en Internet la "e" se utiliza, seguida de un guión, como abreviatura de "electronic", a modo de prefijo de numerosas palabras para indicar que nos estamos refiriendo a la versión electrónica de un determinado concepto; asi, por ejemplo, "e-business" es la abreviatura de "negocio electrónico".

Ecash
- **Inf** Moneda electrónica que substituye al dinero en las transacciones online, incluyendo la seguridad de las tarjetas de crédito, cheques electrónicos y monedas digitales.

EDI (Electronic Data Interchange / Intercambio Electrónico de datos)
- **Inf.** Es Intercambio Electrónico de Datos. EDI provee formatos electrónicos los cuales permiten un intercambio de datos de negocios entre compañías sobre la red.

emisor / issuer
- **R.A.** Persona que enuncia el mensaje en un acto de comunicación.

encripción / encryption
- **Inf.** Del gr. kriptós, oculto, neologismo que significa "transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar". Lo que en español siempre se habia llamado cifrar, a cuya definición en el DRAE pertenece lo anterior. En Internet, se aplica a los mensajes o archivos que se envían por correo electrónico.
- **Inf.** Consiste en la codificación de un texto o información, para evitar que sea visto por el resto de personas. Para acceder al mismo es necesario un código de decodificación. Con ello se busca seguridad y privacidad.
- **Inf.** El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

factura / bill
- **R.A.** Cuenta detallada de cada una de estas operaciones con expresión de número, peso o medida, calidad y valor o precio.
- **R.A.** Relación de los objetos o artículos comprendidos en una venta, remesa u otra operación de comercio.
- **Fin.** Documento que se expide para hacer constar una venta, en el que aparece la fecha de la operación, el nombre del comprador, del vendedor, las condiciones convenidas, la cantidad, descripción, precio e importe total de lo vendido.

Se hace constar también el número de la factura, el nombre del comisionista o agente vendedor, la forma del embarque y otros datos adicionales relativos a cada operación.

firma digital / digital signature

- **Inf.** Información cifrada que identifica al autor de un documento electrónico y auténtica que es quien dice ser.
- **Inf.** Información encriptada con la llave privada de una entidad la cual es agregada al mensaje para asegurar al receptor de la autenticidad e integridad del mensaje. La firma digital provee que el mensaje fue firmado por la entidad propietaria, o con acceso a, la llave privada.

firma electrónica / electronic signature

- **Inf.** Es el proceso de verificación del usuario. Actualmente se está tratando el tema en el Congreso (en España), con el fin de regular el tema. Para autentificar el proceso existen las "Agencia de Certificación", encargadas de verificar y autentificar el proceso.

firewall / cortafuegos

- **Inf.** Es una solución hardware y/o software que permite proteger una red privada de los ataques de los hackers desde Internet.
- **Inf.** Sistema que se coloca entre una red local e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

fraude / fraud

- **R.A.** Acción contrana a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

función hash / hash function

- **Inf.** es una función de un solo sentido, resistente a colisiones que asocia una archivo o documento de longitud arbitraria a una cadena de longitud constante (se usa actualmente 160 bits de salida), las funciones hash más conocidas son: MD5, SHA1, RIPMED 160.

gateway / pasarela

- **Inf.** Es el significado técnico para cualquier hardware o software que permite traducir o convertir información entre dos protocolos distintos. También se utiliza este término para describir cualquier mecanismo que permita o provea el acceso a otro sistema (puerta de entrada a otro sistema).
- **Inf.** Hoy se utiliza el término "router" (direccionador, encaminador, enrutador) en lugar de la definición original de "gateway". Una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes. No debería confundirse con un convertidor de protocolos.

hardware

- **Inf.** Componentes físicos de una computadora, de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.

host / huésped

- **Inf.** Computadora que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. La acepción verbal (*to host*) describe el hecho de almacenar algún tipo de información en un servidor ajeno.

http

Inf. (HyperText Transport Protocol). Protocolo de Transferencia de Hipertexto. Es el protocolo que permite el intercambio de páginas en la World Wide Web. Protocolo de comunicación empleado por los servidores de WWW.

https – **Inf.** (HyperText Transport Protocol Secured). El protocolo de comunicación seguro empleado por los servidores de WWW con en clave. Esto es usado para trasporta por Internet información confidencial como el número de tarjeta de crédito.

hipertexto / hypertext
- **Inf.** Documentos en donde se puede saltar haciendo click en una palabra (link) a otra parte del documento. En el WWW se potencia este concepto, pudiendo saltar a (partes de) documentos existentes en otras máquinas de Internet.
- **Inf.** Texto hiperactivo integrado por el texto propiamente dicho, sonido, imágenes estáticas e imágenes en movimiento. Su verdadera diferencia respecto al texto a secas es que contiene enlaces.

