

Índice

Capítulo I. Introducción	1
1.1 Definición del problema	2
1.2 Antecedentes	5
1.3 Objetivos	8
1.3.1 Objetivo General	8
1.3.2 Objetivos Específicos	8
1.4 Metodología	9
1.5 Estructura del documento	11
Capítulo II. Tecnología de Tarjetas Inteligentes	13
2.1 Definición	13
2.2 Historia y Evolución	15
2.3 Clasificación	23
2.3.1 Según su forma de comunicación	23
2.3.2 Según el tipo de chip	26
2.4 Aplicaciones	28
2.4.1 Servicios financieros	28
2.4.2 Sector salud	29
2.4.3 Identificación	29
2.4.4 Control de acceso físico y presencia	29
2.4.5 Sistemas de votaciones electrónicas	30
2.4.6 Tarjetas telefónicas	31
2.4.7 Entretenimiento	31
2.4.8 Membresía	31
2.4.9 Acceso seguro de datos	32
2.4.10 Telefonía celular y telecomunicaciones	32
2.4.11 Procesos industriales	33
2.5 Características y funcionamiento	33
2.5.1 Características clave	33
2.5.2 Capacidad y desempeño contra costo	36
2.5.3 Tecnologías de memorias	37
2.5.4 Proceso de comunicación	41
2.5.5 Software de las tarjetas inteligentes	46
2.6 Estándares y especificaciones	49
2.6.1 Estándares y especificaciones horizontales	51
2.6.2 Estándares y especificaciones verticales	53
2.7 Conclusión	55

Capítulo III. Seguridad de la Información	56
3.1 Introducción	56
3.2 Elementos de la seguridad de los datos	57
3.3 Mecanismos para la seguridad de los datos	58
3.4 Criptografía	60
3.4.1 Tipos de Criptografía	61
3.4.1.1 Criptografía simétrica.....	61
3.4.1.2 Criptografía asimétrica.....	63
3.4.1.3 Combinación simétrico / asimétrico.....	65
3.4.2 Algoritmo de cifrado DES y 3-DES.....	66
3.4.3 Uso de la criptografía en el proceso de autenticación.....	68
3.4.3.1 Proceso de autenticación de tarjetas inteligentes usando criptografía simétrica	68
3.4.3.2 Proceso de autenticación de tarjetas inteligentes usando criptografía asimétrica	70
3.5 Algoritmos hash y firmas digitales.....	71
3.6 Protocolo de Capa de Socket Segura (SSL).....	72
3.7 Conclusiones	76

Capítulo IV. Diseño del Sistema	77
4.1 Motivación	77
4.2 Requerimientos.....	78
4.3 Diseño del sistema.....	79
4.3.1 Distribución de la información y su administración	80
4.3.2 Arquitectura del sistema.....	85
4.3.2.1 Servidores de administración de bases de datos (DBMS).....	85
4.3.2.2 Servidores de aplicaciones	91
4.3.2.3 Aplicaciones cliente	93
4.3.2.4 Entidades de certificación	95
4.3.2.5 Distribución de los expedientes curriculares electrónicos	97
4.3.3 Seguridad en los enlaces de comunicación	100
4.3.3.1 Uso de redes privadas virtuales en Internet.....	100
4.3.3.2 Conectividad entre clientes y entidades de certificación	102
4.3.3.3 Conectividad entre las entidades de certificación	106
4.3.4 Mecanismo de autenticación e identificación	108
4.3.4.1 Análisis de kits de desarrollo de aplicaciones con tarjetas inteligentes	109
4.3.4.2 Selección del kit de desarrollo	114
4.3.4.3 Autenticación e identificación usando tarjetas inteligentes	117
4.3.5 Datos de la tarjeta inteligente.....	123
4.3.6 Diseño del esquema de almacenamiento de la información personal en la tarjeta	126
4.3.7 Diseño de la estructura de expedientes curriculares electrónicos	132
4.3.7.1 Certificado de Estudios	133
4.3.7.2 Expediente Curricular	133

4.3.7.3 Expediente curricular electrónico.....	133
4.3.7.4 Diseño del expediente curricular electrónico	134
4.3.7.5 Archivo DTD.....	140
Capítulo V. Conclusiones	145
Referencias.....	151
Anexo A – Proceso de personalización de la tarjeta inteligente	159
Anexo B – Estándares ISO / IEC 7816	166
Anexo C – Especificación PC/SC.....	169
Anexo D – Información personal de usuario en la tarjeta inteligente.....	174
Anexo E – Productos generados del proyecto de investigación	177