Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

LLAVE PÚBLICA EN TARJETA INTELIGENTE

Luis Roberto Santizo Alva

Asesorado por: Ing. Rodrigo Céspedes Castro

GUATEMALA, ABRIL DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

LLAVE PÚBLICA EN TARJETA INTELIGENTE

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA

FACULTAD DE INGENIERÍA

POR

LUIS ROBERTO SANTIZO ALVA

Asesorado por: Ing. Rodrigo Céspedes Castro

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, ABRIL DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Ing. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Carlos Humberto Pérez Rodríguez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Bayron Wosbely López López
EXAMINADOR	Ing. José Ricardo Morales Prado
EXAMINADOR	Ing. César Augusto Fernández Cáceres
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

LLAVE PÚBLICA EN TARJETA INTELIGENTE

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha enero de 2003.

_____

Luis Roberto Santizo Alva

Guatemala, febrero de 2005

Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador de Privados y Revisión de Tesis
Escuela de Ciencias y Sistemas

Estimado Ingeniero:

Por medio de la presente, me permito informarle que he asesorado el trabajo de graduación titulado: LLAVE PÚBLICA EN TARJETA INTELIGENTE, elaborado por la estudiante Luis Roberto Santizo Alva, a mi juicio el mismo cumple con los objetivos propuestos para su desarrollo.

Agradeciéndole de antemano la atención que le preste a la presente, me suscribo de usted,

Atentamente,

Rodrigo Céspedes Castro
Ingeniero en Ciencias y Sistemas
Asesor

El Director de la carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor, con el visto bueno del revisor de tesis y del licenciado en Letras, al trabajo de graduación titulado **LLAVE PÚBLICA EN TARJETA INTELIGENTE,** presentado por el estudiante **Luis Roberto Santizo Alva**, aprueba el presente trabajo y solicita la autorización del mismo.

ID Y ENSEÑAD A TODOS

Ing. Luis Alberto Vettorazzi España

DIRECTOR

Ingeniería en Ciencias y Sistemas

Guatemala, abril de 2005

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **LLAVE PÚBLICA EN TARJETA INTELIGENTE,** presentado por el estudiante universitario **Luis Roberto Santizo Alva** procede a la autorización para la impresión del mismo.

IMPRÍMASE:

Ing. Sydney Alexander Samuels Milsons

DECANO

Guatemala, abril de 2005

DEDICATORIA A

A Dios	A Él la gloria y la honra, por los siglos de los siglos, Amén.
A mis padres	José Luis Santizo Berdúo y Liliam Elizabeth Alva Meza de Santizo. Que este triunfo sea una pequeña recompensa a todo el esfuerzo que hicieron y el apoyo que me brindaron.
A mis abuelos	Marcos Santizo Alvarez (Q.E.D.), Jesús Berdúo Jerónimo (Q.E.D.), Julio Rene Alva G. (Q.E.D.), Maria Otilia Meza de Alva, sus ejemplos nos impulsan a ser mejores.
A mis hermanos	Leslie Elizabeth Santizo A. de Lantán, José Fabrice Lantán Paredes, Liliam Rosana Santizo Alva. Parte importante en mi vida y por su amor fraternal.
A mi sobrina	Natalia Estefanía Lantán Santizo, ilusión y alegría de la familia.
A mis amigos	Blanca, Iván, Mónica, Xiomara, Norma, Karla, Carlos, Siomara y todos los demás con quienes he compartido, por su apoyo y amistad.
A Guatemala	"Pequeño Paraíso" en el corazón de América.

AGRADECIMIENTOS

A Dios	Luz divina e infalible que ilumina mi vida.
A mis padres	Por el esfuerzo que hicieron para sacarme adelante.
A mi asesor	Ing. Rodrigo Céspedes, por el apoyo incondicional que me brindó.
A mis amigos	Por su amistad y comprensión en todo momento.
A mis centros de estudio	Por contribuir en mi formación académica.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

AES (*Advanced Encryption Standard*, por sus siglas en inglés, o estándar criptográfico avanzado) es la búsqueda del gobierno de EE.UU. de un sustituto para el viejo estándar DES.

ATM (*Automated Teller Machine*, por sus siglas en inglés, o cajero mecánico automatizado) Es un dispositivo que puede ponerse en un lugar público y permite al poseedor de la tarjeta realizar operaciones bancarias básicas e incluso el retiro de dinero en efectivo.

CA Autoridad de certificación. Gestiona los certificados de clave pública durante toda su vida. La función principal de una autoridad de certificación es emitir certificados vinculando la identidad de un usuario o sistema a una clave pública con una firma digital.

CE Curvas elípticas. Sistema de firmas propuestas por primera vez para ser usadas en aplicaciones criptográficas en 1985 de forma independiente por V.S.Miller y N.Koblitz.

CHIP Es un circuito integrado. Un juego de circuitos electrónicos implementado en un pedazo de material semiconductor.

Criptografía	La criptografía es la ciencia que se asegura que el mensaje esté seguro. Estudia los problemas básicos de la seguridad en la transmisión de la información por un canal inseguro. El sistema criptográfico está basado en los conceptos de autenticación, integridad, confidencialidad y no repudiación.
DES	(*Data Encryption Standard*, por sus siglas en inglés, o cifrado de datos estándar). Algoritmo de encriptación desarrollado por IBM y la Agencia Nacional de Normas Americanas.
DH	Diffie-Hellman (DH) fue el primer sistema de clave pública abiertamente publicado (es más correcto decir que DH es un mecanismo de intercambio de claves).
EEPROM	(*Electrically Erasable Programmable ROM*, por sus siglas en inglés, o programable eléctricamente borrable ROM). Memoria especial no volátil, que puede borrarse los datos y puede recargarse los nuevos datos nuevamente. En tarjeta inteligente se usa típicamente para los datos de la aplicación.
EMV	Estándar desarrollado por Europay Internacional, Master Card Internacional, y Visa Internacional, para sistemas de pago en tarjetas inteligentes.
ETSI	Instituto Europeo de Estándares de Telecomunicaciones. Define una tarjeta inteligente

	pequeña según su tamaño para encajar en los teléfonos de GSM.
GSM	Estándar para el sistema global para las comunicaciones móviles.
IC	(*Integrated circuit*, por sus siglas en inglés, o circuito integrado). Un juego de circuitos electrónicos implemetado en un pedazo de material semiconductor. Sinónimo de *Chip*.
ICC	(*Integrated circuit card*, por sus siglas en inglés, o tarjeta con circuito integrado). Tarjeta en que uno o más circuitos integrados son insertados para que realicen procesos y funciones de memoria. Es sinónimo de "Tarjeta Inteligente".
ISO	(*International Standards Organization* , por sus siglas en inglés, u Organización Internacional de Estándares). Es la federación global de organizaciones de estándares nacionales. Trabaja para asegurar que los fabricantes de *chips*, diseñadores de *software* y compañías de las tarjetas inteligentes obedezcan las mismas especificaciones.
ITSEC	Es un estándar global reconocido para la medición de productos de seguridad.
PC/SC	Especificación del grupo de trabajo PC/SC (*Personal*

	Computer / Smart Card) que construye en las especificaciones existentes EMV e ISO 7816-X, definiendo la tarjeta inteligente en una capa de abstracción de lectura / escritura.
PIN	(*Personal Identification Number*, por sus siglas en inglés, o número de identificación personal). Es un número o código que un poseedor de la tarjeta debe teclear para confirmar que él o ella es el dueño de la tarjeta.
PKI	Infraestructura de llave pública. Sistema que se basa en la utilización de una pareja de claves, una pública conocida por todos y otra privada, sólo conocida por el usuario.
Tarjeta inteligente	Tarjeta en que uno o más circuitos integrados son insertados para que realicen procesos y funciones de memoria. Sinónimo de ICC.
Triple DES	Es una versión fortalecida del algoritmo DES. Normalmente usado en el sector bancario.
RA	Una autoridad de registro (RA), proporciona el interfaz entre el usuario y la autoridad de certificación (CA).
RAM	(*Random Access Memory*, por sus siglas en inglés, o memoria de acceso aleatorio). Es una memoria volátil que la usa el microprocesador para poner datos

temporalmente.

ROM (*Read Only Memory*, por sus siglas en inglés, o memoria de sólo lectura). Es un arrea de la memoria que sólo puede ser leída.

RSA RSA representa las iniciales de los tres hombres que lo inventaron en 1977, ellos son: Ron Rivest, Adi Shamir, y Len Adleman. Las firmas RSA utilizan una clave de hasta 2048 o 4096 *bits* (dependiendo de la implementación).

SSL (*Secure Sockets Layer*, por sus siglas en inglés, o capa de enlace seguro). Es un protocolo diseñado por la Netscape Communications para habilitar encriptación, comunicaciones autenticadas por la Internet.

OBJETIVOS

General

Brindar un documento que dé los conceptos y conocimientos necesarios para la toma de decisiones en la implementación de soluciones donde se utilice la infraestructura de llave pública (PKI).

Específicos

1. Explicar los beneficios, alcances y limitaciones de una infraestructura de llave pública (PKI)

2. Mostrar las bondades de la tarjeta inteligente.

3. Dar a conocer las posibles aplicaciones y usos que puede tener la infraestructura de llave pública (PKI)

4. Mostrar a la infraestructura de llave pública en una tarjeta inteligente como una alternativa de solución a la problemática de seguridad.

5. Explicar la infraestructura de llave pública (PKI) en una tarjeta inteligente del mercado.

RESUMEN

La tarjeta inteligente es un plástico (polivinilo cloruro o PVC) similar en tamaño y otros estándares físicos a las tarjetas de crédito con uno o más microchips incorporados en ella, que almacena información en forma electrónica para que pueda ser accesada de manera fácil, segura y precisa.

La infraestructura de llave pública (PKI) se basa en la criptografía de clave pública. Ésta consiste en la utilización de una pareja de claves, una pública que es conocida por todos y una privada que es sólo conocida por el usuario a quien se le es asignada.

El presente trabajo contiene una descripción general tanto de la tarjeta inteligente, como de la infraestructura de la llave pública y muestra la forma en que pueden ser utilizadas sus bondades para obtener las funciones principales de seguridad.

El presente trabajo consta de seis capítulos. El primero presenta a la tarjeta inteligente, sus orígenes, características, clasificaciones que posee, y los estándares bajo los cuales se rige.

El segundo capítulo nos introduce los conceptos de seguridad y la ciencia que lo estudia: criptografía. Nos muestra las divisiones que tiene la criptografía y los distintos algoritmos que han sido desarrollados, los esquemas de seguridad existentes y termina con la seguridad que posee una tarjeta inteligente.

El tercer capítulo nos define la infraestructura de la llave pública (PKI), sus componentes, funcionamiento, la forma de implementarlo y sus alcances y limitaciones.

El cuarto capítulo nos da algunos ejemplos de los usos más frecuentes que actualmente se le da a la infraestructura de llave pública.

El quinto capítulo pretende demostrar los beneficios que se obtienen al utilizar una tarjeta inteligente en una infraestructura de llave pública. Muestra también las características necesarias que debe poseer la tarjeta inteligente para poder ser usadas en PKI.

El último capítulo hace una propuesta de la utilización de tarjeta inteligente en una infraestructura de llave pública. Describe los componentes que poseería el sistema y describe detalladamente el funcionamiento que tendría la autenticación.

INTRODUCCION

El origen de la tarjeta inteligente se encuentra en Europa a comienzos de los años 70. Dicha tarjeta es similar a las bancarias o a las de crédito, pero capaz de incorporar un dispositivo programable.

El objetivo de la tarjeta inteligente es ofrecer a los clientes un servicio con muchos más beneficios que le facilite su desenvolvimiento diario ofreciendo tres funciones principales que son: almacenamiento de datos, seguridad de la información y procesamiento de datos.

Una infraestructura de clave pública (PKI) es una combinación de productos de *hardware* y *software*, políticas y procedimientos. La criptografía de llave pública se basa en identidades digitales conocidas como certificados digitales.

El problema de un ambiente PKI es bastante similar a cualquier otro sistema de criptografía: el almacenamiento importante seguro, es aquí donde entra la tarjeta inteligente como un medio para guardar las llaves pública y privada. Además, por sus características, ofrece beneficios adicionales como portabilidad, identidad y autenticación del usuario, y otros, se convierte en una solución viable en aplicaciones PKI.

En el presente trabajo encontrará los conceptos necesarios para la toma de decisiones en sistemas de infraestructura de llave pública y propondremos la tarjeta inteligente como la bóveda del banco para guardar la llave pública y privada.

1. TARJETAS INTELIGENTES

1.1 Introducción a tarjetas inteligentes

1.1.1 Evolución de las tarjetas magnéticas

A finales de los años 60 se desarrolló la tarjeta magnética convencional, con el objetivo de identificar a un cliente de forma sencilla y así facilitar la facturación, embarque de pasajeros, transacciones financieras rápidas, etc.

Actualmente, se utilizan y producen alrededor de 1400 millones de tarjetas magnéticas en todo el mundo, una tarjeta magnética tiene una vida útil de 16 meses, dándole un uso frecuente.

La tarjeta de banda magnética evolucionó de la tarjeta de identificación plástica, la cual no posee ninguna propiedad electrónica y funciona solamente, como su nombre lo indica, como un mecanismo de identificación. Estas tarjetas son rectángulos plásticos que miden 86 x 55 mm, con un espesor de 0.8mm. El material plástico es el polivinilo cloruro o PVC, que es mucho más durable que el papel o el cartón.

La tarjeta de banda magnética, tan familiar en la mayoría de personas en las aplicaciones de tarjeta de crédito, posee las características siguientes:

- Tiene un tamaño similar, forma, peso y dimensiones como la tarjeta plástica de identificación. Esto debido a que el Instituto Nacional de Estándares Americanos (ANSI) y la Organización de Estándares Internacionales (ISO) especifica ambas.

- Tiene capacidad limitada; simplemente es un almacén de información, aproximadamente 225 caracteres utilizables en sus 3 huellas que se usan hoy en día: una huella es alfanumérica y dos numéricas.

Debido a que la tarjeta magnética fue diseñada para dar solución a problemas que surgieron hacer más de 25 años y que están ligadas a tecnología de entonces (dependencia de ordenadores centrales y grandes redes dedicadas), no ofrece soluciones para los nuevos mercados y servicios que aparecen: televisión interactiva, telefonía digital, etc. Además, la tarjeta magnética es un elemento pasivo, que ofrece muy baja densidad de datos, baja fiabilidad y poca o ninguna seguridad en la información que lleva.

1.1.2 Historia de la tarjeta inteligente

El origen de la tarjeta inteligente se encuentra en Europa a comienzos de los años 70. Dicha tarjeta es similar a las bancarias o a las de crédito, pero capaz de incorporar un dispositivo programable. A finales de los 80 se dispone ya de *chips* suficientemente pequeños, pero con unas capacidades de memoria muy reducidas.

