

UNIVERSIDAD AUSTRAL DE CHILE



FACULTAD DE CIENCIAS DE LA INGENIERIA
ESCUELA DE INGENIERIA CIVIL EN INFORMATICA

DISEÑO DE UNA PKI PARA EL DESARROLLO DE APLICACIONES BANCARIAS SEGURAS SOBRE INTERNET MEDIANTE FIRMA DIGITAL

TESIS DE GRADO PARA OPTAR AL
TITULO PROFESIONAL DE INGENIERO
CIVIL EN INFORMATICA

PATROCINANTE:
CHRISTIAN HAGEDORN HITSCHFELD
INGENIERO CIVIL EN INFORMATICA

CO-PATROCINANTE:
MARTIN SOLAR MONSALVES
DOCENTE

CARLOS ALBERTO VALLEJOS ARCOS

VALDIVIA - CHILE
2002

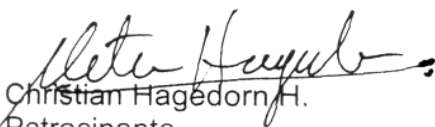
Santiago, 27 de Febrero de 2003

Sra. Miguelina Vega
Directora
Escuela de Ingeniería Civil en Informática
Universidad Austral de Chile
Valdivia
Presente

De mi consideración:

El proyecto de tesis del Sr. Carlos Vallejos "Diseño de una PKI para el desarrollo de aplicaciones bancarias seguras sobre Internet mediante firma Digital" es un aporte al conocimiento de sistemas seguros que faciliten el uso masivo de aplicaciones Internet. Se destaca un esfuerzo personal del estudiante en la comprensión de la tecnología, desarrollo de una metodología para la implementación de estos sistemas, así como el entendimiento de la problemática asociada. Destaca también el desarrollo de un prototipo funcional que complementó el estudio teórico. El Sr. Carlos Vallejos demostró una actitud altamente profesional, cumpliendo cabalmente los objetivos planteados durante el desarrollo del proyecto. Por lo anterior expuesto califico la tesis con nota 7,0 (siete).

Sin otro particular, le saluda cordialmente


Christian Hagedorn H.
Patrocinante

De : Martín Gonzalo Solar Monsalves
A : Directora Escuela Ingeniería Civil en Informática
Ref. : Informe Calificación Trabajo de Titulación

Nombre Trabajo de Titulación:

"DISEÑO DE UNA PKI PARA EL DESARROLLO DE APLICACIONES BANCARIAS SEGURAS SOBRE INTERNET MEDIANTE FIRMA DIGITAL".

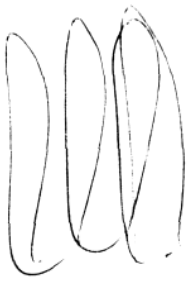
Nombre Alumno:

Carlos Alberto Vallejos Arcos

Evaluación:

Cumplimiento del objetivo propuesto	7.0
Satisfacción de alguna necesidad	6.0
Aplicación del método científico	6.0
Interpretación de los datos y obtención de conclusiones	7.0
Originalidad	7.0
Aplicación de criterios de análisis y diseño	6.5
Perspectivas del trabajo Coherencia y rigurosidad lógica	7.0
Precisión del lenguaje técnico en la exposición, composición, redacción e ilustración	7.0
Nota Final	6.7

Sin otro particular, atte.:



Martín Solar Monsalves



Universidad Austral de Chile

Instituto de Informática

Valdivia. 13 de marzo de 2003

Comunicación Interna N° 027/03

Sra.

Miguelina Vega R.

Directora Escuela Ingeniería Civil en Informática

De mi consideración:

Se me ha solicitado la revisión y evaluación como profesor informante, del Trabajo de Titulación del Sr. Carlos Vallejos Arcos, titulado "-DISEÑO DE UNA PKI PARA EL DESARROLLO DE APLICACIONES BANCARIAS SEGURAS SOBRE INTERNET MEDIANTE FIRMA DIGITAL"

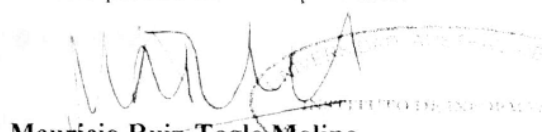
Estimo que el trabajo de titulación de la Sr. Carlos Vallejos cumple los objetivos propuestos, al plantear rigurosamente tanto los fundamentos conceptuales asociados a las transacciones mediante Internet bajo firma digital, como el desarrollo de un prototipo con perspectivas claras de aplicación.