ID / Nombre de Usuario o identificación – **Inf.** Corresponde al nombre del usuario o identificación de la persona que tiene autorización para accesar algún servicio en particular, por ejemplo: modificar su sitio web. El ID está asociado al Password y entre ambos dan acceso a la administración del espacio arrendado en el servidor.

implement – **Inf.** Vocablo en inglés. Que se utiliza para denominar cuando se está poniendo en funcionamiento un sistema.

implementar – **Inf.** Poner en funcionamiento, aplicar métodos, medidas, etc., para llevar algo a cabo.

integridad / integrity – **Inf.** se refiere a que la información no sea modificada

Internet
- **Inf.** Conjunto cualquiera (aislado) de computadoras conectadas. (Con minúscula).
- **Inf.** Un conglomerado internacional de redes computacionales que conecta instituciones comerciales, gubernamentales y académicas. (Con mayúsculas).
- **Inf.** Es una red de cómputo a nivel mundial que agrupa a distintos tipos de redes usando un mismo protocolo de comunicación. Los usuarios en Internet pueden compartir datos, recursos y servicios. Internet se apoya en el conjunto de protocolos TCP/IP De forma más específica, Internet es la WAN más grande que hay en el planeta, e incluye decenas de MAN's y miles de LAN's. Las computadoras que lo integran van desde modestos equipos personales, minicomputadoras, estaciones de trabajo, mainframes hasta supercomputadoras. Internet no tiene una autoridad central, es descentralizada. Cada red mantiene su independencia y se une cooperativamente al resto respetando una serie de normas de interconexión. El organismo que se encarga de regular, establecer estándares, administrar y hacer operacional a Internet es la ISOC (Internet Society).

información / information
- **Inf.** Conjunto de datos codificados que se integran en un contenido mental. La "información" se concreta a partir de un proceso de significación en una mente. La información, como contenido de la realidad circundante, reduce la incertidumbre que tenemos hacia ese entorno y, en este sentido, genera conocimiento cuando se extiende en el tiempo.
- **Inf.** Agregación de datos que tiene un significado específico más allá de cada uno de éstos. Un ejemplo: 1, 9, 8 y 7 son datos; 1987 es una información. La información ha sido siempre un recurso muy valioso, revalorizado hoy más aun por el desarrollo y la expansión de las Tecnologías de Información y de Comunicaciones.

intruso – **R.A.** Que se ha introducido sin derecho

IP (Internet Protocol / Protocolo de Internet) – **Inf.** Es un número único a nivel mundial separado en cuatro partes por puntos. Cada uno de estos números puede ser desde 0 hasta 255. Un ejemplo de número IP es:
200.27.90.2
El orden de jerarquía de los números es de izquierda a derecha, donde el primer número es el más general y así sucesivamente hacia la izquierda.
Cada máquina que está conectada a Internet tiene su propio número IP y es único en todo el mundo.

key / clave, llave – **Inf.** En castellano "Clave". Es un código de signos empleado para transmisión de mensajes secretos.

llave privada / private key – **Inf.** Una llave matemática (guardada en secreta por el propietario) el cual es usado para crear firmas digitales, o decriptar mensajes o archivos.

llave pública / public key – **Inf.** Llave matemática que es disponible públicamente. Es usada para verificar firmas que fueron creadas con su correspondiente llave privada. Las llaves públicas son también usadas para encriptar mensajes o archivos los cuales pueden solamente ser decriptados con su correspondiente llave secreta.

mensaje / message – **R.A.** Recado que envía una persona a otra.

micropago / micropayment – **Inf.** El comercio electrónico inicio con compras pagadas por tarjeta de crédito, este nuevo sistema te permite compras en un rango de una fracción de un centavo hasta 5 us.

monedas digitales / digital coins – **Inf.** Las monedas digitales pueden ser bajadas al disco duro del usuario desde una cuenta en el banco. Cuando el comprador quiere pagar, una cartera se muestra en su pantalla, las monedas son transferidas online desde la computadora del comparador al servidor del vendedor. El vendedor deposita las monedas en su banco

monedero electrónico / electronic purse – **Inf.** Usando la tecnología de una smart card en un monedero electrónico es creada con el efectivo almacenado electrónicamente en un microchip, creando una tarjeta de prepago la cual puede entonces ser usada para comprar bienes y servicios. Este permite asegurar el valor de la transferencia a otro monedero electrónico.

negocios electrónicos (e-business) – **Inf.** Cualquier tipo de actividad empresarial realizada a través de las tecnologías de información y comunicaciones.