Es a principios de los 90 cuando las tarjetas inteligentes inician su despegue al empezar la telefonía móvil GSM (Sistema Global de Telecomunicación Móvil), inicialmente con tarjetas con 1K de memoria. GSM es un estándar Europeo para teléfonos celulares digitales que se ha adaptado ampliamente a lo largo del mundo. Se empezó directamente con GSM Fase 2 en septiembre de 1995, empleando tarjetas con 8K de memoria.

A finales de 1997 aparecieron las tarjetas de 16K, algunas de las cuales ya implementaban GSM Fase 2+ con SIM. Bajo el estándar ETSI, los teléfonos de GSM contienen un SIM, esto no es más que una tarjeta inteligente que identifica al

suscriptor individual, contiene el identificador del suscriptor, la información de seguridad y memoria para un directorio personal de números que le permiten llamar desde cualquier dispositivo GSM. A lo largo de 1999 aparecen diferentes tarjetas Java, aunque no son compatibles entre sí, y a finales del mismo año, las tarjetas de 32K.

En los últimos años hemos visto evolucionar el sector de las tarjetas inteligentes desde el momento en que un circuito integrado fue incluido en ellas. En el campo del monedero electrónico se inicia el despegue en 1997, con la aparición del monedero VisaCash, versión propietaria implementada por Visa España. Hasta finales de 1999 salen al mercado de forma masiva tarjetas sin contacto.

Los datos que se enumeran a continuación forman parte de la historia de las tarjetas inteligentes:

- 1970 el Dr. Kunitaka Arimura de Japón presentó la primero y única patente sobre el concepto de tarjeta inteligente.

- 1974 el Señor Roland Moreno de Francia patento la tarjeta original con circuito integrado.

- 1979 Motorola desarrolla el primer espacio seguro en *chip* micro controlado para uso en los bancos de Francia.

- 1984. Presentan pruebas para tarjetas con *chip* para ATM bancarios con excelente conducta.

- 1986, en marzo, 14,000 tarjetas equipadas con el CP8 de Bull fueron distribuidos de Bank of Virginia y Maryland National Bank. 50,000 tarjetas de

Casio son distribuidas a clientes del First National Palm Beach Bank y del Mall Bank.

- 1987. Primera aplicación implementada a gran escala con tarjeta inteligente en los Estados Unidos con el U.S. Department of Agriculture's en conjunto con Peanut Marketing Card.

- 1991. Primera transferencia de beneficio electrónico con tarjeta inteligente, proyecto lanzado por el Wyoming Special Supplemental Nutrition, programa para mujeres, infantes y jóvenes.

- 1994. Europay, Master Card y Visa (EMV) unidos publicaron las especificaciones para una tarjeta inteligente para bancos global.

- 1996. En las Olimpiadas de Atlanta, Visa Cash llegó a sumas superiores a 1.5 millones en transacciones.

- 1996. Master Card y Visa comienzan a patrocinar y trabajar para resolver los problemas de interoperabilidad con tarjetas inteligentes. Dos diferentes soluciones de tarjetas fueron desarrolladas, Java Card por Visa y Multi Aplication Operating Systems (Multos) por MasterCard.

- 1998. En septiembre de este año, el U.S. Government's General Services Administration y la United States Navy unen esfuerzos e implementan nueve aplicaciones para sistemas de tarjeta inteligente y soluciones de manejo de tarjeta en el Smart Card Technology Center en Washington, DC. El Technology Center's primeramente propuso esto para demostrar y evaluar la integración del Multi-Aplicación de Tarjeta inteligente con otros tipos de tecnología, escaparate de sistemas disponibles para uso en el Federal Government.

- 1998. Microsoft anunció un nuevo Windows, sistema operativo que soporta tarjeta inteligente.

- 1998. Francia comienza un piloto con tarjeta inteligente sanitaria para 50 millones de ciudadanos.

- 1999. El U.S. Government's General Services Administration estubo involucrado en el proyecto Smart Access Common ID (SACI). En el programa SACI establecería el vehículo de contacto para uso de todos los agentes federales para adquirir un estándar, tarjeta de identificación de empleados ínter operable, de uno o más vendedores, capaz de proveer acceso lógico y físico (sistema / redes) para todos los empleados federales.

- 1999. El United States Government (General Services Administration) comienza un piloto con multi-aplicación sobre Java Card en Washington, DC, en el área metropolitana.

1.2 Definición de tarjetas inteligentes

Existen varias formas de referirse a una tarjeta inteligente, la más común en documentos técnicos es ICC (*Integrated Circuit(s) Card*) o tarjeta de circuito integrado, pero es más conocida comercialmente como tarjeta inteligente. En el presente trabajo nos referiremos a ella simplemente como "tarjeta inteligente".

El estándar EMV (se expondrá al final del capítulo) define a la tarjeta inteligente de la siguiente forma: "Tarjeta en que uno o más circuitos integrados son insertados para que realicen procesos y funciones de memoria."

Para dejar en claro lo que es una tarjeta inteligente, diremos que: “es el resultado lógico del desarrollo de la microelectrónica y la informática. La tarjeta inteligente es un plástico (polivinilo cloruro o PVC) similar en tamaño y otros estándares físicos a las tarjetas de crédito con uno o más microchips incorporados en ella que almacena información en forma electrónica para que pueda ser accesada de manera fácil, segura y precisa.”

Una tarjeta inteligente contiene un microprocesador de 8 Bytes como mínimo con su CPU, su RAM y su ROM, su forma de almacenamiento puede ser EPROM o EEPROM, el programa ROM consta de un sistema operativo que maneja la asignación de almacenamiento de la memoria, la protección de accesos y maneja las comunicaciones.

El objetivo de la tarjeta inteligente es ofrecer a los clientes un servicio con muchos más beneficios que le facilite su desenvolvimiento diario.

La tarjeta inteligente surge de la evolución de la tarjeta de plástico convencional y su combinación con un circuito integrado ofreciendo así tres nuevos elementos que vinieron a favorecer la utilización generalizada. Estos elementos son:

Miniaturización

Las densidades de integración de controladores y memorias que se alcanzan en la actualidad, permiten ofrecer un nuevo abanico de posibilidades y de funciones, lo que origina su expansión en el mercado y un nuevo medio de intercambio de información.

Lógica programable

La tarjeta inteligente incorpora la potencia de los ordenadores, incluyendo las funciones lógicas y de control que se aplican a los negocios, junto con funciones avanzadas de seguridad y nuevas aplicaciones.

Interfaz directa de comunicaciones electrónicas

Las comunicaciones están en crecimiento constante. Cada nuevo avance ofrece un nuevo campo en el que puede aplicarse las tarjetas inteligentes.

1.2.1 Características

Dentro de las características que tiene la tarjeta inteligente podemos mencionar tres que son las mas importantes:

1.2.1.1 Inteligencia

Es capaz de almacenar y procesar cualquier tipo de información, además es autónoma en la toma de decisiones al momento de realizar transacciones.

1.2.1.2 Utiliza clave de acceso o PIN

Para poder utilizarse es necesario digitar un número de identificación personal, es posible además incorporar tecnología más avanzada como identificación por técnica biométrica, huella digital o lectura de retina.

1.2.1.3 Actualización de cupos

Después de agotado el cupo total de la tarjeta inteligente, es posible volver a cargar un nuevo cupo.

1.2.2 Funciones principales

Las tarjetas inteligentes poseen tres funciones principales, las cuales son:

1. Almacenamiento de datos.
2. Seguridad en la información.
3. Procesamiento de datos.

1.2.3 Beneficios

Entre los principales beneficios que ofrecen las tarjetas inteligentes se encuentran:

- Portabilidad de los datos que se encuentra en la tarjeta.
- Identificación y autenticación del usuario por medio de una clave personal, evitando de esta manera el uso de la misma por una persona distinta del titular.
- Sustituyen los medios tradicionales de pago a través de los archivos monederos residentes en la tarjeta.
- Posibilidad de realizar transacciones de comercio electrónico a través de Internet, haciendo uso de un lector de tarjetas inteligentes conectado a una computadora personal.

- Posibilidad de encriptación de la información que viaja por Internet, con el fin de evitar la intersección de la misma, y por ende que sólo sea desencriptada en el destino.
- Reducen el fraude.
- Reducen el trabajo con papel.
- Reducen los tiempos de cada transacción.

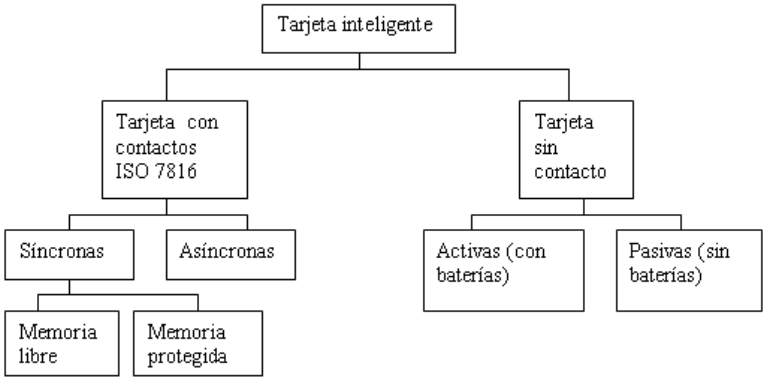
1.3 Tipos de tarjetas inteligentes

Las tarjetas inteligentes se pueden clasificar por categoría de tecnología o por categoría de capacidad.

1.3.1 Por categoría de tecnología

Podemos diferenciar por el tipo de tecnología que utiliza la tarjeta en la comunicación con el lector dos tipos de tarjetas inteligentes: la tarjeta inteligente de contacto y la tarjeta inteligente sin contacto. A continuación, se muestra un diagrama de cómo esta dividida, por su tecnología, la tarjeta inteligente.

Figura 1. Tarjeta inteligente por categoría de tecnología

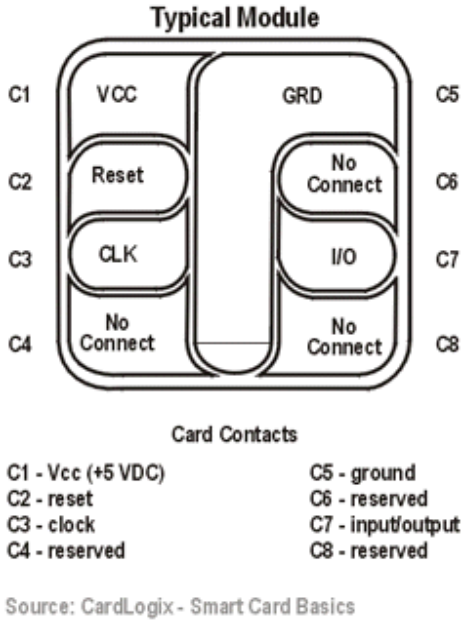


1.3.1.1 Tarjeta inteligente de contacto

Contiene un módulo de contacto en la superficie de la tarjeta en conformidad con el estándar de ISO 7816 que definiremos al final de este capítulo. Estas tarjetas son las que necesitan ser insertadas en un lector de tarjeta inteligente para que por medio de los contactos pueda ser leída.

Las tarjetas inteligentes de contacto utilizan un módulo de contacto para conectarse físicamente con el lector de tarjetas inteligentes. Se definen cinco puntos en este módulo, que se muestran en la figura: Voltaje (+5 Voltios de corriente directa), reseteado, reloj, tierra, y entrada / salida (I/O).

Figura 2. Módulo de contacto de la tarjeta de contacto



Existen dos tipos de tarjeta inteligente en la rama de tarjetas inteligentes de contacto: las sincrónicas y las asincrónicas.

1.3.1.1.1 Tarjetas inteligentes síncronas

Son tarjetas con sólo memoria, se encuentran y utilizan principalmente en tarjetas prepagadas para hacer llamadas telefónicas. Estas tarjetas contienen un chip de memoria que se utiliza generalmente para el almacenamiento de datos y aplicaciones de identificación. Los datos pueden ser cualquier información requerida para utilizar en una aplicación específica. Dentro de esta categoría, existen dos tipos de tarjeta:

1.3.1.1.1.1 Memoria libre

Este tipo de tarjetas síncronas carece de mecanismos de protección para acceder a la información. La información puede ser leída sin presentar ninguna seguridad.

1.3.1.1.1.2 Memoria protegida

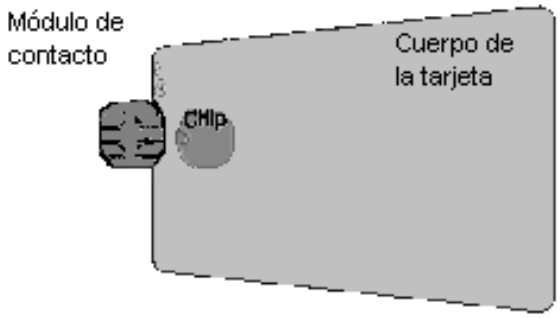
Este tipo de tarjeta inteligente síncrona necesita de códigos secretos y pasos previos para tener acceso a la información. Estas tarjetas son desechables, cargadas previamente con un monto o valor que va decreciendo a medida que se utiliza, una vez se acaba el monto se vuelve desechable, se utilizan a nivel internacional para el pago de peajes, teléfonos públicos, maquinas dispensadoras y espectáculos.

1.3.1.1.2 Tarjetas asíncronas

Son tarjetas inteligentes con microprocesador. Dentro del plástico se encuentra un elemento electrónico junto con la memoria RAM, ROM y EEPROM en el mismo chip. Cada tarjeta inteligente tiene un sistema operativo que activa las instrucciones interiores de la aplicación. La función principal del sistema operativo es habilitar el acceso a la memoria. El sistema operativo también se encarga de la seguridad de la tarjeta. Una tarjeta con microprocesador, usando el sistema operativo, tiene una conducta predefinida

que permite a la tarjeta y a la aplicación comunicarse utilizando las órdenes predefinidas.

Figura 3. Tarjeta inteligente de contacto



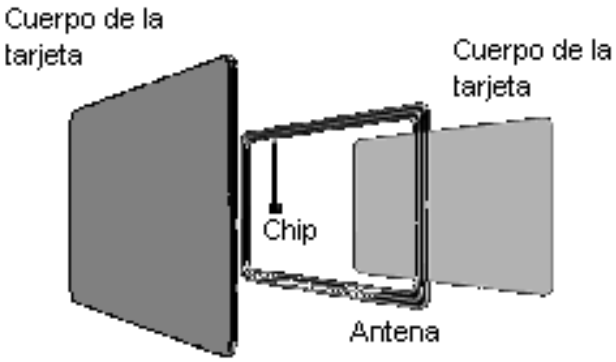
1.3.1.2 Tarjeta inteligente sin contacto

Las tarjetas inteligentes sin contacto realizan la conexión por medio de transmisiones de radio frecuencia. El lector de la tarjeta genera un campo de radio frecuencia por el que se transfiere la información entre el lector y la tarjeta, utilizando para esto una antena que posee la tarjeta. Son similares a las de contacto con respecto a lo que pueden hacer y a sus funciones pero utilizan diferentes protocolos de transmisión en capa lógica y física, no utiliza contacto galvánico sino de interfase inductiva, puede ser de media distancia (radio de comunicación de aproximadamente 10 centímetros) sin necesidad de ser introducida en una terminal de lector inteligente.