El trabajo del Sr. Vallejos tiene a mi juicio un doble mérito, ya que además del diseño y desarrollo del prototipo, contiene fundamentación teórica de muy buena calidad, asociada a los conceptos relativos a la firma digital, como la criptografía, el comercio electrónico y su marco jurídico.

Sugiero mejorar algunos aspectos formales de la tesis, de modo de no restar calidad al trabajo realizado.

Por todo lo anteriormente expuesto, califico el trabajo de titulación del Sr. Carlos Vallejos con nota 7.0 (siete coma cero).

Sin otro particular. se despide atte.


Mauricio Ruiz-Tagle Molina
Instituto de Informática

AGRADECIMIENTOS

Al momento de finalizar este documento, no quiero dejar de agradecer a todas las personas que de alguna u otra manera me han ayudado durante mi vida, mi carrera y más concretamente a quienes han hecho posible la conclusión de este proyecto

En primer lugar quisiera dar gracias a Dios por todas sus bendiciones y por su infinita misericordia para con mi persona, dar gracias especialmente por la bendición de tener junto a mí a mis padres, Pedro y Amelia, quienes han sido el pilar sobre el que se cimentó mi formación como persona y profesional, y en los cuales encontré siempre la motivación y la fuerza para no desfallecer ante las dificultades y alcanzar continuamente mis metas. Gracias finalmente Señor por permitirme disfrutar la vida con toda la gente que quiero.

Gracias también a ustedes, mis queridos viejitos por soportar todas mis mañas, que no son pocas, y procurarme todo cuanto pudieron y tuvieron a su alcance. Gracias por el ejemplo de esfuerzo y constancia que toda la vida me han dado, y por demostrarme que las cosas son difíciles sólo hasta cuando se comienza a hacerlas.

Quisiera dar gracias también a mis tías, Margarita y Ester por todo su incondicional apoyo y cariño, y gracias también a todos mis otros familiares que de distintas formas me ayudaron y acogieron en el instante que los necesité.

Gracias también a mis amigos y compañeros de universidad junto a los cuales compartí muchas cosas. Gracias también a EFT Banca por haber patrocinado este proyecto, y gracias a todos mis compañeros de trabajo.

TABLA DE CONTENIDOS

INDICE DE FIGURAS	6
INDICE DE TABLAS	8
RESUMEN	9
SUMMARY	11
INTRODUCCION	13
1.1 Preámbulo	13
1.2 Antecedentes Generales	15
1.3 Justificación	18
1.4 Definición de objetivos	20
1.4.1 Objetivos Generales	20
1.4.2 Objetivos Específicos.....	20
COMERCIO ELECTRONICO.....	22
2.1 Preámbulo	22
2.2 Introducción	22
2.3 Internet.....	24
2.3.1 Funcionamiento.....	26
2.4 El E-Comercio	26
2.4.1 Proyecciones del e-Comercio.....	29
2.5 Seguridad del Entorno Virtual	32
2.5.1 Amenazas.....	34
2.5.2 Estadísticas de Seguridad.....	37
2.6 Herramientas y Protocolos de Seguridad	43
2.6.1 Métodos de Control de Acceso	44
2.6.2 Kerberos.....	46
2.6.3 SET	49
2.6.4 SSL	53
2.6.5 S-HTTP.....	57
2.6.6 S/MIME	58
2.6.7 PGP	59
2.6.8 WTLS.....	61
2.6.9 IPSec.....	63
CRIPTOGRAFIA.....	66
3.1 Preámbulo	66
3.2 Introducción	66
3.3 Historia	68
3.4 Criptología	70
3.5 Importancia Estratégica y Legal	73
3.6 Criptosistemas.....	74
3.7 Clasificación de Métodos Criptográficos.....	76
3.7.1 Criptografía Clásica	77
3.7.1.1 Sustitución	77
3.7.1.2 Transposición.....	80
3.7.2 Criptografía Moderna.....	81
3.7.2.1 Números Aleatorios	82
3.7.2.2 Cifradores de Bloque y de Flujo	83
3.7.2.3 Sistemas de Cifrado Simétrico.....	83
3.7.2.3.1 DES	84
3.7.2.3.2 TDES.....	88
3.7.2.3.3 AES	88