Netcheque – **Inf.** Un sistema de pago electrónico en cheque que puede ser enviado por mail. Cuando el cheque es depositado, como un cheque de papel, los fondos son trasladados desde la cuenta del emisor del cheque a la cuenta del receptor. Tiene un mecanismo de firma digital.

no repudio / no repudiation – **Inf.** se refiere a no poder negar la autoría de un mensaje o de una transacción.

offline – **Inf.** Fuera de línea. Es todo aquello que se realiza sin estar conectado a Internet.

online – **Inf.** Conectado a Internet.

pagador / payer – **R.A.** Persona que paga.

página web / web page - **Inf.** Es el resultado en hipertexto e hipermedia que proporciona un visualizador de World Wide Web después de obtener la información solicitada.

pago / pay - **R.A.** Entrega de un dinero o especie que se debe.

pedido, orden / order - **R.A.** Encargo hecho a un fabricante o vendedor, de géneros su tráfico.

privacidad / privacy - **Inf.** se refiere a tener control en el acceso de la información y solo permitirlo a personas autorizadas.

protocolo / protocol - **Inf.** Conjunto de normas que gobiernan el intercambio de información entre computadoras.
- **Inf.** Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

recibo - **R.A.** Escrito o resguardo firmado en que se declara haber recibido dinero u otra cosa.

red / net, network - **Inf.** Agrupación tanto de equipos como de programas que comparten recursos entre sí, observando "reglas de comportamiento" a partir del uso de un lenguaje y medios de transmisión comunes, sin importar -en lo esencial- la naturaleza de cada elemento dentro de la red.

reembolso - **R.A.** Acción o efecto de volver una cantidad a poder del que la había desembolsado.
- **Fin.** Sustitución de un antiguo pasivo por medio de la venta de una nueva emisión.

RSA (Rivest, Shamir, Adleman) - **Inf.** Es un sistema de encripción basado en criptografía de llave pública que significa que cada usuario tiene sus 2 llaves digitales – una para encriptar información, y la otra para decriptarla. Provee autenticación del emisor y del receptor.

seguridad / security - **R.A.** Se aplica también a ciertos mecanismos que aseguran algún buen funcionamiento, precaviendo que este falle, se frustre o se violente.
- **Inf.** Mecanismos de control que evitan el uso no autorizado de recursos.

servidor / server - **Inf.** Es una computadora conectada permanentemente a Internet, la cual está dispuesta para servir a cuantos clientes le hagan alguna petición. Del mismo modo que un mesero en un restaurante sirve lo que los clientes piden, del mismo modo el servidor. Existen servidores de correo electrónico o e-mail, de WWW y FTP. Los servidores de Netfactor son múltiples pues ejercen estas tres últimas opciones. Computadora que presta servicios a muchos usuarios. Provee información y programas a Internet.
- **Inf.** Es un computador o un software que provee una clase especial de servicio al software clientes que están corriendo en otros computadores y que lo accesan para realizar una función determinada. Un computador funcionando como servidor puede tener operando software de servidores para prestar servicios, por ejemplo: servidor de WWW, servidor de Mail, etc.

sesión remota / remote session **Inf.** Uso de los recursos de una computadora desde una terminal que no precisamente se encuentra cercana a ella.