El estándar que regula este tipo de tarjeta es el ISO 14443. Una de las ventajas que tiene es que como no existen contactos externos con la tarjeta, es más resistente a los elementos externos tales como la suciedad.

Existen dos tipos de tarjetas inteligentes sin contacto: las pasivas, que no contienen una batería, y las activas, que posee una batería.

Figura 4. Tarjeta inteligente sin contacto



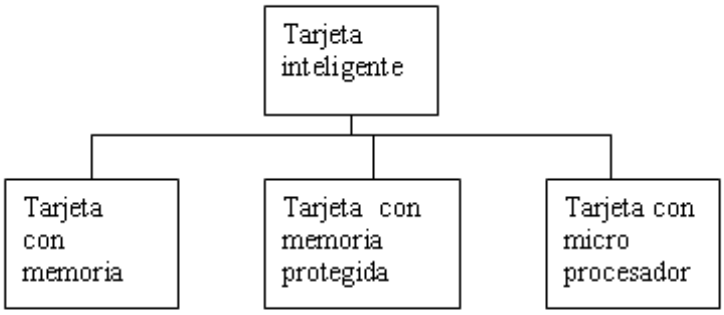
1.3.1.3 Tarjeta inteligente híbrida

Este tipo de tarjetas son una combinación de tarjetas inteligentes de contacto y sin contacto. Incluyen un micromódulo para la comunicación con el lector de contacto y también incluye una antena para la comunicación con el lector sin contacto. En esencia, podemos decir que en la misma tarjeta plástica se encuentra tanto una tarjeta sin contacto como una con contacto.

1.3.2 Por categoría de capacidad

El segundo tipo de clasificación que se le puede dar a las tarjetas inteligentes es por su categoría de capacidad. En esta clasificación existen tres tipos: tarjeta con memoria, tarjeta con memoria protegida y tarjeta con microprocesador.

Figura 5. Tarjeta inteligente por categoría de capacidad



1.3.2.1 Tarjeta con memoria

La tarjeta de memoria almacena y recupera una serie de flujo de datos que son enviados o recibidos del chip de la propia tarjeta. Este tipo de tarjeta no requiere de ninguna seguridad para que sea accesada la información almacenada en la memoria.

1.3.2.2 Tarjeta con memoria protegida

Este tipo de tarjeta inteligente requiere un código secreto (PIN), que es necesario que sea introducido antes de poder enviar y recibir datos el chip.

1.3.2.3 Tarjeta con microprocesador

Las tarjetas con microprocesador tienen un chip microprocesador. Éste puede contener un micro código que define una estructura de comando, una estructura de archivos y una estructura de seguridad en la tarjeta. Es similar a una computadora en miniatura. Puede agregar, borrar y manipular información en la memoria de la tarjeta.

1.4 Estándar de las tarjetas inteligentes

Las normas de las tarjetas inteligentes definen el funcionamiento de la tecnología y promueven la interoperabilidad de productos entre los distintos fabricantes de tarjetas inteligentes. Debido a que hay una variedad de aplicaciones de tarjetas inteligentes que requieren de soluciones diferentes, se necesitaron varias normas para definir la tecnología de tarjetas inteligentes. La Organización Internacional para la Estandarización (ISO) 7816-X define las características completas de la tecnología de tarjetas inteligentes. Otras características alteran este estándar para reunir los requerimientos a la aplicación específica.

1.4.1 Estándar ISO 7816

La ISO u Organización Internacional de Estándares es la federación global de organizaciones de estándares nacionales. Ha definido a las tarjetas inteligentes formalmente con el Estándar 7816.

La ISO 7816 establece los requerimientos físicos de la tarjeta, su módulo de contacto, protocolo de transmisión y sus reglas para identificar aplicaciones y elementos de datos. Describe los estándares de las tarjetas de contacto de circuito integrado en siete partes:

Parte 1 1987:

Describe las características físicas de la tarjeta.

Parte 2 1988:

Describe las dimensiones y ubicación del módulo de contacto de la tarjeta. Incluye estándar sobre el número, función y posición del contacto eléctrico.

Parte 3 1989:

Estandariza las señales eléctricas y protocolo de transmisión.

Parte 4 1995:

Comandos inter-industria para intercambio.

Parte 5 1994:

Sistema de enumeración y procedimiento de registro para identificar aplicaciones.

Parte 6 1995:

Elementos de datos inter-industria para intercambio.

Parte 7 1998:

Lenguaje de comandos de consulta de tarjeta inteligente.

1.4.2 Estándar ISO/IEC 14443-1

La Organización de Estandares Internacionales (ISO) y la Comisión Internacional Electrotécnica (IEC) define la especificación para las tarjetas sin contacto. Este cambia la definición de módulo de contacto a una antena, y define el protocolo de comunicación por el aire.

1.4.3 Estándar ETSI

El Instituto Europeo de Estándares de Telecomunicaciones (ETSI), define una tarjeta inteligente pequeña según su tamaño para encajar en los teléfonos de GSM.

1.4.4 Estándar EMV

Estándar desarrollado por Europay International, Master Card International, y Visa International (EMV), para sistemas de pago en tarjetas inteligentes. Este estándar define el camino entre la tarjeta inteligente y la terminal de pago indistintamente del lector. Esto provoca un aumento en la seguridad previniendo la lectura de la tarjeta para la información de bajo nivel.

1.4.5 Estándar PC/SC

Esta especificación del grupo de trabajo PC/SC (*Personal Computer/Smart Card*) construye en las especificaciones existentes EMV e ISO 7816-X, definiendo la tarjeta inteligente en una capa de abstracción de lectura / escritura. Esta es una especificación complementaria que define el dispositivo de bajo nivel, aplicaciones API de dispositivos independientes y dirección de recursos, que permite a las múltiples aplicaciones compartir los dispositivos de la tarjeta inteligente en un sistema. En diciembre de 1997, el grupo de trabajo publicó la primera versión de las especificaciones en la dirección http://www.smartcardsys.com/ .

1.4.6 Estándar JavaCard

Este estándar define la manera en que la máquina virtual Java implementa que un usuario final pueda ejecutar cualquier applet de Java en una tarjeta inteligente. El Java Card Forum maneja esta especificación.

1.4.7 Estándar WHQL

Desarrollado por Microsoft's Windows Hardware Quality Labs (WHQL). El Microsoft WHQL fácilmente define las pautas para productos que son compatibles con el sistema operativo de Microsoft. Su enfoque es asegurarse de que los dispositivos trabajaran en el ambiente Windows y es compatible con otros dispositivos. Los requerimientos de WHQL para las tarjetas inteligentes es que sean completamente compatibles con el estándar ISO 7816.

1.4.8 Estándar GSM

La industria de telecomunicaciones europea también adoptó los estándares ISO 7816 en su especificación de tarjetas inteligentes para el sistema global, para las

comunicaciones móviles (GSM), con el fin de habilitar la identificación y autenticación de usuarios de teléfonos móviles.

2 SEGURIDAD

2.1 Introducción a seguridad

En los últimos años, el crecimiento vertiginoso de las redes de comunicaciones y el aumento de usuarios de éstas está conllevando nuevos problemas a los cuales no les sirven las soluciones obtenidas hasta el momento. Un ejemplo claro lo encontramos en la seguridad. A medida que la autopista de la información cruza fronteras, las puertas cerradas ya no bastan para proteger uno de los activos más valiosos de las compañías: la información.

En cuanto a comercio electrónico, parece ser que la falta de confianza en el sistema y en los comerciantes involucrados en la transacción es la razón principal por la que la mayoría de dichos intercambios de bienes generados por Internet se concluyan en efecto fuera de la Red. El contacto personal les da a los compradores la seguridad de que la compañía que está detrás del sitio en Internet realmente existe y está preparada para realizar su cometido.

A pesar de lo cambiante del entorno, los requisitos de seguridad siguen siendo los mismos: autenticación, confidencialidad, integridad y no repudio; aunque los objetivos y la implementación de los mismos evoluciona a velocidad vertiginosa.

- Confidencialidad: garantía de que la información no ha sido leída por otro. Mantener privada la información.
- Integridad: demostrar que la información no ha sido manipulada.

- Autentificación: es el proceso de cómo la tarjeta, terminal o la persona prueba quien es de verdad.
- No repudio: garantizar que no se puede rebatir la propiedad de la información.

En el caso de las tarjetas inteligentes, nos encontramos ante una tecnología que, con productos diseñados e implantados de la manera apropiada, nos puede proporcionar una oportunidad incomparable para mitigar y, potencialmente, eliminar algunos de los problemas de fraude con los que actualmente nos enfrentamos.

Las tarjetas inteligentes hacen uso de la criptografía para su seguridad, es por eso que a continuación la exponemos.

2.2 Criptografía

Es la ciencia que se asegura que el mensaje esté seguro. La criptografía como ciencia estudia los problemas básicos de la seguridad en la transmisión de la información por un canal inseguro. El sistema criptográfico está basado en los conceptos de autenticación, integridad, confidencialidad y no repudiación.

Podríamos decir también que la criptografía es una disciplina matemática que no sólo se encarga del cifrado de textos para lograr su confidencialidad, protegiéndolos de ojos indiscretos, sino que también proporciona mecanismos para asegurar la integridad de los datos y la identidad de los participantes en una transacción.

La criptografía garantiza la confidencialidad encriptando un mensaje mediante una clave secreta en conjunto con un algoritmo. Esto da como resultado una versión "codificada" del mensaje que el receptor puede desencriptar, utilizando la clave original, para recuperar su contenido. La clave empleada debe mantenerse en secreto entre las dos partes.

Es necesario mencionar un protocolo que hace uso de la criptografía y que es de los más usados actualmente, es el SSL: capa de enlace seguro. Estándar de facto propuesto por Netscape, ampliamente disponible en navegadores y servidores web. Es un protocolo cliente servidor que negocia el establecimiento de canales virtuales seguros. SSL es un protocolo de comunicación que proporciona principalmente tres servicios básicos de seguridad: confidencialidad, autenticación e integridad. Con el fin de garantizar dichos servicios, SSL hace uso tanto de la criptografía asimétrica (basada en la existencia de un par de claves, la pública y la privada) como de la criptografía simétrica (basada en la utilización de una única clave secreta).

Como lo mencionamos anteriormente, la criptografía se divide en criptografía simétrica y criptografía asimétrica, temas que expondremos a continuación.

2.2.1 Criptografía simétrica

La criptografía simétrica resuelve el problema de la confidencialidad y usa algoritmos como DES, TRIPLE DES, y AES para transmitir información cifrada, y que sólo con una única clave simétrica puede leer el contenido de la información. Esta clave la llamaremos "clave simétrica" y tiene en general una longitud de 128 bits. El problema aquí es que antes de realizar la conexión segura es necesario que ambos lados tengan la misma clave simétrica.

El tamaño de clave simétrica suele oscilar entre los 40 y los 128 bits. Las claves de 40 bits pueden romperse en cuestión de horas, mientras que las claves de 128 bits son irrompibles actualmente.

Algunos algoritmos que utiliza la criptografía simétrica son:

2.2.1.1 Algoritmo DES

DES (Data Encryption Standard o cifrado de datos estándar). Fue desarrollado por IBM y la Agencia Nacional de Normas Americanas. Fue usado por primera vez a finales de los años setentas. Desde entonces, se ha vuelto el más usado tanto en el sector comercial como en el sector bancario. En su versión original, opera con una longitud de 56 bit.

Este algoritmo fue reventado por fuerza bruta por la EFF (Electronic Frontier Foundation) usando una máquina especializada en sólo 56 horas. La fuerza bruta básicamente involucra intentar las 2^{56} claves hasta encontrar la correcta. La fuerza bruta necesita, en promedio $2^{long.clave\ -1}$ - así que en el caso de DES la máquina tiene que intentar aproximadamente 2^{55} veces el descifrado antes de ser recompensado con el texto en claro correcto. Más recientemente, el tercer desafío DES propuesto por RSA fue ganado en menos de un día por la máquina de la EFF.

2.2.1.2 Algoritmo triple DES

Es una versión fortalecida del algoritmo DES. Normalmente usado en el sector bancario. 3DES consiste en tres aplicaciones del cifrado DES en modo CDC (cifrado-descifrado- cifrado) con claves independientes. El cifrado se ejecuta como sigue:

$$TextoCifrado=DES_{k1}(DES^{-1}_{k2}(\ DES_{k3}(TextoClaro)))$$

Y el descifrado:

$$TextoClaro=DES^{-1}_{k3}(DES_{k2}(\ DES^{-1}_{k1}(TextoCifrado)))$$

3DES tiene un tamaño de bloque de 64 bits y una longitud de clave de 168 (3*56) bits. Por la construcción de 3DES, se piensa que ofrece una seguridad equivalente a un cifrado de bloque de 112 bits.

Triple-DES es al menos 2^{56} (aprox. 10^{17}) veces más difícil de romper que el DES original y como tal puede ser considerado muy seguro. Un adversario tendría que intentar en promedio 2^{111} claves para romper un solo mensaje 3DES (y necesitaría una gran cantidad de espacio de almacenamiento para almacenar los valores intermedios).

En palabras de Bruce Schneier: "Ciertamente triple-DES es una mejor elección que AES, en algunas aplicaciones. Triple-DES será posiblemente el algoritmo elegido para muchas aplicaciones bancarias incluso después de que el estándar AES sea aprobado."

2.2.1.3 Algoritmo AES

AES (Advanced Encryption Standard o estándar criptográfico avanzado) es la búsqueda del gobierno de EE.UU. de un sustituto para el viejo estándar DES. Utiliza bloques de 128 bits.

El Instituto de Estándares y Tecnología (NIST), hizo una primera solicitud pública de algoritmos el 12 de septiembre de 1997. Varios criptógrafos bien conocidos (Rivest, Schneier, Knudsen, Biham, Rijmen, Coppersmith, etc) desarrollaron algoritmos candidatos para el AES que cumplían los criterios solicitados. De los 15 algoritmos iniciales, cinco (Mars, RC6, Rijndael, Serpent y Twofish) han sido seleccionados para pasar a la segunda ronda.

Aunque este proceso de selección sólo elige un cifrado para el gobierno estadounidense, se cree que AES, cuando sea seleccionado, se convertirá en el estándar

internacional durante el próximo milenio. Todos los candidatos AES aceptan claves de 128, 196 o 256 bits y tienen un tamaño de bloque de 128 bits.

2.2.2 Criptografía asimétrica

La criptografía asimétrica consiste en algoritmos basados en problemas de un solo sentido, es decir que por un lado sea muy fácil realizarlo, pero a la inversa sea "difícil" de realizarlo, como es problema de la factorización entera, es fácil realizar el producto de dos números pero es "difícil" factorizar un número producto de dos números primos grandes.

El tamaño de clave asimétrica oscila entre los 512 bits y los 4096 bits. No se recomienda el uso de claves inferiores a 768 bits. Cuando elegimos una clave asimétrica, estamos limitados por dos principios:

i. Seguridad. Uno de los factores clave en la fortaleza de los sistemas es el tamaño de los pares de claves públicas / privadas.
ii. Velocidad. Cuanto mayor es la clave, tanto más lentas serán las operaciones de clave pública.