3.7.2.3.4	IDEA	90
3.7.2.3.5	BLOWFISH	91
3.7.2.3.6	RC	92
3.7.2.4	Sistemas de Cifrado Asimétrico.....	93
3.7.2.4.1	RSA.....	95
3.7.2.4.2	DSA.....	98
3.7.2.4.3	ECC.....	101
3.8	Funciones Hash.....	102
3.8.1	MD5.....	104
3.8.2	SHA-1	105
3.8.3	RIPE-MD160	105
PKI		107
4.1	Preámbulo	107
4.2	Introducción	107
4.3	Firma Digital.....	109
4.4	Infraestructura de Claves Públicas	114
4.4.1	Políticas de Certificación	116
4.4.2	Autoridad de Certificación.....	117
4.4.2.1	Certificados Digitales.....	119
4.4.2.1.1	Tipos de certificados	121
4.4.2.1.1.1	Certificados de Identificación.....	122
4.4.2.1.1.2	Certificados de Autorización.....	123
4.4.2.1.1.3	Certificados de Transacciones.....	124
4.4.2.1.1.4	Certificados de Tiempo	124
4.4.2.2	Listas de Revocación	125
4.4.2.3	Declaración de Practicas de Certificación.....	128
4.4.3	Autoridad de Registro	130
4.4.4	Repositorio de Certificados.....	131
4.4.5	Jerarquías de Certificación.....	132
4.4.6	Estándares PKI.....	136
4.4.6.1	X.500.....	137
4.4.6.2	LDAP	137
4.4.6.3	X.509.....	138
4.4.6.4	PKCS	144
4.4.6.5	PKIX	148
4.4.6.6	OCSP	148
4.5	Aplicaciones.....	149
4.6	Problemas de PKI	151
MARCO JURIDICO		154
5.1	Preámbulo	154
5.2	Introducción	155
5.3	¿Qué es un Documento y Firma Electrónica?	156
5.4	Aspectos esenciales de una Ley de Firma Digital	159
5.5	Características de las Legislaciones	160
5.5.1	Modelo UNCITRAL	162
5.5.2	Unión Europea	165
5.5.3	EE.UU.....	168
5.5.4	España.....	172
5.5.5	Argentina	179
5.6	La Normativa Legal en Chile.....	183
METODOLOGIA		189
6.1	Preámbulo	189
6.2	Introducción	189
6.3	Planificación de la PKI	190
6.4	Requerimientos	193
6.4.1	Directivas del Negocio.....	194
6.4.2	Aplicaciones.....	195
6.4.3	Usuarios	197
6.4.4	Niveles de Seguridad	198
6.5	Arquitectura	199

6.5.1	Planificación	200
6.5.1.1	CA raíz.....	201
6.5.1.2	CA interna v/s de terceros.....	201
6.5.1.3	Rendimiento y Número de CA.....	204
6.5.1.4	Estructura del Repositorio.....	207
6.5.1.5	Roles de Administración.....	208
6.5.1.6	Proveedores Criptográficos.....	210
6.5.2	Modelo de Confianza	210
6.5.2.1	Modelo Enraizado.....	211
6.5.2.2	Modelo en Red.....	213
6.5.2.3	Modelo Híbrido.....	214
6.5.3	Diseño Estructural.....	214
6.5.3.1	Basada en Uso de Certificados.....	214
6.5.3.2	Basada en la Estructura Organizacional.....	215
6.5.3.3	Basada en la Localización.....	216
6.5.4	Consideraciones de Seguridad	217
6.5.5	Localización de Bases de Datos.....	218
6.5.6	Nombres.....	218
6.6	Configuración Certificados.....	219
6.6.1	Plantillas de Certificados	220
6.6.2	Algoritmos y Largo de Claves	221
6.6.3	Ciclo de Vida	223
6.7	Operaciones	225
6.7.1	Seguridad	226
6.7.2	Plan de Administración de Certificados.....	227
6.7.2.1	Enrolamiento y Emisión.....	227
6.7.2.2	Revocación.....	229
6.7.2.3	Recuperación de claves.....	231
6.7.2.4	Publicación.....	232
6.7.2.5	Renovación	233
6.7.3	Planificación de CPS.....	233
6.8	Despliegue	242
6.8.1	Instalación.....	242
6.8.2	Revisión	243
6.8.3	Actualización	244
DISEÑO PROTOTIPOS PKI.....		246
7.1	Preámbulo	246
7.2	Diseño Prototipo Autoridad Certificadora	246
7.2.1	Ámbito	246
7.2.2	Requerimientos	247
7.2.3	Restricciones.....	249
7.2.4	Modelo Estático	251
7.2.5	Modelo Funcional	253
7.3	Diseño Prototipo Autentificador de Documentos Electrónicos.....	259
7.3.1	Ámbito	259
7.3.2	Requerimientos	259
7.3.3	Restricciones.....	260
7.3.4	Modelo Estático	261
7.3.5	Modelo Funcional	262
7.4	Diseño Prototipo Portal Web Bancario	266
7.4.1	Ámbito	266
7.4.2	Requerimientos	267
7.4.3	Restricciones.....	268
7.4.4	Modelo Estático	268
7.4.5	Modelo de Datos	270
7.4.6	Modelo Funcional	271
PRESENTACION PROTOTIPOS.....		275
8.1	Preámbulo	275
8.2	Desarrollo.....	275
8.3	Recursos utilizados	276
8.4	Presentación Prototipo CA.....	276