SET (Secure Electronic Transaction / Transacciones Electrónicas Seguras)

- **Inf.** Corresponde a las siglas "Secure Electronic Transaction". Es un sistema que garantiza la seguridad en las transacciones electrónicas. Es empleado por el Comercio Electrónico y por entidades bancarias y financieras.
- **Inf.** Autentica las compras con tarjeta de crédito en la red. Las firmas digitales son usadas por todas las partes que participan en este sistema. La transacción de información es encriptada usando encripción RSA de 1024 bits.

site, web site / sitio web

- **Inf.** Término comúnmente utilizado en Internet para denominar el lugar virtual de una empresa u organización que tiene por medio de un servidor de WWW.

sistema / system

- **R.A.** Conjunto de cosas que ordenadamente relacionadas entre sí contribuyen a determinado objeto.
- **Inf.** Conjunto de procesos o elementos interconectados e interdependientes que forman un todo complejo.

smart card / tarjeta inteligente

- **Inf.** Es una tarjeta de crédito de plástico con un chip integrado. El chip puede ser recargado con fondos. El valor almacenado en las tarjetas es deducido conforme la transacción sea hecha. La tarjeta también puede almacenar información de identificación, detalles de salud de la persona, información de seguridad y otro tipo de servicios.

solicitud / request

- **R.A.** Memorial en que se solicita algo.

software

- **Inf.** Programas o elementos lógicos que hacen funcionar una computadora o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos de la computadora o la red.

SSL (Secure Socket Layer)

- **Inf.** Corresponde a las Siglas " Secure Socket Layer". Consiste en la encriptación de la información para enviarla a un destinatario. Es empleado en el comercio electrónico para enviar datos confidenciales.

tarjeta / card

- **R.A.** Adorno plano y oblongo que se figura sobrepuesto a un miembro arquitectónico, y que lleva por lo común inscripciones o emblemas.

tarjetahabiente / cardholder

- Tenedor de una cuenta de tarjeta de crédito válida y usuario de un software browser certificado reteniendo un certificado de soporte para el comercio electrónico.

tarjeta de débito / debt card

- **Inf.** Es substituto del efectivo para consumidores. Se parecen a las tarjetas de crédito, pero no proveen el crédito. Las cantidades para las compras son inmediatamente deducidas del balance del banco del usuario.

TCP/IP (Transfer Control Protocol / Internet Protocol)

Inf. Protocolo de Control de Transmisión/Protocolo Internet. Protocolos fundamentales de Internet que establecen un método por el cual son transmitidos datos a través de Internet entre dos computadoras.

tenedor / payee

R.A. Persona que tiene o posee un algo, especialmente la que posee legítimamente alguna letra de cambio u otro valor endosable.

texto cifrado / ciphertext

- **Inf.** Datos encriptados.

texto en claro / plaintext

- **Inf.** Datos sin ser encriptados.

tienda virtual

- **Inf.** Es un sitio Web estructurado con una página inicial, listas de precios, información sobre pagos y formas de envío, páginas sobre anuncios especiales,

noticias, un formulario para las órdenes, políticas de la empresa y preguntas comunes.
El modelo de negocios de una tienda virtual está basado en un inventario limitado y en una estructura de costos que están asociados generalmente con tiendas tradicionales o compañías de correos.

transacción / transaction
- **Fin.** Trato, convenio, negocio.

valor / value
- **R.A.** Títulos representativos de participación en haberes de sociedades, de cantidades prestadas, de mercaderías, de fondos pecuniarios o de servicios que son materias de operaciones mercantiles.
- **Fin.** Es el grado de utilidad o aptitud de las cosas, para satisfacer las necesidades o proporcionar bienestar o deleite. Equivalencia de una cosa a otra. En plural, títulos representativos de participaciones o haberes de sociedades, de cantidades prestadas, de mercancías, de fondos pecuniarios o de servicios que son materia de operaciones mercantiles.

vendedor / merchant
- **R.A.** Que expone u ofrece al público los géneros o mercancías para el que las quiera comprar.
- **Inf.** Persona que ofrece bienes, servicios, y/u otra información que acepta pagos para esos artículos electrónicamente. El vendedor quizá también provee venta de servicios electrónicos y/o entrega electrónica de artículos para venta.

venta / sale
- **R.A.** Acción y efecto de exponer u ofrece al público los géneros o mercancías para el que las quiera comprar.
- **Fin.** Acción mediante la cual uno de los contratantes se obliga a transferir la propiedad de una cosa o de un derecho a otro que a su vez se obliga a pagar por ello un precio determinado en dinero.

virtual
- **Inf.** Algo que tiene existencia aparente y no real. Es un término de frecuente utilización en el mundo de las Tecnologías de la Información y de las Comunicaciones para designar a dispositivos o funciones simulados. "virtual circuit", "Virtual Private Network".