Para la mayoría de los usuarios, el principal factor en la selección del tamaño de una clave pública sería la seguridad. La velocidad rara vez será un factor condicionante.

La siguiente tabla, lista las longitudes de clave pública recomendadas para protegerse contra ataques por una sola corporación (¡las claves deberían ser significativamente más grandes para protegerse contra las agencias de inteligencia!):

Tabla I. Longitud recomendada de claves asimétricas

Año	Longitud de clave recomendada
1995	1280
2000	1280
2005	1536
2010	1536
2015	2048

A continuación se describe algunos de los sistemas asimétricos para la obtención de la clave pública y privada.

2.2.2.1 Sistema RSA

RSA representa las iniciales de los tres hombres que lo inventaron en 1977, ellos son: Ron Rivest, Adi Shamir, y Len Adleman. RSA se anunció en 1978. Las firmas RSA utilizan una clave de hasta 2048 o 4096 bits (dependiendo de la implementación). La seguridad del sistema RSA se basa en el problema RSA (PRSA). Se conjetura, aunque no ha sido probado, que este problema es equivalente al Problema de la Factorización de Enteros (PFE).

Se define el PRSA así: "dado un entero positivo n que es producto de dos primos enteros impares p y q, un entero positivo e tal que mcd(e,(p-1)(q-1))=1, y un entero c, encontrar un m tal que m^e es congruente con c (mod n)."
Los mejores ataques conocidos contra RSA son:

El ataque Meet In The Middle (MITM) (encontrarse en el medio). Este ataque puede teóricamente ser usado contra cualquier cifrado múltiple. En el caso de DES, este

ataque requiere 524.288 Terabytes de almacenamiento, 2112 cifrados y 2112 consultas de tabla.

Ataques MITM optimizados. Algunos compromisos tiempo / memoria aplicados al ataque MITM estándar pueden hacer que MITM sea ligeramente más realizable. Se necesitan 2108 operaciones de cualquier modo para el ataque "realizable" en términos de memoria.

Ataque con clave relacionada. Necesita una consulta con clave relacionada, una consulta con texto cifrado elegido y de 256 a 272 intentos de cifrado *offline*.

Dado que RSA no utiliza intensamente el tiempo de procesador en comparación con otros sistemas de firma, se ha convertido en el sistema usado en pequeños dispositivos de poca potencia, tales como: tarjetas inteligentes o pequeños chips.

Es relativamente fácil entender las matemáticas que están detrás de la encriptación de llave pública RSA. Para su explicación, lo dividen en 5 pasos:

- Encuentre P y Q, dos números primos grandes (1024 bits).
- Elija E tal que E es mayor que 1, E menor que PQ y tal que E y (P-1)(Q-1) son relativamente primos, que los medios entre ellos no tenga ningún factor primo en común. E no tiene que ser primo, sino que debe ser impar. (P-1)(Q-1) no puede ser primo porque es un número par.
- Cálculo D tal que (DE-1) es uniformemente divisible por (P-1)(Q-1). Matemáticos escriben esto como DE=1(mod(P-1)(Q-1), y ellos llaman a D como el inverso multiplicativo de E. Esto es fácil de hacer, simplemente encontrando un entero X que cause que D=(X(P-1)(Q-1)+1)/E sea un entero. Después uso el valor D.

- La función del cifrado es C = (T^E) MOD PQ , donde está el texto cifrado C (un número entero positivo), T es el texto plano (un número entero positivo), y ^ indica la exponenciación. El mensaje que es cifrado, T , debe ser menor que el módulo, PQ .
- La función del desciframiento es T = (C^D) MOD PQ , donde está el texto cifrado C (un número entero positivo), T es el texto plano (un número entero positivo), y ^ indica el exponenciacion.

Su llave pública es el par (PQ, E) . Su llave privada es el número D (no lo revele a nadie). El producto PQ es el módulo (a menudo llamado N en la literatura). E es el exponente público. D es el exponente secreto.

Usted puede publicar su llave pública libremente, porque no hay métodos fáciles sabidos de calcular D , P , o Q dado solamente (PQ, E) (su llave pública).

Un ejemplo práctico del algoritmo RSA seria el siguiente:

- P = 61 <= primer número primo (destruya esto después de computar E y D)
- Q = 53 <= segundo número primo (destruya esto después de computar E y D)
- PQ = 3233 <= el módulo (dé esto a otros)
- E = 17 <= el exponente público (dé esto a otros)
- D = 2753 <= el exponente privado (guarde éste en secreto)
- Su llave pública es (E,PQ). Su llave privada es D.
- La función de encriptación es: el encrypt(T) = (T^E) el mod PQ = (T^17) mod 3233
- La función de desencriptación es: el decrypt(C) = (C^D) el mod PQ = (C^2753) mod 3233

Para Encriptar el texto plano con valor 123, haga esto: el encrypt(123) = (123^17) mod 3233

= 337587917446653715596592958817679803 mod 3233

= 855

Para Descifrar el texto plano con valor 855, haga esto: el decrypt(855) = (855^2753) mod 3233

=504328889584160687344228991273944666314538783600355093155549675645010556286120825599787442454281100543834986542893363849302464514415078517209179665478263530709963803538732650089668607477182974582295034295040790358184594095637793858659893688380836028401325097686207669773966753325054282609347573513798806325648263933445309259438556242923301751977190016924916912809150596019178760171349725439279215696701789902134307146468971279610277181378394586967728986934236524031169321708926961764372652131566583315871245975980304250314400683788324610178483071758547454725206968892599589254436670143220546954317400228550092386369424448559733330630516073853028632193029135037454719467577767135795496520291979050578153287155839207030315958593749366328354860209083063550704455658896319318011934122017826923344101330116480696334024075046952588669876586690062240241020884665075302639538705266319335847348109487615622712603732759736037523738836414808894843809615775704538008107946980066734877795883758289985132793070353355127509043994817897905489933812173294585354474132680569810872633482854638168850488243465889783933346625445400661964521876669479552802308841246594823927510577049113329025684306505229256142730389832089007051511055250618994171231777951579794297117954752963018378438629139778776612982073890727967672023501139927158196427307640741898919048686074812454931579537437712441601438765069145868196402276027766869530903951314968319097324505452345944772565878876926933539186923548185185424209230649964068221844901191357108854244285211207737122383110545543126530739407591

27890822606043171133395752266034451645259763161842774590432019134528932
99321613074405322274705728948121435868319784155972764963570909012151313
04157569209798518321041155969357848833665315951327344675243940875769777
89084901269153228420809496307929724713044221942439065903081428939302915
84830873687450789770869218452967411463211556678655283381648067954559418
91006950919658990854567980723923708463025535456869192355462995715735879
06227458619572172111078828657563859709419077632050978323957134641190250
04702084856040821750949107716553117652974738031767658205876731402889103
28834318508844721164427193903740413155649869959137365162108451137402243
35185995766577539693628125425390068552624545614192588094374021288866697
44109721845342218171980899119537075455420339119645393664617929681653426
52234639936742330970183533904623677693670380534264482173582384219251590
43814852473889686424437031866541996153779139696490030395876065491524494
50436001359392771339521012519285720925978875116019596296156902711643189
46373426500236310045557180036935860552649100009072451837866895644171649
07278356281009708545241354696608448116133878065485451517616730860510806
57829365241087232636672280540038794108643482267500907782651210137281958
31653139698309088731741747453598868429855980718519221597004650810606844
55953648089224944054276632967459230889848486843586547985051154284401646
23526969317993778443021785701919709875162965466513027800996658005217820
81393172323790132324946826092008199810376848471678749891936949979148247
16345060937125654122501953795166897601855087599313367797793952782227323
33752958026312266535894820556651528946636903208328768043239061154935095
45909340667640225867084833760536998679410262047090571567447056531112428
62907354888492989983560999636092141128497745861469604028702967070147817
94902482829074841600836804586668550760461922520943498047157452688181318
50859150194852763596503458153641656549316013061330407434457965108380304
06224027889804282518909471629226689801668448096364519809051090579651307
57037924595807447975237126676101147387874214414915481359174392799496956

41565386688389171544630561180536972834347021920634899953191764016110392
49043917980339897549176539592360851180765318470647331801578207412764787
59273908749295571685366518591266637383123594589126787095838000224515094
24457564874484086877530845395521730636693891702394037184780362774643171
47085583049195989514677629439214310024561306111429937000557751339717282
54911005600894089841967131970911816554290876109008324997831338240786961
57849234198629916800867749593407759306602207814943807854996798945399364
06368572269742236185841142504837245124465580270859179795591086523099756
51983827795294575699657424557868838354442368572236813990212613637440821
31478483203563615611346287019851423901842909741638620232051039712184983
35528630868518428263461502744187358639504042281512399505995983653792227
28584742207167783667945134363807086579774219853595393166279988789721695
96345534633649794922113017661316207477266113107012321403713882270221723
23308547267953301507998062253835458948024820043144726191596190526034069
06193093929072410284948700167172969517703467909979440975063764929635675
55800711621827727603182921790350290486090976266285396627024392536890256
33710147168327404504583060228676314215815990079164262770005461232291921
92997169907690169025946468104141214204472402661658275680524166861473393
32265959127006456304474160852916721870070451446497932266687321463467490
41185886760836840306190695786990096521390675205019744076776510438851519
41619318479919134924388152822038464729269446084915299958818598855195149
06630731177723813226751694588259363878610724302565980914901032783848214
01136556784934102431512482864529170314100400120163648299853251663490560
53794585089424403855252455477792240104614890752745163425139921637383568
14149047932037426337301987825405699619163520193896982544786313097737491
54478427634532593998741700138163198116645377208944002854850002696859826
44562183794116702151847721909339232185087775790959332676311413129619398
49592613898790166971088102766386231676940572959325380786434441005121380
25081797622723797210352196773268441946486164029610598990277105325704570

16332613431076417700043237152474626393990118997278453629493036369149008
81060531231630009010150839331880116682151638931046666595137827498923745
56051100401647771682271626727078370122424655126487845492350418521674263
83189733332434674449039780017846897264054621480241241258338435017048853
20601475687862318094090012632419690922520226798801134080730122162644041
33887392600523096072386158554965158001034746119792130767224543803671883
25370860671331132581992279755227718486484753261243028041779430909389923
70938053652046462551472678849615277327411926570911661358008414542148 76
87310394441054796393085308968803656085047721445921725001265007170689694
28154627563704588389042191773981906487319080148287390581594622278672774
18610111027632479729041222119941173882045263357017590906786281592815199
82214576527968538925172187200900703891385628400073322585075904853480465
64543498370732876259358914278543182665872946080723896522915990217388879
57736477387265746104008225511241827200961681888284938946788104688473126
55417262097890567845810965179753008730631546490302112133528180847612299
04095764278573163641248809309497707395675884229631711584645698420245510
90298823985179536841258914463527918973076838340736961314097452298563866
82726910433575176771288945278813686239650666540898943949516191200216077
78988768647364818378253248466991683072812203107919354666840159148582699
99337442767725227540385332219685229859085154811040229657916338257385513
31482345959163328144581984361459630602499361753097925561238039014690665
16367371885958277252568311998998464602721646279764077057074816406450769
77986995510618004647193780822325014893407851137833251073753823403466269
55329260881384389578409980417041041777608463062862610614059615207066695
24301843857503176293954302631267377406936404705896083462601885911184367
53252984588804084971092299919565539701911191919188327308603766775339607
72245563211350657219106758751186812786344197572392195263333856538388240
05719010256494923394451965959203992392217400247234147190970964562108299
54774619322898118128605556588093851898811812905614274085809168765711911

22476328865871275538928438126611991937924624112632990739867854558756652
45305619750989114578114735771283607554001774268660965093305172102723066
63573946233413638045914237759965220309418558880039496755829711258361621
89014035954234930424749053693992776114261796407100127643280428706083531
594582305946326827861270203356980346143245697021484375 mod 3233
= 123

2.2.2.2 Sistema curvas elípticas

Las curvas elípticas (CE) fueron propuestas por primera vez para ser usadas en aplicaciones criptográficas en 1985 de forma independiente por V.S.Miller y N.Koblitz.

Las curvas elípticas son interesantes porque presentan las siguientes ventajas sobre DH y RSA:

Tamaño de clave. Una clave de curva elíptica tiene habitualmente unos 160 bits, mientras que las claves DH y RSA deben tener 1.024 bits para conseguir el mismo nivel de seguridad.

Velocidad. Los sistemas de curva elíptica son significativamente más rápidos que los sistemas basados en RSA o DH (ante igual nivel de seguridad, no misma longitud de clave).

Certicom (Empresa comercial que trabaja con tecnología CE) ha emitido recomendaciones sobre los tamaños de claves CE frente a las RSA.

Tabla II. Comparación de longitudes de clave RSA frente a CE

Longitud clave cifrados de bloque	Longitud clave RSA	Longitud clave CE
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

2.2.2.3 Sistema DH

Diffie-Hellman (DH) fue el primer sistema de clave pública abiertamente publicado (es más correcto decir que DH es un mecanismo de intercambio de claves) y como tal ha sido objeto de detallados análisis por eminentes criptógrafos.

Diffie-Hellman junto con sus derivados como ElGamal están cubiertos por la patente U.S. número 4.200.700 que expiró el 6 de septiembre de 1997. Actualmente, el sistema DH sólo ofrece DSS como algoritmo de firmado. DSS significa *Digital Signature Standard* (Estándar de Firma Digital) y produce una firma de longitud constante (independiente del tamaño de las claves públicas / privadas).

La seguridad del sistema DH se basa en el problema de Diffie-Hellman (PDH). Se conjetura (no se ha demostrado) que es equivalente al Problema del Logaritmo Discreto (PLD).

El PDH es equivalente al PLD bajo la "conjetura de Diffie-Hellman". Esto asume que es improbable calcular g^{ab} conociendo sólo g^{a} y g^{b}.

Hay varias desventajas en usar DH frente a RSA:

a. Expansión del mensaje. El tamaño del mensaje cifrado se dobla respecto al original. Esto sin embargo no es un obstáculo real en ElGamal ya que sólo se utiliza para cifrar la clave de sesión de cada receptor.

b. Fortaleza de la firma. Las implementaciones actuales de DH sólo ofrecen DSS como algoritmo de firmado. Esto limita la longitud de la clave a sólo 1024 bits lo que podría, por sí solo, ser insuficiente para la seguridad a largo plazo. Las firmas RSA utilizan una clave de hasta 2048 o 4096 bits (dependiendo de la implementación).

c. Intensidad computacional. Tanto DH como DSS utilizan más intensamente el tiempo de procesador que RSA. En los procesadores modernos esta diferencia no es apreciable pero en dispositivos de poca potencia (tarjetas inteligentes o pequeños chips), DH/DSS podrían no ser utilizables. Si el tiempo de procesador o el tamaño de la clave son importantes un sistema asimétrico basado en curvas elípticas podría ser una mejor elección que tanto RSA como ElGamal.

d. La necesidad de una "buena" aleatoriedad. El valor aleatorio "k" en DH / DSS necesita ser único e impredecible. Si un adversario obtiene dos mensajes cifrados con el mismo "k" o recupera "k" entonces puede obtener la clave privada, esto es realmente un fallo catastrófico.