8.5 Presentación Prototipo Autenticador de Documentos Electrónicos 286

8.6 Presentación Prototipo Portal Web Bancario 298

CONCLUSIONES 306

9.1 Preámbulo 306

9.2 Conclusiones 306

9.3 Mejoras 309

9.4 Investigaciones futuras..... 310

BIBLIOGRAFIA 313

10.1 Libros y Publicaciones..... 313

10.2 Direcciones Internet 317

GLOSARIO..... 320

LEY 19799 326

CERTIFICACION DE PERSONA 336

CERTIFICACION SERVIDOR..... 340

CRYPTLIB..... 347

MICROSOFT CRYPTOAPI 349

CODIGOS FUENTE 351

INDICE DE FIGURAS

Figura 1: Costo transacciones bancarias en Europa Fuente: Booz Allen & Hamilton.	29
Figura 2: Proyección transacciones B2B Fuente: CCS.	32
Figura 3: Uso no autorizado de Sistemas últimos 12 meses Fuente: CSI.	38
Figura 4: Tecnologías de seguridad utilizadas Fuente: CSI.	39
Figura 5: Orígenes más frecuentes de ataques Fuente: CSI.	39
Figura 6: Dólares perdidos en el 2002 por tipo de ataque Fuente: CSI.	40
Figura 7: Organizaciones que han detectado ataques a su sitio Web Fuente: CSI.	42
Figura 8: Mensaje firmado mediante PGP.	60
Figura 9: Esquema Criptosistema.	75
Figura 10: Diagrama funcionamiento DES.	86
Figura 11: Esquema de generación de firma digital.	111
Figura 12: Esquema de verificación de firma digital.	112
Figura 13: Esquema PKI.	116
Figura 14: Certificado Digital almacenado en IExplorer.	120
Figura 15: Detalle contenido de un certificado digital.	121
Figura 16: Lista de certificado revocados.	126
Figura 17: Detalle lista de certificados revocados.	127
Figura 18: Jerarquía de certificación compuesta.	135
Figura 19: Formato ASN.1 certificado X.509.	139
Figura 20: Propiedades campos de certificado.	141
Figura 21: Formato ASN.1 CRL.	142
Figura 22: Características legislaciones Latinoamericanas Fuente: CCS.	161
Figura 23: Visión general metodología implantación PKI.	193
Figura 24: Principales pasos para definir requerimientos.	193
Figura 25: Principales pasos para definir la arquitectura.	200
Figura 26: Modelo de confianza jerárquica enraizada.	212
Figura 27: Modelo de confianza jerárquico en red.	213
Figura 28: Estructura basada en el uso de certificados.	215
Figura 29: Jerarquía basada en la estructura organizacional.	216
Figura 30: Jerarquía basada en la localización.	217
Figura 31: Principales pasos para configurar certificados.	220
Figura 32: Principales pasos para definir las operaciones.	226
Figura 33: Principales pasos para el despliegue.	242
Figura 34: Funcionalidades prototipo CA.	249
Figura 35: Modelo estático prototipo CA.	251
Figura 36: Modelo funcional prototipo CA.	254
Figura 37: Descomposicion funcionalidades prototipo CA.	255
Figura 38: Proceso Generar Claves CA.	255
Figura 39: Proceso Emitir Certificado CA.	256
Figura 40: Proceso Generar Claves Usuario.	256
Figura 41: Proceso Emitir Certificado Usuario.	257
Figura 42: Proceso Publicar Certificado.	257
Figura 43: Proceso Exportar Certificado.	258
Figura 44: Proceso Revocar Certificado.	258
Figura 45: Proceso Publicar CRL.	259
Figura 46: Funcionalidades prototipo Autenticador documentos electrónicos.	260
Figura 47: Modelo estático prototipo Autenticador documentos electrónicos.	262
Figura 48: Modelo funcional prototipo Autenticador documentos electrónicos.	262
Figura 49: Descomposición funcionalidades prototipo Autenticador.	263
Figura 50: Descomposición firma documento.	264
Figura 51: Descomposición verificación firma documento.	264
Figura 52: Descomposicion cifrado de documento.	265
Figura 53: Descomposición descifrado de documento.	266
Figura 54: Funcionalidades prototipo Portal Web Bancario.	268
Figura 55: Modelo estático prototipo Portal Web Bancario.	269
Figura 56: Modelo funcional prototipo Portal Web Bancario.	271
Figura 57: Descomposición funcionalidades Portal Web Bancario.	272