URL (Uniform Resource Locator)
- **Inf.** Localizador Universal de Recursos. Permite acceder de forma uniforme a los distintos recursos de Internet. Se utiliza profusamente en la World Wide Web. La dirección de una fuente de información. Está compuesto por cuatro partes distintas: el tipo de protocolo (http, ftp, gopher), el nombre de la máquina, la ruta del directorio y el nombre del archivo.

Web
- **Inf.** Servidor de información WWW. Se utiliza también para definir el universo WWW en su conjunto.

WWW (World Wide Web)
- **Inf.** Sistema de acceso a información distribuida en Internet mediante enlaces hipertexto.
Conjunto de información distribuida basada en hipertexto, (interfase gráfica, atractiva y amigable) para un acceso a recursos de Internet, especialmente en el ámbito comercial concebida en el CERN, Ginebra.

X.500
- **Inf.** El directorio X.500 es una base de datos distribuida que permite la consulta de datos sobre objetos del mundo real. A través de X.500 se puede buscar información sobre personas, departamentos y organizaciones de todo el mundo. Puede proporcionar direcciones de mensajería electrónica, direcciones postales, teléfonos y números de Fax.

ABREVIATURAS Y SIGLAS

A	Adquirente
AC	Autoridad Certificadora (Certificate Authority)
ACH	Casa Automática de Aclaramiento (Automated Clearing House)
B2B	Negocio a Negocio (Business to Business)
B2C	Negocio a Consumidor (Business to Consumer)
C	Cliente/Comprador
CA	Certificate Autorithy (Autoridad Certificadora)
CARI	Collect all relevant information/Colección de toda la información relevante
DATE	Fecha / hora
DESC	Descripción de la orden/pedido
E	Emisor
E_x	Encripción
e-commerce	Comercio Electrónico (Electronic Commerce)
e-mail	Correo Electrónico (Electronic Mail)
e-bussines	Negocio Electrónico (Electronic Business)
H()	Función Hash
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
Fin.	Finanzas
FV	First Virtual
ID	Identificador
Inf.	Informática
iKP	Protocolo de Llaves en Internet (Internet Keyed Protocol)
IP	Protocolo de Internet (Internet Protocol)
ITP	Information Technology Partners/Socios de Tecnología de Información
K	Llave
Kpr	Llave Privada
Kpu	Llave Pública
PIN	Número de identificación
NONCE	Número aleatorio
NREQ	No Requisito
R.A.	Real Academia
REQ	Requisito
SALT	Número Aleatorio
SET	Secure Electronic Transaction
Sig	Firma
SM	Servidor de Monedas
SSL	Secure Socket Layer
TCP	Transfer Control Protocol
TCP/IP	Transfer Control Protocol / Internet Protocol
TID	Identificador de la Transacción
us	Doláres
V	Vendedor
VCC	Tarjeta de Crédito Virtual / Virtual Credit Card
WWW	World Wide Web

Bibliografía

BIBLIOGRAFÍA

- Anush, Anup K. E-Commerce Security: Weak Links, Best Defenses. Wiley Computer Publishing. Estados Unidos, 1998. Pp.288. ISBN: 0-471-19223-6
- O'Mahony, Donald; Perice, Michael; Tewari, Hitesh. Electronic Payment Systems. Artech House. Estados Unidos, 1997. Pp 254. ISBN: 0-89006-925-5
- Cook, David; Seller, Debora. Inice su negocio en Web. Prentice Hall. Primera edición, México, 1997. Pp. 621.
- Boizard Piwonka, Alicia; Pérez Arata, Miguel. Internet en Acción. McGraw Hill. Primera edición, Santiago, Chile, 1996. Pp. 292.
- Simon, Julio A. Tarjetas deCrédito. Abeledo-Pedot. Primera edición, Buenos Aires, Argentina, 1990. Pp. 158.
- Ambegaonkar, Prakash. Kit de Recursos de Intranet. McGraw Hill. Primera edición, España, Madrid, 1997. Pp 495.
- Drew, Grady N., Using SET for Secure Electronic Commerce. Prentice Hall. Primera edición, J. ISBN: 0-13-0099715-3
- EspasaCalpe. Diccionario de la Real Academia Española. Editorial EspasaCalpe S.A. de C.V. Vigésima Primera edición, Madrid, 1992. Tomo I, Tomo II. pp. 1077, pp. 1077-2133
- Tejera, Héctor G. Diccionario Enciclopédico de Informática. Grupo editorial Iberoámerica, S.A. de C.V. Primera edición, México, 1994. Tomo I, Tomo II. pp. 682, pp. 683-1377
- Cultural. Diccionario Enciclopédico Universal. Cultural, S.A. Primera edición, Madrid, España, 1999
- Corominas, Joan. Breve Diccionario Etimológico de la Lengua Castellana. Gredos. Tercera edición, Madrid, España, 1998. pp. 627
- Valbuena. Novisimo Diccionario Español-Latino. Valbuena. Paris, ia ed. 1897. Gamier hermanos libreros editores.
- Daniel, Wayne W.; Bioestadistica.;Noriega Editores; Tercera Edición, México, 1999. P.P. 878. ISBN: 968-18-5196-X
- Ayala Martínez, Adriana. Mejoramiento de Transacciones y obtención de Servicios haciendo uso de Tarjetas Inteligentes.
- Macías Pérez, Patricia. Metodología y herramientas para mantener y crear una Tienda Virtual en el Web.