La otra cara de la moneda es que hay varios beneficios en usar DH/DSS frente a RSA:

a. ElGamal está totalmente libre de *copyrights* y patentes. Esto significa que ElGamal puede ser utilizado globalmente sin necesidad de una licencia. El

uso de RSA en EE.UU. y Canadá requiere, sin embargo, obtener una licencia de RSA Labs si se utiliza en productos comerciales. RSA proporciona licencias gratuitas para una cierta librería RSA, pero hay algunas prohibiciones en la licencia.

b. Usando RSA, alguien podría generar un primo falso o de una clase especial que facilitase su factorización. Sin acceso a la clave privada es simplemente imposible comprobarlo.

c. No es apropiado usar RSA en situaciones en las que la generación de la clave ocurre regularmente (en cada mensaje), como en sistemas de clave efímera.

d. RSA ofrece menos seguridad por cada bit de clave que DH/DSS.

e. DH parece estar basado en una teoría matemática más sólida.

f. Las claves de sesión DH son evanescentes. Usando la aplicación más simple de la generación de claves RSA, Alice crea una clave de sesión y se la transmite a Bob usando la clave pública de Bob. Un "mirón" que pueda coaccionar a Bob posteriormente para que le revele su clave privada puede recuperar el texto completo de la comunicación entre Alice y Bob. Como contraste, si Alice y Bob usan DH para generar la clave de sesión, la destruyen después del fin de la sesión, y no almacenan su comunicación, ni la coacción ni el criptoanálisis permitirán al "mirón" descubrir la información intercambiada.

2.3 Esquemas de seguridad

2.3.1 Firma digital

La firma digital es un número natural, de más o menos 300 dígitos, que tiene las mismas propiedades que la firma convencional. Es decir es posible asociar un número único a cada persona o entidad, existe un método de firma y un método de verificación de la firma. Esta firma digital resuelve satisfactoriamente el problema de autenticación y no rechazo.

Tipos de firmas digitales

- El método más usado para firmar digitalmente es el conocido como RSA. Lo importante de este método es que es el más usado actualmente y por lo tanto es conveniente usarlo para poder ser compatible. Este criptosistema, creado en 1978 por Rivest Shamir y Adleman (de aquí su nombre), utiliza esencialmente que la tarea de factorizar es muy difícil.

- Otro método reconocido para firma digital es el llamado como DSA que es oficialmente aceptado para las transacciones oficiales en el gobierno de USA.

- Una tercera opción es el método que usa curvas elípticas. Este método tiene la ventaja a los dos anteriores a reducir hasta en 164 bits, es decir como 45 dígitos las claves, manteniendo la misma seguridad. Por lo que es más propio para ser usado donde existen recursos reducidos como en tarjetas inteligentes.

- Diffie-Hellman (DH) fue el primer sistema de clave pública abiertamente publicado.

2.3.2 Certificado digital

El certificado digital es un archivo de aproximadamente 1k de tamaño que contiene, primero, los datos del propietario, después, su clave pública y la firma digital de una autoridad competente. Cuando una persona solicita un certificado digital, se generan su par de claves, la pública y la privada. La clave pública viene en el certificado digital explícitamente. La clave privada queda en custodia del propietario del certificado.

El tercer elemento importante que tiene el certificado digital es la firma digital de una autoridad certificadora, quien garantiza que los datos corresponden al propietario. El certificado digital queda muy parecido entonces a un documento oficial de identificación como un pasaporte o una licencia de conducir. En la actualidad, tenemos un formato (estándar) que se ha extendido casi para todas las aplicaciones, este es el llamado X.509.

En síntesis, la misión fundamental de los certificados es permitir la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma electrónica, pertenece realmente a ese usuario, ya que así lo hace constar en el certificado una autoridad que da fe de ello.

Un ejemplo de certificado digital es:

issuer:C=ES ST=L=Barcelona O=SECURITY ZUTANEZ OU=Division de certificados CN=Fulano Menganez Email=Fulano@fulanez.es subject: C=ES ST=O=OU=CN=Jaimito Email=Jaimito@jaimito serial:15 Certificate: Data: Version: 1

(0x0) Serial Number: 21 (0x15) Signature Algorithm: md5WithRSAEncryption Issuer: C=ES ST=L=Barcelona O=SECURITY ZUTANEZ OU=Division de certificados CN=Fulano Menganez Email=Fulano@fulanez.es Validity Not Before: Nov 18 15:15:31 1998 GMT Not After : Nov 13 15:15:31 1999 GMT Subject: C=ES, ST=, O=, OU=, CN=Jaimito Email=Jaimito@jaimito Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:9e:74:de:c9:1 a:6b:f4:fe:d1:04:30:58:7e:8b:51:7a:98:23:e9:45:a9:c2:a7:7c:f8:f8:b5:9a:a2:ea:c1:99:68:b a:f7:c3:d8:06:05:1b:6a:47:a1:44::2c:a6:e0:4b:6f:ce:02:c4:06:32:20:34:be:13:97:39:a3:aa :6f:2f:41:a7:bc:14:c8:f3:0c:ad:9d:9:63:8a:f5:eb:60:5b:06:a6:01:fb:1a:07:b2:c6:39:48:bb: b7:00:56:4e:20:6d:87:3f:67:0b:2f:f4:b0:5f:74:7f:90:6b:b4:47:6f:56:1a:b5:c5:42:5:9b:e5: e3:00:e2:4f:e3:14:47 Exponent: 65537 (0x10001) Signature Algorithm: md5WithRSAEncryption
3b:2b:e9:ff:48:48:35:ab:30:5c:e2:d1:88:c9:29:8b:bc:09:2:58:80:17:9c:e7:08:0a:7d:8a:5e: 46:a8:83:3b:ee:84:de:2:e3:ea:51:cb:92:bc:fa:db:90:bd:cd:9f:25:d4:4a:48:63:ac:b8:93:f9: dc:9c:cf:ef:fd:45------BEGIN CERTIFICATE------
MIICOzCCAeUCARUwDQYJKoZIhvcNA
QEEBQAwgaYxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbHVueWExD
DAKBgNVBAcTA0JjbjEVMBMGA1UEChMMU0VDVVJJVFkgQkNOMRowGAYD
VQQLExFzZWNjaW8gZCdlbXByZXNlczEdMBsGA1UEAxMURGF2aWQgR3VlcnJl
cm8gVmlkYWwxIzAhBgkqhkiG9w0BCQEWFGd1ZXJyZXJvQGdyZWMudXBjLmV
zMB4XDTk4MTExODE1MTUzMVoXDTk5MTExMzE1MTUzMVowZjELMAkGA1
UEBhMCRVMxCTAHBgNVBAgTADEJMAcGA1UEChMAMQkwBwYDVQQLEw
AxGDAWBgNVBAMUD0NhbHZpbiAmIEhvYmJlczEcMBoGCSqGSIb3DQEJARYN
Y2FsdmluQGhvYmJlczCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAnnTey
Rpr9P7RBDBYfotRepgj6UWpwqd8+Pi1mqLqwZlouvfD2AYFG2pHoURcLKbgS2/O
AsQGMiA0vhOXOaOqby9Bp7wUyPMMrZ0JY4r162BbBqYB+xoHssY5SLu3AFZOI
G2HP2cLL/SwX3R/kGu0R29WGrXFQlSb5eMA4k/jFEcCAwEAATANBgkqhkiG9w0
BAQQFAANBADsr6f9ISDWrMFzi0YjJKYu8CbJYgBec5wgKfYpeRqiDO+6E3mLj6l
HLkrz625C9zZ8l1EpIY6y4k/ncnM/v/UU= - -----END CERTIFICATE-----

Este es un certificado válido durante un año, emitido por la autoridad certificadora SECURITY ZUTANEZ para el usuario Jaimito, cuya clave pública es:

exponente: 65537 modulo:
1112719555297182749770200010532872549711535743256394864652426542649114539614030882310105443040321585401884991855044788817550616458932058891843404404841771733136829794829081324994736239836517710754461093651982670656788110901071526325923888891015101576104046239067444510485252645768853648368107736215039741184 71

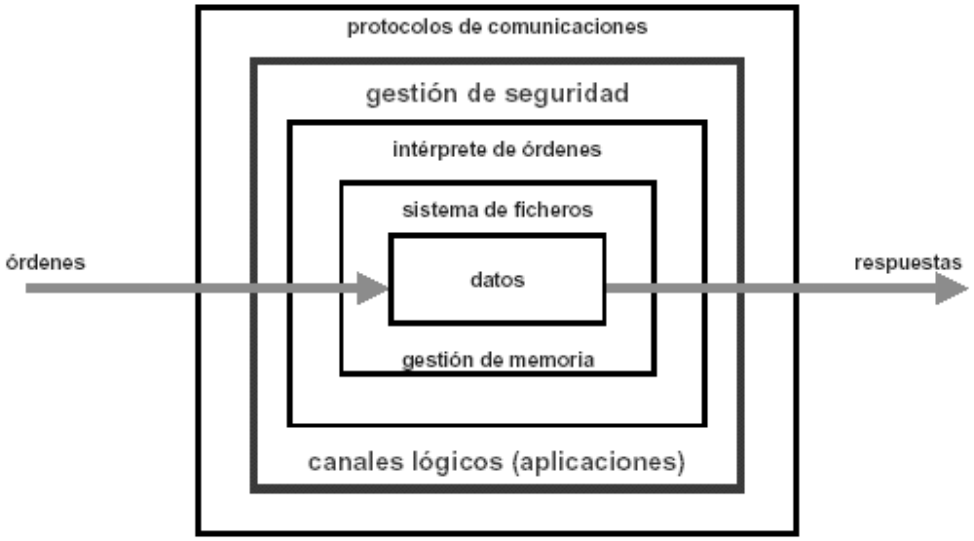
2.4 Seguridad en tarjetas inteligentes

2.4.1 Gestión de seguridad

El sendero interno de comunicación entre los elementos de la tarjeta inteligente (BUS) es totalmente inaccesible desde fuera del chip de silicona, es por ello que la única manera de comunicarse está totalmente bajo control de sistema operativo y no hay manera de poder introducir comandos falsos o requerimientos inválidos que puedan sorprender las políticas de seguridad.

Podemos apreciar en la siguiente figura cómo en una tarjeta inteligente es necesario que una orden pase por la gestión de seguridad del sistema operativo, y también cómo la respuesta a la orden pasa por esa seguridad.

Figura 6. Gestión de seguridad de tarjeta inteligente



Las tarjetas inteligentes dependen de tres zonas fundamentales:

1. Zona abierta: contiene información que no es confidencial (el nombre del portador y su dirección).
2. Zona de trabajo: contiene información confidencial (aplicaciones bancarias: cupo de crédito disponible, el número de transacciones permitidas en un periodo de tiempo).
3. Zonas secretas: la información es totalmente confidencial. El contenido de estas zonas no es totalmente disponible para el portador de la tarjeta, ni tiene por qué conocerla la entidad que la emite ni quien la fabrica.

2.4.2 Mecanismo de seguridad

Hay diferentes tipos de mecanismos usados en las tarjetas inteligentes. Aquellos necesarios para tarjetas de memoria y menos sofisticados que aquellos para tarjetas de microprocesador. Dado que estos mecanismos utilizan ampliamente la criptografía, lo incluimos en este capítulo. Se pueden mencionar, entre los mecanismos de seguridad que maneja la tarjeta inteligente, los siguientes:

2.4.2.1 Verificación de contraseña

La verificación de contraseña es el mecanismo en el que el usuario introduce la contraseña de acceso. Ésta es mandada a la tarjeta inteligente, ésta valida si el código de acceso es el correcto, habilitando que se pueda leer el área específica de datos, de lo contrario decrementa un contador de ratificaciones en el que se especifica la cantidad de veces que puede ser presentado erróneamente la contraseña. Al llegar el contador de ratificaciones a cero, la tarjeta bloquea el área de datos especificada.

2.4.2.2 Autenticación externa

Este mecanismo sirve para que la tarjeta inteligente autentique la terminal de trabajo. El proceso es el siguiente: la terminal solicita un número randómico que genera la tarjeta (CRnd), este número es operado por la terminal para obtener un criptograma de autenticación externa (EAC) utilizando la llave de autenticación (Kaut) y el algoritmo triple des, de la siguiente forma: EAC = 3DES (CRnd,Kaut). Este resultado es mandado a la tarjeta inteligente. La tarjeta realiza las mismas operaciones criptográficas y compara los resultados. Si los resultados concuerdan, la terminal fue autenticada.

2.4.2.3 Autenticación interna

Este mecanismo sirve para que la terminal de trabajo autentique la tarjeta inteligente. El proceso es el siguiente: la terminal general un número randómico (TRnd) que se mandada a la tarjeta. La tarjeta inteligente opera ese número para obtener un criptograma de autenticación interno (IAC) utilizando la llave de autenticación (Kaut) y el algoritmo triple des, de la siguiente forma: IAC = 3DES(TRnd,Kaut). Este resultado es mandado a la terminal. La terminal realiza las mismas operaciones criptográficas y compara los resultados. Si los resultados concuerdan, la tarjeta inteligente fue autenticada.

2.4.2.4 Firma digital de los datos

La firma digital que se expondrá al final del capítulo es un mecanismo en el que el comando y los datos a enviar a la tarjeta inteligente son pasados por procesos criptográficos con la ayuda de llaves y de algoritmos triple des, para obtener una firma digital. Esta firma es adjuntada al comando y los datos. Cuando la tarjeta recibe el comando, los datos y la firma, realiza las mismas operaciones criptográficas y compara su resultado con la firma mandado por la terminal. Si la comparación no concuerda, entonces la instrucción ha sido alterada.

2.4.2.5 Datos cifrados

Otro mecanismo de seguridad que utiliza la tarjeta inteligente es el de datos cifrados. Consiste en que los datos son enviados a la tarjeta de forma cifrada. La tarjeta los descifra y realiza las operaciones del comando.

2.4.3 Definiendo la seguridad

Al definir la seguridad de una tarjeta inteligente, se debe de tener en cuenta el control de dos vías para el acceso de la información: quien puede accesar a la información y como puede ser accesada la información.

2.4.3.1 Quién puede acceder a la información

Se debe de tener bien claro el quién puede acceder a la información, algunas veces es necesario que todos puedan tener acceso, otras veces, se requiere que sólo el poseedor de la tarjeta, y algunas veces una tercera persona.

- Todos. Algunas tarjetas inteligentes no requieren *password*. Cualquiera que posea la tarjeta puede tener acceso.

- El poseedor de la tarjeta solamente. La más común forma de *password* para un poseedor de la tarjeta es un PIN (Numero Personal de Identificación), de 4 ó 5 dígitos, los cuales son ingresados en un teclado. Si un individuo ingresa erróneamente 3 o 4 veces el PIN la tarjeta puede ser bloqueada.

- Una tercera persona especificada. Algunas tarjetas inteligentes pueden ser accesadas por la parte emisora (ejemplo: las tarjetas de monedero pueden ser usadas por el banco emisor).