Figura 58: Descomposición autenticar usuario.	273
Figura 59: Descomposición realizar servicio.	273
Figura 60: Descomposición firmar transacción.	274
Figura 61: Cuadro presentación prototipo CA.	277
Figura 62: Cuadro inicio de sesión prototipo CA.	277
Figura 63: Cuadro administración prototipo CA.	278
Figura 64: Pantalla emisión certificados persona.	278
Figura 65: Pantalla emisión certificados servidor.	279
Figura 66: Cuadro confirmación publicación CRL.	279
Figura 67: Pantalla búsqueda de certificados.	280
Figura 68: Cuadro bloqueo de aplicación.	280
Figura 69: Cuadro confirmación publicación certificados.	280
Figura 70: Pantalla exportar certificado y claves a formato PKCS #12.	281
Figura 71: Menú emergente para certificados válidos.	282
Figura 72: Resultado Menú Abrir Certificado.	282
Figura 73: Cuadro confirmación eliminar certificado.	282
Figura 74: Cuadro confirmación publicar certificado.	283
Figura 75: Cuadro revocar certificado y opciones de revocación.	283
Figura 76: Menú emergente para certificados revocados.	284
Figura 77: Menú Configuración de la aplicación.	284
Figura 78: Menú Acción de la aplicación.	285
Figura 79: Visualizar archivo de eventos de la CA.	285
Figura 80: Cuadro confirmación firmar archivo eventos CA.	286
Figura 81: Pantalla presentación prototipo autenticador.	286
Figura 82: Pantalla principal prototipo autenticador.	287
Figura 83: Pantalla presentación de archivo a firmar.	288
Figura 84: Pantalla de selección de certificado para firma.	288
Figura 85: Certificado utilizado para firmar documento.	289
Figura 86: Cuadro confirmación de acceso a clave privada.	289
Figura 87: Cuadro proceso de firma terminado.	290
Figura 88: Visualización archivo de texto firmado.	290
Figura 89: Menú cambio tipo de archivo a firmar.	291
Figura 90: Cuadro descripción de código a firmar.	291
Figura 91: Cuadro solicitud certificado para firma de código.	292
Figura 92: Pantalla visualización archivo para verificar firma.	293
Figura 93: Cuadro de confirmación verificación de firma.	293
Figura 94: Certificado asociado a firma de documento.	294
Figura 95: Cuadro confirmación verificación firma archivo código.	294
Figura 96: Cuadro información firmante archivo de código.	295
Figura 97: Certificado asociado a firma archivo de código.	295
Figura 98: Cuadro destino archivo a envolver.	296
Figura 99: Cuadro selección ruta archivo a envolver.	296
Figura 100: Cuadro selección de destinatarios del mensaje.	296
Figura 101: Cuadro mensaje fin proceso de envoltura.	297
Figura 102: Visualización archivo de texto cifrado.	297
Figura 103: Cuadro selección ruta destino archivo descifrado.	297
Figura 104: Cuadro mensaje fin proceso descifrado.	298
Figura 105: Página principal prototipo Web.	299
Figura 106: Cuadro solicitud de autenticación del cliente.	300
Figura 107: Cuadro solicitud contraseña del certificado.	300
Figura 108: Pagina de servicios del prototipo bancario.	301
Figura 109: Pagina servicio de transferencia de fondos.	302
Figura 110: Cuadro alerta de acceso a certificado digital.	302
Figura 111: Cuadro información selección certificado para firma.	303
Figura 112: Cuadro selección de certificados para firma.	303
Figura 113: Cuadro alerta de acceso a clave privada.	304
Figura 114: Cuadro solicitud contraseña para acceso a clave privada.	304
Figura 115: Pagina de información termino de transacción.	305
Figura 116: Imagen tabla Firmas.	305
Figura 117: Zoom campo firma de tabla Firmas.	305
Figura 118: Arquitectura Microsoft CryptoAPI.	349