HEMEROGRAFÍA

- Comercio Electrónico en Latinoamérica.
- Luna, David. Red. Monedero Electrónico: ¿El Dinero del Futuro?. Agosto,1999. Num. 107
- Red. Comercio Electrónico. Con un paso Adelante. Diciembre,1999. Num. 111

- Flohr,Udo. BYTE MEXICO. Dinero Electrónico. Junio, 1999. Num. 101

URL's

- http://e-comm.pcwebopedia.com/TERM/s/security.html
- http://www.cybercash.com
- http://web.mit.edu/reagle/www./commerce/compete/final.htm
- http://cism.bus.utexas.edu/works/articles/cyberpayments.html
- http://www.cbintel.com/nu/fraudbanking.htm
- http://www.fraud.org/telemarketing/teleset.htm
- http://www.niksula.cs.hut.fi/~ronnys/fv.html
- http://www.cis.ohio-state.edu/htbin/rfc/rfc1898.html
- http://home.netscape.com/eng/security/SSL_2.html
- http://developer.netscape.com/docs/manual/security/sslin/contents.htm
- http://home.netscape.com/eng/ssl3/draft302.txt
- http://developer.netscape.com/tech/security/ssl3/howitworks.html
- http://www.terisa.com/shttp/current.txt
- http://activex.adsp.or.jp/Japanese/Specs/pct.htm
- http://www.dat.etsit.upm.es/~mmonjas/cripto/08.html
- http://www.timagazine.net/magazine/0497/firmas.cfm
- http://www.cs.bris.ac.uk/~cooper/crypto.html
- http://www.fstc.org/projects/echeck/echeck2.html
- http://www.ideal.es/cibernauta/
- http://www.kriptopolis.com/criptograma/cg.html
- http://activex.adsp.or.jp/Japanese/Specs/pct.htm
- http://www.cisat.jmu.edu/common/coursedocs/CS685netsecnew/Networks/WebSecurity/web_security.html
- http://www.eed.usv.ro/misc/doc/prog/windows/ActiveX/ch8.htm
- http://emision.uson.mx/detodounpoco/glosario.htm
- http://www.viared.cl/club/glosario.htm
- http://www.banregio.com/glosario.htm
- http://www.shcp.sse.gob.mx/cuenta_publica/Glosario/glosario.htm
- http://www.fullweb.cl/glosario_1.html
- http://www.ucm.es/info/rfiscal/glosario.htm
- http://www.chasque.apc.org/lvx/glosario.htm
- http://www.cyberkyosco.com/glosario/index.htm
- http://www.ati.es/PUBLICACIONES/novatica/glointv2.html
- http://www.atlas-iap.es/~pepcardo/glosario.htm
- http://www.boldgold.com/resources/ecommerce/glossary.html
- http://www2.vnu.co.uk/e_com/e_07_01.htm
- http://www.seas.gwu.edu/~cs701/slides/lecture7/index.htm
- http://www.cbintel.com/nu/fraudbanking.htm
- http://www.fraud.org/telemarketing/teleset.htm
- http://exodus.dcaa.unam.mx/publica/tarjeta_inteligente/principal.html
- http://www.visa.com.mx/#
- http://www.arrakis.es/~corpotec/tarjetas.html
- http://www.upm.es/informacion/carneupm/htdocs/infgen1.html
- http://www.counterpane.com/smart-card-threats.html
- http://www.kriptopolis.com/criptograma/0012_4.html