2.4.3.2 Cómo puede ser accesada la información

Al definir la seguridad en una tarjeta inteligente se debe tomar en cuenta el tipo de información que se guardara en ella. La información de la tarjeta inteligente puede ser dividida en varias secciones.

- Información que es solamente leída.
- Información que es solamente agregada.
- Información que es solamente modificada.
- Información que no se puede acceder.

2.4.4 Comprometiendo la tarjeta inteligente

Cuando se define la seguridad en la tarjeta inteligente, la meta debería ser siempre llegar a una situación en la que el coste o el esfuerzo del ataque fuera significativamente mayor al beneficio que obtendría si tuviese éxito.

Al hablar de los recursos que se necesitan para comprometer una tarjeta inteligente diríamos que los recursos primarios son: conocimientos, capacidad e inversión. Distintos tipos de ataques requieren distintas capacidades por parte del atacante.

Los ataques al "*hardware*" requieren un cierto grado de ingeniería inversa del "*chip*". Se requiere un cierto nivel de conocimientos de ingeniería para hacerlo, y también cierta capacidad y experiencia en el manejo del equipo y las técnicas requeridas.

Los ataques al "*software*" requieren otro tipo de conocimientos: cálculo, diseño de protocolos y seguridad informática. También requieren una capacidad especial. Las tarjetas inteligentes dependen de la criptografía para su seguridad, como ya se dijo, utiliza mecanismos de seguridad como verificación de contraseña, autenticación externa, firma de datos y datos cifrados. Los conocimientos de criptografía y la capacidad para la misma son diferentes de los requeridos para el "*hardware*" y el "*software*". La criptografía requiere un talento especial.

Al poner en balanza estos requerimientos y sus costes (monetarios y tiempo), y el beneficio que obtendrían, si tuvieran éxito, se vería una marcada diferencia contra los beneficios.

3 INFRAESTRUCTURA DE LA LLAVE PÚBLICA (PKI)

3.1 Definición de PKI

El PKI se basa en la criptografía de clave pública, cuyos orígenes se remontan al artículo semanal de Diffie y Hellman en 1976, donde se explica la idea revolucionaria de servirse para las operaciones criptográficas de una pareja de claves, una pública, conocida por todos, y otra privada, sólo conocida por el usuario a quien le es asignada.

Las propiedades de que goza la criptografía de clave pública, cuyo uso más común se plasma en la firma digital, la convierten en candidata ideal para prestar servicios como la autenticación de usuarios, el no repudio, la integridad de la información, la auditabilidad (para identificar y rastrear las operaciones, especialmente cuando se incorpora el estampillado de tiempo), y el acuerdo de claves secretas para garantizar la confidencialidad de la información intercambiada, esté firmada o no.

PKI confía en la criptografía asimétrica RSA o DSA para encriptar o desencriptar los datos. La criptografía mediante clave pública, de por sí, no basta si deseamos reproducir en un mundo electrónico las condiciones del comercio tradicional basado en el papel. También necesitamos:

- Políticas de seguridad para definir las reglas según las cuales deben funcionar.
- Productos para generar, almacenar y gestionar las claves.
- Procedimientos para establecer cómo generar, distribuir y emplear las claves y certificados.

En esencia, necesitamos una infraestructura de clave pública (PKI). La PKI proporciona el marco de acción para un amplio conjunto de componentes, aplicaciones,

políticas y prácticas para combinar y obtener las cuatro funciones principales de seguridad (confidencialidad, integridad, autentificación y no repudio).

3.2 Componentes de PKI

Una infraestructura de clave pública es una combinación de productos de *hardware* y *software*, políticas y procedimientos. La PKI se basa en identidades digitales conocidas como "certificados digitales", que actúan como "pasaportes electrónicos", y vinculan la firma digital del usuario a su clave pública.

La PKI debe constar de:

- Una política de seguridad.
- Autoridad de certificación (CA).
- Autoridad de registro (RA).
- Sistema de distribución de certificados.
- Aplicaciones habilitadas por PKI.

3.2.1 Política de seguridad

Una política de seguridad establece y define la dirección de máximo nivel de una organización sobre seguridad de información, así como los procesos y principios para el uso de la criptografía. Regularmente establece cómo gestionará la empresa las claves y la información valiosa, y definirá el nivel de control requerido para afrontar los niveles de riesgo.

3.2.1.1 Declaración de practica de certificados (CPS)

Algunos sistemas de PKI se gestionan mediante autorizadores de certificados comerciales (CCA) o terceras partes seguras, y, por lo tanto, requieren un CPS. Éste es un documento en el que se detallan los procedimientos operativos sobre cómo ejecutar la política de seguridad y cómo aplicarla en la práctica. Por lo general, incluye definiciones sobre cómo se construyen y operan los CA, cómo se emiten, aceptan y revocan certificados, y cómo se generan, registran y certifican las claves, dónde se almacenan y cómo se ponen a disposición de los usuarios.

3.2.2 Autoridad de certificación (CA)

En esta se encuentra la base de confianza de una PKI, ya que gestiona los certificados de clave pública durante toda su vida. La función principal de una autoridad de certificación es emitir certificados vinculando la identidad de un usuario o sistema a una clave pública con una firma digital.

Si una organización implanta una PKI, puede manejar su propio sistema de autoridad de certificación (CA), o emplear el servicio de un CA comercial o tercera parte segura.

Aunque desde un punto de vista técnico cualquiera puede erigirse en CA (sólo es necesario disponer de un par de claves pública-privada para firmar y verificar la firma, y todo aquel que desee obtener un certificado las tiene), una CA, además de emitir certificados, debería ofrecer los siguientes servicios:

- Búsqueda de certificados: una persona puede querer buscar el certificado referente a otra persona o entidad.
- La comprobación de la identidad de los solicitantes de los certificados.

- No almacenar las claves privadas de los usuarios, para preservar su privacidad y evitar la posibilidad de que sean suplantados, ya que hasta cierto punto puede decirse que la identidad digital de un usuario reside en su clave privada.
- Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años, con el fin de garantizar que los certificados puedan ser aportados como prueba en los procesos judiciales que pudieran surgir en relación con el uso de la firma.
- Revocación: si un certificado se pierde, el titular debe poder informar a la AC para que lo anule y emita otro. También si la clave privada ha quedado comprometida debe ser posible su revocación.
- Suspensión: la AC debe suspender la validez de un certificado si se hace un uso anormal de él.
- Estado del certificado: las personas a las que se les presenta un certificado deben de poder comprobar que no ha sido revocado o suspendido.
- Programa las fechas en la que expiran los certificados.
- Garantiza que los certificados se revocan cuando sea necesario, publicando listados de revocación de certificados (CRL).

3.2.3 Autoridad de registro (RA)

Una autoridad de registro (RA) proporciona el interfaz entre el usuario y la autoridad de certificación (CA). Su función es capturar y autentificar la identidad de los usuarios y entregar la solicitud de certificado a la autoridad certificadora (CA).

3.2.4 Sistema de distribución de certificados

Los certificados se pueden distribuir de varias formas, dependiendo de la estructura del entorno PKI. Se pueden distribuir, por ejemplo, por los propios usuarios o

a través de un servicio de directorios. Puede que ya exista un servidor de directorios dentro de una organización, o se pude suministrar uno como parte de la solución PKI.

3.2.5 Aplicaciones habilitadas por PKI

Una PKI es un medio para conseguir un fin, que proporciona el marco de seguridad con el que se pueden distribuir las aplicaciones habilitadas por PKI para obtener ventajas finales.

En definitiva, una PKI incluirá una o varias autoridades de registro para certificar la identidad de los usuarios; una o varias autoridades de certificación que emitan los certificados de clave pública; un repositorio de certificados, accesible vía web u otro medio, donde se almacenen los certificados; las listas de revocación de certificados (CRL), donde se listan los certificados suspendidos o revocados; y, por supuesto, los propios certificados.

3.3 Funcionamiento de PKI

Supongamos que Baltasar (B) y Alicia (A) comparten una clave secreta, y que A recibe un mensaje cifrado supuestamente de B. En principio, tras la recuperación exitosa del mensaje, A no tiene ninguna duda de que dicho mensaje proviene de B (autenticación), pero este esquema no es de firma digital porque B siempre puede repudiar el mensaje alegando que realmente lo produjo A.

Sin embargo, este problema se puede resolver fácilmente usando un cifrado de clave pública de la siguiente forma. B envía a A un mensaje cifrado con su clave secreta, A lo descifra con la clave pública de B, y guarda la versión cifrada. Así, si B pretende repudiar su firma, A tiene una prueba definitiva: nadie, salvo B, podría haber generado el mensaje cifrado.

Ahora, ¿como sabría Alicia (A) de que realmente la clave pública es de Baltasar (B) y no de otra persona quien a dicho ser Baltasar y no lo es?, ahí es donde entra la infraestructura de la clave pública.

El proceso para que Baltasar y Alicia tengan una comunicación segura sobre una infraestructura de llave pública sería: una autoridad de registro (RA), obtiene los datos de Baltasar y autentica de que realmente es Baltasar el solicitante, pasa la solicitud a una autoridad certificadora, esta le provee de un certificado con la llave pública y llave privada a Baltasar.

Ya obtenido el certificado, la llave pública de Baltasar puede ser entregada a Alicia por el mismo Baltasar o a través de directorios publicados por la autoridad certificadora (CA). Baltasar envía un mensaje a Alicia encriptado con su llave privada, Alicia lo recibe y desencripta con la llave pública. A puede estar segura de que B lo ha enviado consultando el certificado de la autoridad certificadora quien confirma la identidad de B. Pero, ¿quién garantiza de que el certificado de CA es auténtico?

Para verificar que el certificado es correcto deberíamos hacernos con el certificado digital emitido para dicha CA por una segunda CA. Para verificar la veracidad de este segundo certificado deberíamos obtener el certificado digital emitido para la segunda CA por una tercera CA. Como este proceso podría eternizarse, existen las llamadas autoridades raíz que firman sus propios certificados.

3.4 Implementación de PKI

La PKI resulta ideal en una intranet, en la que se comparten documentos (trabajo en grupo), se accede a recursos de red (cálculo, servidores de archivos, bases de datos, etc.), se intercambia correo certificado entre los empleados, etc. PKI resulta mucho más

ágil que los sistemas tradicionales de control basados en nombre y contraseña y listas de control de acceso.

En el caso de extranets o de Internet, PKI es de uso obligado. De hecho, es la única forma conocida actualmente de prestar confianza, tanto en el comercio entre empresas, como en el comercio al por menor, entre vendedores y compradores particulares por Internet.

Al querer implementar una solución PKI es necesario evaluar que cumpla con los componentes, así como requerimientos adicionales que engrosaran una solución PKI. Éstos son:

- Flexibilidad: todos los componentes de una PKI deberán ser compatibles. Esto es porque es improbable que todos provengan de un mismo proveedor. Por ejemplo, la autoridad certificadora deberá poder conectarse con los sistemas existentes anteriormente.

- Sencillez de manejo: la solución PKI debe permitir que el personal no especializado la maneje con confianza. La interfaz con el usuario debe ser sencilla, grafica e intuitiva.

- Ampliabilidad: inicialmente, una solución PKI sólo soporta una aplicación, pero debe tener la suficiente versatilidad como para soportar más aplicaciones. A medida que crece el PKI deberá poder soportar un número mayor de certificados, esto implica que debe ser posible la adición de componentes de autoridad de certificación (CA) y autoridad de registro (RA).

- Compatibilidad: debido a que la tecnología de PKI aún se encuentra en desarrollo, los estándares para PKI aun están evolucionando y en algunos casos

no existen, para proteger la inversión y evitar problemas de compatibilidad en el futuro, es fundamental que una solución PKI sea totalmente abierta y construida para cumplir los estándares comerciales más comunes.

- La seguridad de la autoridad de certificación (CA) y autoridad de registro (RA): si se pone en entredicho esta seguridad, correrá peligro toda la PKI. La PKI debe garantizar lo siguiente:

    - La clave privada de la autoridad de certificación (CA) debe situarse en un módulo de seguridad a prueba de manipulaciones y se deben realizar copias de seguridad para la recuperación de desastres.
    - El acceso a la autoridad de certificación (CA) y a la autoridad de registro (RA) debe vigilarse muy atentamente, por ejemplo, empleando tarjetas inteligentes para garantizar una mejor autentificación de usuarios.
    - También debe ser posible configurar el proceso de gestión de certificados de forma que un operador deba autorizar las solicitudes de certificación.
    - Todas las solicitudes de certificación deben firmarse digitalmente mediante una fuerte autentificación criptográfica para detectar e impedir a los piratas informáticos que generen deliberadamente certificados falsos.
    - Todas las acciones llevadas a cabo por el sistema de CA/RA deben registrarse en un registro de auditoria seguro, en el que cada entrada tenga asignada una fecha/hora y reciba una firma, para asegurar que las entradas no pueden falsificarse.
    - La CA debe ser aprobada y verificada por un organismo independiente, por ejemplo al menos hasta ITSEC E2, pero preferiblemente hasta ITSEC E3 (criterios de evaluación de seguridad de tecnología de la información). ITSEC es un estándar global reconocido para la medición de productos de seguridad y la evaluación E3 representa el mayor nivel de seguridad comercial de hoy día.

3.5 Alcances y limitaciones de PKI

Los alcances de una infraestructura de llave pública (PKI) están directamente ligados con el alcance de los requerimientos adicionales expuestos anteriormente. Por ejemplo, una interfaz con el usuario sencilla, gráfica e intuitiva generará una amplia aceptación de la infraestructura, esto es sumamente importante ya que el personal (por lo regular) no es especializado.

Si un PKI no es lo suficientemente flexible, se verá limitado al no ser compatible con otros componentes. Que provengan de otros proveedores o de sistemas existentes anteriormente.

Uno de los mayores alcances que puede tener una infraestructura de llave pública sería la ampliabilidad. El hecho de poder adicionar componentes de autoridad de certificación (CA) y autoridad de registro (RA) le da la capacidad de poder soportar un número mayor de certificados.

Podemos concluir que una infraestructura de llave pública puede tener un sinfín de alcances si se implementa de una forma efectiva.

4 APLICACIONES Y USOS MÁS FRECUENTES DEL PKI

4.1.1 Firma de documentos

La firma de documentos es una de las formas de mayor uso de la infraestructura de llave pública. Actualmente se habla de que la eliminación de papeleo en las oficinas es un hecho en el futuro. Detrás de este movimiento se encuentra la infraestructura de llave pública. La firma digital es el equivalente de la firma convencional, en el sentido de que es un añadido al mensaje conforme se esta de acuerdo con lo que allí se dice.

En el área en donde se apreciaría la firma de documentos sería en lo que se conoce como *WordFlow* (Flujo de palabra). Esto consiste en el flujo de documentos que se da dentro de una empresa en que todos por los que pasa el documento, tienen que hacerle revisiones y modificaciones y al finalizar firmar el documento. Con la utilización de PKI podemos asegurarnos de que las personas firmantes, sean en realidad ellas, y que las modificaciones que realizaron fueron hechas por ellas. También se tiene otra ventaja, de que al utilizar una firma digital se elimina la utilización de papel y se agiliza la operatoria *WordFlow*.