INDICE DE TABLAS

Tabla 1: Usuarios Internet y hábitos de consumo Fuente: CCS.....	30
Tabla 2: Proyecciones Comercio B2C en Chile Fuente: CCS.....	30
Tabla 3: Porcentaje empresas conectadas a Internet Fuente: CCS.	31
Tabla 4: Ejemplo cifrado sustitución de Cesar.	79
Tabla 5: Ejemplo cifrado sustitución polialfabética.....	79
Tabla 6: Cifrado de transposición por columnas.	80
Tabla 7: Comparación fortaleza relativa de claves ECC y RSA.	102
Tabla 8: Abreviaturas para el campo identidad.....	140
Tabla 9: Cronología Leyes de Firma Digital.	158
Tabla 10: Tabla Ejemplo definición de requerimientos.....	198
Tabla 11: Ejemplo roles administrativos PKI.	209
Tabla 12: Ejemplo lista de acciones realizadas por roles PKI.....	209
Tabla 13: Ejemplo ciclos de vida de certificados.	225
Tabla 14: Descripción actor usuarios.	252
Tabla 15 : Descripción actor CA.....	252
Tabla 16: Descripción tabla Clientes.	270
Tabla 17: Descripción tabla Transacciones.....	271
Tabla 18: Descripción tabla Firmas.....	271
Tabla 19: Resumen algoritmos y parámetros utilizados por Cryptlib.....	347

RESUMEN

Desde el establecimiento de Internet como medio común de comunicación, el e-comercio ha experimentado un vertiginoso crecimiento, con el consecuente aumento en el número de transacciones de bienes y servicios realizados a través de este mundo virtual.

Hoy en día, se procesan, almacenan y transmiten diariamente más datos que en cualquier otro período de la humanidad. De forma adicional, no sólo ha aumentado el volumen de la información que se procesa sino que también en alto grado su importancia.

Por consiguiente, la seguridad de los sistemas que administran dichas transacciones y sus datos asociados, se convierte en un problema de vital importancia para el progreso del e-comercio y la sociedad digital. Bajo este punto de vista, el presente trabajo de tesis busca afrontar la problemática de mejorar la seguridad en el ámbito del desarrollo de aplicaciones Internet orientadas a la banca y plantear una alternativa a los sistemas actuales.

En esta búsqueda, el trabajo de tesis analiza la situación actual del e-comercio, las bases sobre las cuales se ha construido la seguridad de la información y los aspectos fundamentales que definen seguridad, y con los cuales toda aplicación que utilice Internet como medio de operación debiera contar.

La solución que esta tesis propone para el problema implica el diseño e implementación de una Infraestructura de Claves Públicas y la utilización de la firma digital como herramientas garantes de la seguridad en los servicios proporcionados en un entorno Web. Ya que estas herramientas se han visto beneficiadas además de

la reciente promulgación en nuestro país de la “Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma”, que avala para efectos legales a los documentos electrónicos y la utilización en ellos de la firma digital.

SUMMARY

Since the appearance of Internet as common mean of communication, the e-commerce has experienced a vertiginous growth, with the consequent increase in the number of transactions of goods and services carried out through this virtual world.

Nowadays, more data than in any other period of the humanity are processed, stored and transmitted daily. Of additional form, it has not only increased the volume of information processed but also in the extreme its importance.

Therefore, system's security that manage these transactions and its data associated becomes a problem of vital importance for the progress of e-commerce and the digital society. Under this point of view, the present thesis looks for to confront the problem of to improve the security in the environment of development of Internet applications oriented to the banking, and propose an alternative to the present systems.

In this search, the thesis work analyzes the present situation of the e-commerce, the bases on which the security of the information has been constructed and the fundamental aspects that define security and with which every application that uses Internet as mean of operation should count.

The solution that this thesis proposes for the problem implies the design and implementation of an Infrastructure of Public Key and the use of the digital signature as guarantor tools of the security of the services provided in Web environment. Since these tools have been beneficiated with the recent promulgation in our country of "Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha

firma”, that endorses for legal effects to the electronic documents and the use in them of the digital signature.