4.2 Correo electrónico certificado

La infraestructura de llave pública se utiliza en el correo electrónico de la siguiente forma: en principio, el correo electrónico funcionaba cifrando el documento con la clave privada para obtener una firma digital segura, cualquier persona podría descifrarlo con la clave pública, demostrándose así la identidad del firmante.

En la práctica esto no se da así debido a que los algoritmos de clave pública son muy ineficaces a la hora de cifrar documentos largos, por lo que los protocolos de firma digital se implementan junto con funciones unidireccionales de resumen (*hash*), de manera que en vez de firmar un documento, se firma un resumen del mismo. Este mecanismo implica el cifrado, mediante la clave privada del emisor, del resumen de los datos, que serán transferidos junto con el mensaje. Éste se procesa una vez en el receptor, para verificar su integridad.

Mediante el uso de Microsoft Outlook™ Express o Outlook 98, un usuario puede seleccionar un certificado de clave pública emitido por una entidad emisora de certificados de confianza que se puede utilizar para firmar digitalmente y descifrar mensajes seguros.

4.3 Comercio electrónico

La barrera principal a la adopción de comercio de Internet es la falta de seguridad y confianza. El comercio electrónico entre los negocios y consumidores confía en afianzar los pagos. Pero el mercado del *business-to-business* es mucho más exigente. Requiere un sistema no sólo de firmar las transacciones financieras, también mensajes electrónicos que llevan órdenes, contratos, facturas y otros documentos confidenciales. Las infraestructuras de llave públicas es la solución más prometedora en esta área.

Tanto para las empresas vendedoras como para los clientes, el uso del PKI tiene grandes beneficios. El estar ambos en una infraestructura de llave pública, por un lado las empresas se aseguran de que las órdenes de compra son de sus clientes y que éstos no pueden negar haber realizado el pedido, ya que estaría firmada por su llave, por otro lado, los clientes se aseguran de que las empresas existan, que cuentan con el suficiente respaldo como para realizar el trabajo, y que los documentos que se manejan son validos ya que están firmados. Gracias a la autoridad de certificación, tanto las empresas como los clientes pueden confiar en las llaves que el otro utiliza.

4.4 Transacciones bancarias

La infraestructura de llave pública es de vital importancia en las transacciones bancarias. Los bancos están instalando un sistema de PKI para ofrecer una plataforma segura y fiable para que los clientes comerciales del banco lleven a cabo sus operaciones bancarias por Internet. Con esto, los bancos ofrecen todos los beneficios propios de PKI sobre las transacciones bancarias.

Cuando se realiza una transacción bancaria utilizando una llave pública, tanto el usuario del banco como el banco mismo obtienen beneficios. El usuario puede realizar todo tipo de transacciones gracias a la utilización de las llaves. La comunicación entre el usuario (que se encuentra en un lugar remoto) y el banco se puede realizar encriptando con las llaves la información que se proporcionan y firmando las órdenes de transferencia. Tanto el banco está seguro de que el cliente y sólo el cliente está realizando transacciones y el cliente recibe la seguridad en sus transacciones.

4.5 Autenticación de clientes

La autenticación de clientes implica la identificación y validación de un cliente en un servidor para establecer un canal de comunicación seguro. Un protocolo seguro, como nivel de *sockets* seguros (SSL) o seguridad de nivel de transporte (TLS), se suele utilizar junto con un certificado de clave pública de confianza proporcionado por el cliente, que identifica al cliente en el servidor. El cliente puede ser Internet Explorer ejecutándose en una plataforma Windows, y el servidor, *Internet Information Server* (o algún otro servidor Web que admita SSL/TLS).

La sesión segura se establece mediante la autenticación de clave pública, con intercambio de claves, para derivar en una sola clave de sesión que se puede utilizar y así garantizar la integridad y confidencialidad de los datos durante la sesión. Se puede obtener autenticación adicional mediante la asignación del certificado a una cuenta de usuario o grupo con privilegios de control de acceso establecidos previamente.

4.6 Sistemas de comunicación

Los sistemas de comunicación han incorporado las técnicas de criptografía, y más aún, la infraestructura de llave pública. Ahora es común el establecimiento de servidores web basados en SSL. Como mencionamos en el capítulo 2, SSL es un protocolo de comunicación que hace uso de tanto de la criptografía asimétrica (basada en la existencia de un par de claves, la pública y la privada) como de la criptografía simétrica (basada en la utilización de una única clave secreta).

La infraestructura de llave pública resulta ideal en una intranet en la que se comparten documentos (trabajo en grupo), se accede a recursos de red (cálculo, servidores de archivos, bases de datos, etc.), se intercambia correo certificado entre los empleados, etc. PKI resulta mucho más ágil que los sistemas tradicionales de control basados en nombre y contraseña y listas de control de acceso.

En el caso de extranets o de Internet, PKI es de uso obligado. Las últimas iniciativas de las administraciones públicas para descargar procedimientos administrativos, realizados en papel y sometidos a la venalidad burocrática, hacia procesos digitales interactivos, hacen uso también de tecnología PKI.

4.7 Control de acceso

Con una solución *software* que se implementaría en los ordenadores clientes sería capaz de gestionar todos los eventos relacionados con la sesión de un usuario. Para conseguir esto se modificaría el sistema de control de accesos de Microsoft Windows por un módulo propio; en dicha implementación, se enlaza la gestión de la acción a realizar por parte del propio sistema operativo (abrir, bloquear o cerrar una sesión de usuario) con las operaciones propias sobre la tarjeta inteligente (inserción, extracción,

validación del PIN, lectura de datos administrativos, etc.) y el sistema gestor de acceso y reservas.

Tras su instalación, procede a tomar el control del módulo de accesos de Windows, reemplazando el esquema tradicional de *login*/*password*, por otro basado en la utilización de la tarjeta inteligente. El usuario debe introducir su tarjeta inteligente en el lector que se encontrará en el equipo del cual quiere hacer uso.

Dentro la tarjeta inteligente se tienen las llaves públicas y privadas, con las que se firmará la solicitud de acceso. Según sea definido en la política de control de accesos, se podrá obligar a que el usuario tenga introducida su tarjeta durante el tiempo que se encuentra en el ordenador.

5 PKI SOBRE TARJETA INTELIGENTE

5.1 Introducción

El proceso entero de la infraestructura de llave pública depende de mantener la seguridad y confidencialidad de las llaves privadas. El problema de un ambiente PKI es bastante igual a cualquier otro sistema de criptografía: "el almacenamiento importante seguro". Sin este eslabón esencial, la cadena se rompería cada vez que un usuario se niega a reconocer su firma. Aquí es donde la tarjeta inteligente entra en acción.

En la actualidad, la tarjeta inteligente es la solución más segura para guardar el par de llaves del usuario. Sobre todo para la llave privada, ya que es la parte más sensible del sistema PKI.

5.2 Beneficios de PKI en tarjeta inteligente

Gracias a su microprocesador asegurado, los propios algoritmos codificadores e integrando los dispositivos de anti-piratería, la tarjeta inteligente cierra con llave las llaves publicas y privadas del usuario.

Guardar las llaves en una tarjeta inteligente es como guardarlos en una bóveda del mini-banco. Es por eso que se puede confiar para generar las firmas digitales.

Pero las ventajas de la tarjeta no terminan con la seguridad. Muchos afirman que la capacidad de interactuar con la tarjeta inteligente estará presente en diversos dispositivos habilitados para el comercio electrónico como computadoras personales, equipos de televisión por cable, teléfonos públicos y celulares, etc.

Para un usuario resulta muy útil el llevar una tarjeta que contenga sus llaves y certificados, ya que podría acceder a los mismos servicios no sólo desde su computadora personal o el de su oficina, sino desde quioscos instalados en las oficinas de la empresa que le preste servicio. Todo sin sacrificar la seguridad.

Para una empresa resulta conveniente, ya que el cliente no tiene que conocer los detalles de la criptografía, ni la forma de instalar los dispositivos. Se puede diseñar aplicaciones en los que el usuario simplemente debe instalar un lector compatible y sólo debe de insertar la tarjeta cuando las aplicaciones habilitadas para la criptografía se lo pidan, esto sería cuando haya que firmar un mensaje o descifrar uno que haya recibido.

5.3 Características de tarjeta inteligente para PKI

Podríamos plantear la siguiente pregunta: ¿todas las tarjetas pueden ser usadas para la implementación de PKI? La respuesta sería NO. Existen tarjetas inteligentes diseñadas especialmente para guardar las llaves públicas y privadas de un usuario. Esto es por los requerimientos de criptografía necesarios para las operaciones de firma y descifrado de los mensajes y por los requerimientos de espacio para guardar las claves públicas y privadas en la tarjeta.

Dado que RSA no utiliza intensamente el tiempo de procesador y que la potencia que tiene la tarjeta inteligente es baja, el sistema RSA es el utilizado en las tarjetas inteligentes.

5.4 Tarjetas inteligentes de PKI en el mercado

Distintos fabricantes ofrecen sus tarjetas inteligentes con sus características personales. Uno de estos fabricantes es Gemplus, quien nos ofrece entre su abanico de tarjetas inteligentes, la tarjeta GPK, diseñada para la infraestructura de la llave pública. Basada en esta, Gemplus ofrece GemSafe Logon, GemSafe Enterprise, componentes de una infraestructura de llave pública que incorporan las ventajas de las tarjetas.

5.4.1 GPK (*Gemplus Public Key*)

Figura 7. Tarjeta inteligente GPK

La llave pública de *Gemplus* (GPK) almacena los pares de llaves que se usan en las operaciones de firma digital y cifrado de mensajes. Esta tarjeta tiene un microprocesador capaz de llevar a cabo las operaciones de firma y descifrado de mensajes directamente en la tarjeta.

Con esta tarjeta, la llave privada jamás sale de la tarjeta, lo que permite que incluso si un usuario hace uso de la misma en un equipo en el que hayan sido instalados programas que interceptan los mensajes, no es posible que lleguen a tener acceso a esta clave pues los mensajes dejan el equipo cifrados, viajan hacia la tarjeta y de allí salen en su forma original sin que sea posible conocer los detalles de la forma como la operación fue llevada a cabo.

Adicionalmente, la tarjeta GPK tiene protegida las llaves por una contraseña para tener acceso a ellas. Esto impide que un desconocido pueda usar la tarjeta si ésta es extraviada por su dueño.

Una versión de GPK es la GPK 16000, que fue sacadá en junio de 1999 e incorpora los siguientes rasgos:

- Rápida operación 512 / 768 / 1024 RSA incluyendo una alta seguridad en la generación de llave a bordo.
- Camino de migración hacia las nuevas plataformas abiertas.
- GPK 8000 la compatibilidad ascendente.
- Monedero, niveles de seguridad bancario probado.
- ISO7816-1-2-3-4

5.4.2 GemSafe

Figura 8. Tarjeta inteligente *GemSafe*

Es una tarjeta GPK que fue desarrollada basada en protocolos, algoritmos e interfaces estándar de la industria. Es un componente de una infraestructura de llave pública que contiene todo lo necesario para incorporar las ventajas de las tarjetas proporcionando a las empresas lectores, tarjetas y *software* para tener la funcionalidad en operación en muy poco tiempo sin requerir ningún desarrollo adicional en la PKI disponible en la empresa.

GemSAFE es la heramienta para administrar tarjetas inteligentes en una infraestructura de llave pública y la tarjeta inteligente es el *token* más adecuado al esquema de seguridad de una empresa al nivel mundial.

La tecnología de la tarjeta inteligente usando *GemSAFE* proporciona portabilidad, seguridad y facilidad de uso para abrir el potencial lleno de su solución de PKI.

La tarjeta inteligente proporciona dos formas de autenticación: lo que usted tiene (su tarjeta inteligente) y lo que usted sabe (con PIN de acceso).

La tarjeta puede usarse para realizar las firmas digitales y encriptación de correo electrónico y transacciones de Internet, mientras que proporciona el nivel más alto de no repudiación, un rasgo crucial para la aprobación de B2B, financiero y transacciones de comunicaciones.

Con *GemSafe* sus certificados son portátiles, esto es importante para los usuarios móviles; convenientes y fáciles para usar; y controlable, esto es esencial por su valor elevado en las transacciones comerciales.

5.4.3 GemSafe Logon

Figura 9. Tarjeta inteligente *GemSafe Logon*

GemSAFE Logon es una tarjeta inteligente *GemSafe* 16K, que basó su solución en una simple y amistosa resolución de los problemas relacionados al manejo de la aplicación de control de acceso. Esta tarjeta contiene una aplicación programada especialmente para el control de acceso.

Con esta tarjeta se proporciona una herramienta a los usuarios para guardar sus contraseñas convenientemente y manejar el control de acceso de la aplicación.

Cuando la tarjeta gobierna el acceso de PC, los usuarios pueden escudar su puesto de trabajo fácilmente del acceso desautorizado quitando la tarjeta simplemente del lector.

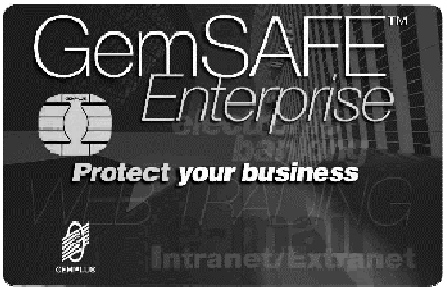
Al querer ingresar en una computadora personal y/o una red, se solicita al usuario que ingrese la contraseña. La tarjeta GemSafe Logon es insertada en el lector de tarjeta, ésta lee la contraseña guardada en su interior lo que permite el acceso. El *software* de GemSafe Logon automáticamente asocia las multiples contraseñas guardadas en la tarjeta con la aplicación correspondiente. Estas aplicaciones pueden ser: SAP, Microsoft Outlook, Windows Logon, etc.

Al dejar la computadora desatendida, la tarjeta debe ser removida, la aplicación que está en uso es cerrada con llave a través de un protector de pantalla seguro que le pide al usuario que inserte la tarjeta y que ingrese un PIN de acceso.

El *GemSAfe* Logon funciona bajo los sistemas operativos de Windows 98, ME, NT, 2000.

5.4.4 GemSafe Enterprise

Figura 10. Tarjeta inteligente *GemSafe Enterprise*



Con *GemSAFE Enterprise*, *Gemplus* ofrece una solución fácil de uso basada en tarjetas inteligentes para mejorar la seguridad de las transacciones de su red.

El objetivo de esta tarjeta está enfocado en proveer una solución segura a cada cliente, usando un servidor basado en Windows para su red.

Entre las funciones que ofrece una estación *GemSafe Enterprice* están:

- Autenticación de usuario y *logon* con tarjeta inteligente.
- Encriptado y firma de correo electrónico.
- Autenticación del cliente en la Web usando SSL.
- Firmar macro en Office 2000.
- Estación de usuario fuera de línea.