1.1 Preámbulo

La transformación de Internet en un medio habitual de comunicación, el auge del e-comercio, la convergencia de las telecomunicaciones hacia la, el aumento de los anchos de banda y la baja en los costos de conexión, entre otras varias razones han llevado sin duda a un aumento de las transacciones realizadas de forma electrónica, debido a sus ventajas en cuanto a reducir costos y tiempos comparado con hacer las mismas actividades de forma presencial.

Sin duda no sólo ha crecido de manera explosiva la cantidad de información que es procesada, almacenada y transmitida por la mayor red pública del planeta sino que también ha aumentado su grado de importancia.

Este increíble crecimiento de los datos circulantes y de las redes computacionales que los transmiten, ha sido uno de los factores más importantes que ha llevado a la seguridad en el uso de sistemas informáticos a cobrar una relevancia vital, sobre todo en aquellos que se encuentran interconectados a Internet, ya que esta interacción, si bien trae consigo muchas posibilidades de compartir información y agilizar numerosas actividades que antes requerían la presencia formal de los individuos, también trae consigo diversos peligros, los que pueden provenir desde cualquier parte del mundo. Esto debido a que la red por sus características permite el anonimato, lo que dificulta garantizar la identidad de las personas que se relacionan mediante este medio de comunicación.

En esta nueva sociedad global llamada también de la información, aumenta entonces la preocupación y desconfianza por la identidad de las personas, la correcta utilización de los datos y la protección de estos para evitar que sean interceptados y mal utilizados por los Ciberdelincuentes¹.

Dentro de este panorama, las empresas -que ya consideran a la información como parte prioritaria dentro de sus activos- y también las personas, se enfrentan a una creciente realidad, la necesidad de seguridad en los datos, los servicios, las transacciones y las partes involucradas en estas operaciones.

Hasta el momento la seguridad de los sistemas informáticos y los datos que estos manejan, se ha basado en la restricción del acceso y en la criptografía o proceso de hacer ilegible la información. En el primero de los casos la forma más común de administración del acceso a la información es mediante la utilización de un nombre de usuario y una contraseña, en el segundo es el cifrado de los datos mediante una clave secreta que debe ser compartida por dos o más entes confiables.

Pero estos procedimientos por las características de las personas que los utilizan no son suficientes para garantizar una serie de aspectos de seguridad que se transforman en una necesidad a ser satisfecha por cualquier aplicación orientada a la plataforma Web, como son la autenticidad, confidencialidad, integridad y el no repudio de transacciones.

Debido a esto es necesario desarrollar herramientas y aplicaciones que permitan disminuir la desconfianza e inseguridad en las transacciones que ocurren en el mundo virtual y que satisfagan las necesidades antes mencionadas, para así ayudar a que el comercio electrónico y la sociedad digital prosiga con su acelerado

¹ Delincuentes informáticos.

crecimiento, ya que como toda actividad humana requiere de la necesaria confianza para su desarrollo.

1.2 Antecedentes Generales

La seguridad no tiene una definición estricta ni tampoco un objetivo único, pero si posee algunos aspectos o servicios fundamentales que permiten la construcción de una solución eficiente en el envío de información sensible a través de una red pública como Internet, entre estos destacan:

- *Confidencialidad*
- *Integridad*
- *Autenticidad*
- *No repudio*

- **Confidencialidad**

Es la característica de un servicio de seguridad que se refiere a garantizar que la información no puede ser revelada o no pueda ser alcanzada por personas no autorizadas para tales efectos, para garantizar este aspecto se utilizan el control de acceso a la información y el cifrado de los datos.

- **Integridad**

Es el aspecto de seguridad referido a garantizar que la información no ha sido alterada por personas no autorizadas, ya sea para agregar o quitar datos, bien de forma accidental o intencional.

- **Autenticidad**

Este aspecto de la seguridad trata de proporcionar los medios para comprobar que el origen de cierta información es el correcto, y determinar ese origen, para de esta forma evitar la suplantación de identidades.

- **No repudio**

Esta característica permite asegurar que cualquier ente participante en una transacción no puede negar haber realizado una acción determinada, por ejemplo no puede negar el envío o recepción de datos.