6 PROPUESTA

6.1 Definición de la propuesta

La propuesta en el presente trabajo de graduación consiste en la implementación de un sistema de infraestructura de llave pública en una tarjeta inteligente, para la identificación de los extranjeros en Guatemala, como documento de identificación dentro de todo el territorio nacional.

Para la autenticación de usuarios es ideal la firma digital que se logra con la criptografía de clave pública. Como se ha mencionado anteriormente, esta criptografía nos garantiza también la integridad de la información, el no repudio y, algo importante para este sistema, la auditabilidad.

La aplicación consiste en proporcionar de un carné de identidad a cada extranjero que ingrese al país, el cual será una tarjeta inteligente sobre el cual se implementará una infraestructura de llave pública.

El visitante extranjero proporcionara sus documentos de identificación propios del país al que pertenece, se ingresará a la base de datos del sistema y se le personalizará el carné de identificación. Todas las fronteras estarán conectadas al sistema. En cada frontera existirán terminales que tendrán un lector/grabador para las tarjetas inteligentes y una impresora para la impresión de los datos en el plástico.

Además, se tendrán terminales autenticadoras que identificaran la validez de la tarjeta y, por ende, la del extranjero. Estas terminales serán usadas en las salidas del país, en los puestos de registro, etc.

6.2 Componentes del sistema

Definiremos los componentes que contendrá el sistema para definir la infraestructura de llave pública. Como ya mencionamos anteriormente, una PKI es una combinación de productos de *hardware* y *software*, políticas y procedimientos, por tal razón, se indicarán los componentes básicos que debe tener el sistema.

- Una política de seguridad.
- Autoridad de certificación (CA).
- Autoridad de registro (RA).
- Sistema de distribución de certificados.
- Aplicaciones habilitadas por PKI.

6.2.1 Política de seguridad propuesta

Debido a que la definición de una política de seguridad puede ser un documento mayor al presente trabajo, me permitiré referirme a las declaraciones de prácticas de certificados o CPS que son gestionados mediante autorizadores de certificados comerciales (CCA).

6.2.2 Autoridad de certificación propuesto (CA)

Aunque podríamos manejar nuestro propio sistema de autoridad de certificación, debido a que en ésta se encuentra la base de confianza de una PKI, se propone una entidad de certificación comercial que es muy utilizada por empresas bancarias y que posee gran aceptación a nivel mundial, se habla de VeriSign.

La ventaja de elegir una empresa comercial internacional y no nuestro propio sistema es que con esto cumplimos requerimientos adicionales como flexibilidad, ampliabilidad y, sobre todo, la seguridad de la autoridad de certificación.

6.2.3 Autoridad de registro (RA)

Debido a que la RA proporciona el interfaz entre el usuario y la CA y que la función de la autoridad de registro es la captura y autenticación de la identidad de los usuarios, en este caso el Departamento de Migración de Guatemala, y la entrega de la solicitud de certificado a la autoridad certificadora, esta función es cumplida por la CA comercial que se ha propuesto.

6.2.4 Sistema de distribución de certificados a utilizar

Como hemos elegido una autoridad de certificación comercial, el sistema de distribución podría ser la CA elegida, ya que proveen de servicios de búsqueda de certificados. Debido a que nuestros certificados es necesario que se encuentren en las aduanas y aeropuertos del país, podríamos utilizar el servidor central como servidor de directorios.

6.2.5 Aplicación de migración

La aplicación propuesta será utilizada por el departamento de migración de Guatemala y servirá para la autenticación segura de los extranjeros dentro del territorio nacional. Se tendrá un servidor central que tendrá almacenado los certificados propios que se lleguen a tener y la base de datos de los extranjeros. En esta base de datos, se podrá tener una bitácora de entradas y salidas del extranjero, un listado de extranjeros buscados en otros países, extranjeros no gratos para Guatemala, consultas realizadas por el extranjero dentro del territorio nacional, etc.

La aplicación tendrá una interfaz con el usuario sencilla, gráfica e intuitiva, poseerá versatilidad por si en algún momento llegase a implementar la misma aplicación en toda Centroamérica. Con esto engrosaremos la solución PKI que nos darán los requerimientos adicionales como: sencillez de manejo y ampliabilidad.

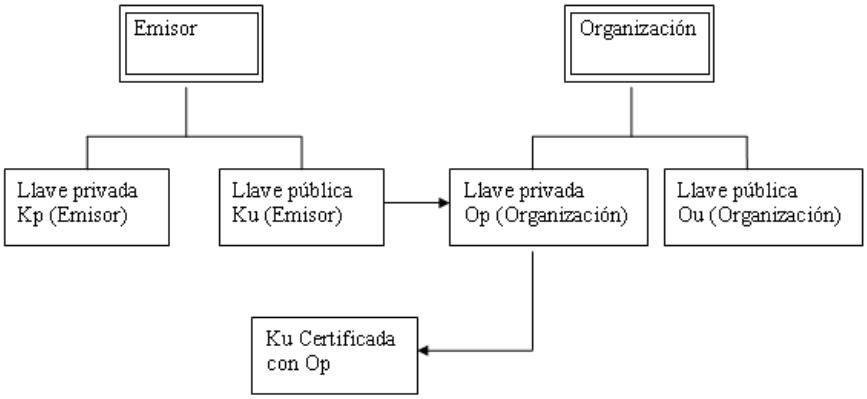
6.3 Funcionamiento de autenticación

A continuación se definirán los pasos necesarios para llegar a la autenticación de una tarjeta en una infraestructura de llave pública. Se identificará al Departamento de Migración como el emisor de las tarjetas, y a la empresa elegida como autoridad de certificación como organización.

Los pasos siguientes son necesarios para la certificación con la empresa de autoridad de certificación (CA).

- Para iniciar, el emisor generará un par de llaves, una pública y una privada.
- El emisor envía su la llave publica (Ku) a la autoridad de certificación u organización y ésta genera el certificado con su llave privada (Op).
- La organización envía la llave pública (Ku) certificada con su llave privada (Op) como se muestra en la figura 11.

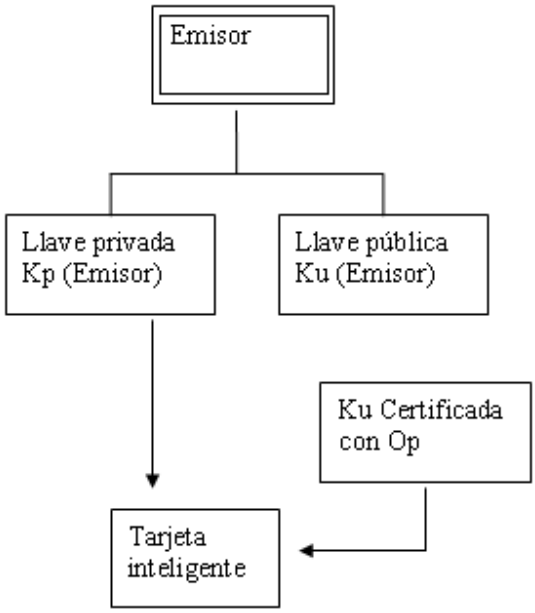
Figura 11. Certificación de llave pública



Los pasos siguientes se refieren a la personalización de cada tarjeta para ser entregada a cada extranjero.

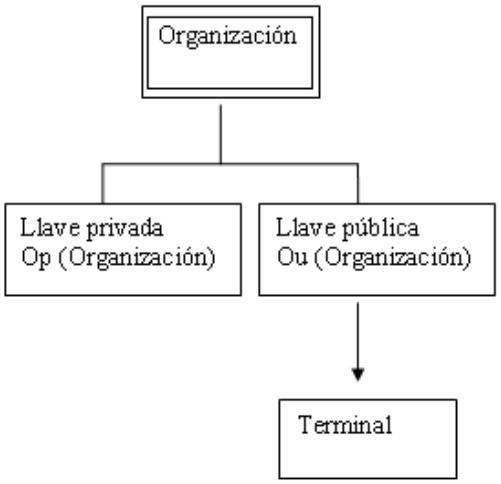
- El emisor genera una firma digital para cada tarjeta utilizando su llave privada (Kp). La firma es guardada en la tarjeta. Ésta es única para cada tarjeta.
- El emisor guarda en la tarjeta su llave pública (Ku) certificada con la llave privada de la organización (Op). Esta llave es única para cada emisor. La figura 12 nos muestra como se personaliza la tarjeta.

Figura 12. Personalización de tarjeta



- La organización tiene publicada su llave pública, ésta es instalada en cada terminal como se muestra en la figura 13.

Figura 13. Personalización de terminal

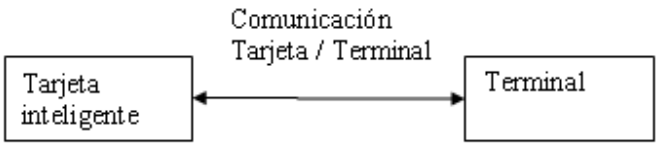


Si existieran más autoridades de certificación, las llaves públicas de éstas también tendrían que estar en las terminales.

Todos los pasos anteriores tienen como fin autenticar la tarjeta inteligente. Los siguientes pasos sirven para autenticar la misma desde cualquier terminal.

- La terminal lee la firma digital generada por el emisor con su llave privada (Kp).
- Junto con lo anterior, lee el certificado generado por la organización (Ku certificada con Op).
- La terminal usa la llave pública de la organización (Ou) para verificar que la llave pública del emisor (Ku) haya sido certificada por la organización. Con esto es verificada la autenticidad del emisor y recupera su llave pública (Ku).
- Con la llave pública del emisor (Ku) la terminal verifica la firma digital de la tarjeta y con esto su autenticidad.

Figura 14. Autenticación de tarjeta



6.4 Alcances y limitaciones del sistema

Los alcances del sistema están directamente ligados con la efectiva implementación del sistema y su uso acertado. Se propone un sistema flexible y con una interfaz de usuario sencilla, lo que generá una amplia aceptación del sistema.

Otro de los alcances que tiene el sistema es que puede ser implementado en el territorio nacional, pero que a su vez puede ser extendido en todo el territorio centroamericano debido a su capacidad de añadir componentes de autoridad de certificación.

Una limitación para este sistema sería el coste inicial del mismo, debido a la compra de los componentes de *hardware* necesarios para su funcionamiento.

CONCLUSIONES

1. Las tarjetas inteligentes se están volviendo una importante y útil herramienta de seguridad para uso en ambientes de computadoras personales. Estándares como JavaCard y PC/SC para tarjetas inteligentes mantienen un potencial casi ilimitado de aplicaciones para computadoras personales.

2. En sistemas de comunicación bancarios, financieros, de salud, de seguridad, por citar algunos ejemplos, las tarjetas inteligentes han demostrado ser las llaves de los mismos transformándose en una utilidad con valor agregado. Millones de transacciones son realizadas cada día con diversos tipos de tarjetas, generalmente para realizar pagos o diversas formas para una rápida identificación.

3. Podemos concluir que una infraestructura de llave pública puede tener un sinfín de alcances si se implementa de una forma efectiva. Esto es, si cumple con los requerimientos adicionales como flexibilidad, sencillez de manejo, ampliabilidad, compatibilidad y la seguridad de la autoridad de certificación (CA) y autoridad de registro (RA).

4. La PKI proporciona el marco de acción para un amplio conjunto de componentes, aplicaciones, políticas y prácticas para combinar y obtener las cuatro funciones principales de seguridad (confidencialidad, integridad, autentificación y no repudio). Debido a esto, PKI es utilizado en una amplia gama de aplicaciones como la firma de documentos, correo electrónico certificado, comercio electrónico, transacciones bancarias,

autenticación de clientes, sistemas de comunicación, control de acceso, etc.

RECOMENDACIONES

1. Que todo emisor de tarjetas inteligentes medite cuidadosamente sobre el nivel de seguridad que desea tener en la tarjeta, en contraste con el tipo de información que posea en ella. Además, que solicite revisiones de seguridad independientes que confirmen que posee un nivel de seguridad adecuado para sus aplicaciones.

2. Definir correctamente cuáles son las necesidades exactas y se elija la estrategia PKI que mejor se adapte a su modelo de negocio. Exija soluciones / productos integrables centrados en su proceso de negocio.

3. Si esta pensando en implementar un PKI sobre una tarjeta inteligente, realice un análisis de costo beneficio de forma minuciosa. Podría ser que en realidad lo que se necesita no es un PKI con una tarjeta inteligente, sino una tarjeta inteligente de menor costo que le dé los mismos beneficios sin arriesgar la seguridad.

4. Acérquese a un experto certificado que pueda asesorarlo para establecer los parámetros de acción y obtener soluciones acordes a sus necesidades y modelo de negocio.

BIBLIOGRAFÍA

1. 2Mil500, S.A. http://www.2mil500.com. (Enero de 2001).
2. *Bull smart cards and terminals*. http://www.smartcard.bull.com. (Junio de 2002).
3. EMV. http://www.emvco.com. (Marzo de 2002).
4. *ETSI specification for GSM*. http://www.etsi.org. (Abril de 2002).
5. *European Smart Card Industry Association. EuroSmart*. http://www.eurosmart.com/index.htm. (Febrero de 2002).
6. *Gemplus cards, readers, and applications*. http://www.gemplus.com. (Enero de 2002).
7. IBM. http://www.chipcard.ibm.com/ (Junio de 2002).
8. Incatel. http://incatel.20m.com/home.html. (Marzo de 2002).
9. *ISO smart card standards*. http://www.iso.ch/cate/3524015.html. (Julio de 2002).
10. Java Card Special Interest Group. http://www.javacard.org. (Mayo de 2002).
11. Key Corp. http://www.keycorp.net/default.htm. (Febrero de 2002).
12. Linux. http://www.linuxnet.com/smartcard/index.html (Febrero de 2002).
13. Map. http://www.map.es/csi/silice/Global30.html. (Abril de 2002).
14. Microsoft Windows for Smart Cards. http://www.microsoft.com. (Abril de 2002).
15. MundoCripto. http://webs.ono.com/usr005/jsuarez/index.htm. (Mayo de 2002).
16. PS/SC Workgroup: http://www.pcscworkgroup.com . (Febrero de 2002).
17. *RSA Security*. http://www.rsasecurity.com/. (Junio de 2002).
18. Sandoval, Juan Domingo y otros. **Tarjetas inteligentes**. España: Paraninfo, 1999.
19. *Schlumberger smart cards*. http://www.1.slb.com/smartcards. (Febrero de 2002).

20. *Siemens smart cards*. http://www.fujitsu-siemens.com/ en/solutions/security /index.html. (Mayo de 2002).
21. *Smart Card Alliance*. http://www.smartcardalliance.org. (Febrero de 2002).
22. *Smart Card Consulting, Development / Tools*. CARDWERK. http://www.cardwerk.com/default.aspx. (Marzo de 2002).
23. *Smart Card Industry Association Knowledge Base*. http://www.scia.org/ knowledgebase/default.htm. (Abril de 2002).
24. Smart Card Sys: http://www.smartcardsys.com. (Marzo de 2002).
25. Verifone. http://www.verifone.com/ (Marzo de 2002).
26. Wilson, Chuck. **Get Smart**. Estados Unidos: Mullaney Publishing Group, 2001.