El orden o prioridad que se les da a estos aspectos depende mucho del entorno del sistema que los aplique, pues por ejemplo en el ámbito militar la característica más importante podría ser la confidencialidad siendo los demás aspectos menos críticos, en un ambiente de transacciones bancarias por otro lado, la integridad, autenticidad y no repudio de una transferencia de fondos sería mucho más importante que la confidencialidad de ésta.

Es en este entorno, el bancario, donde el presente trabajo de tesis apunta a mejorar las condiciones de seguridad. Hasta este momento las aplicaciones Web bancarias utilizan como medio de identificación de sus usuarios un nombre o palabra que los identifica de forma única en el sistema², asociado a este identificador existe una contraseña que sólo el usuario debe conocer, con lo que se demuestra que éste es quien dice ser.

Este método de identificación sería infalible si los usuarios utilizaran una buena política de contraseñas, como podría ser utilizar extensas combinaciones de números y letras, pero a media que las contraseñas se hacen más complejas para

dificultar su descubrimiento, son más difíciles de recordar, por lo que los usuarios prefieren utilizar contraseñas cortas y fáciles de imaginar, lo que las hace factibles de ser adivinadas por terceros.

Por otro lado no hay una forma clara de garantizar el no repudio de una transacción en el entorno bancario, puesto que como usuario perfectamente se puede fundamentar que la contraseña a sido descubierta -no necesariamente por un error propio- y que no se ha dado origen a una transacción ya realizada, no teniendo la contraparte en este caso el banco forma de probar lo contrario, lo que además puede terminar en largas y costosas disputas.

Adicionalmente, hasta ahora la forma de comprobar una transacción es manteniendo un registro o archivo electrónico donde se encuentran los datos asociados a dicha acción, los que pueden ser alterados, por lo que no cuentan con un respaldo legal concreto.

En definitiva la pregunta que a la que se pretende dar respuesta es ¿Cómo mejorar esta situación?, ¿Cómo mejorar las aplicaciones Web bancarias para proporcionar los servicios básicos de seguridad antes descritos?.

Como respuesta, este trabajo de tesis plantea la utilización de la firma digital apoyada por la reciente “Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma” y la Infraestructura de Claves Públicas o PKI como solución a la problemática presentada.

Por lo tanto se proyecta la construcción de un prototipo de PKI que apoye los servicios de las entidades bancarias, como por ejemplo los sistemas de pago y transferencias electrónicas vía Web, y que permita el intercambio de documentos

² Generalmente se utiliza el RUT del individuo.

digitales firmados electrónicamente garantizando su autenticidad, confidencialidad, integridad y no repudio. Para ello se proporcionará a los usuarios las herramientas necesarias que les permitan la firma de documentos electrónicos y la verificación de éstos.

1.3 Justificación

Entre las razones que justifican la realización de este proyecto está el impacto que tendrá en el país y el mundo esta tecnología, debido a que distintas naciones están realizando grandes esfuerzos para apoyar la firma digital y desarrollar un marco jurídico que avale la utilización de ésta.

También por la seguridad que proporciona a las organizaciones y personas al momento de realizar transacciones a través de Internet, disminuyendo los riesgos de fraudes y minimizando las pérdidas por disputas o conflictos judiciales.

Porque puede garantizar la confidencialidad, veracidad e integridad de las comunicaciones, fomentando así el desarrollo del e-comercio y la sociedad digital.

Por las mejoras que puede realizar a la gestión pública y privada, aumentando la eficiencia, la eficacia y el ahorro en recursos humanos y materiales ya que permite el reemplazo de los documentos firmados físicamente por archivos firmados de forma digital.

Por su uso potencial en el ambiente de la administración estatal, donde se puede publicar todo tipo de información y comunicados de carácter oficial firmados digitalmente por el Estado. Además se podrá realizar cualquier tipo de tramitación ante la administración pública³ donde de ser necesaria una firma manuscrita será

³ El Estado está preparando un proyecto de ventanilla única a través del Web, donde realizar entre otros el pago de impuestos.

suficiente con su homóloga electrónica. Todo este tipo de actos por supuesto se podrá realizar también en un entorno de privados. Otra de las principales aplicaciones para el Estado está también en el ámbito de la democracia, donde basados en esta tecnología se puede desarrollar un sistema de sufragio electrónico.

Sin duda una de los principales servicios que pueden aprovechar la firma digital es la mensajería de información sensible a través del correo electrónico, donde el emisor puede ser identificado de manera innegable mediante su firma digital.

Las redes es otro nicho de aplicaciones por ejemplo, los paquetes de información que son enviados sobre éstas también pueden ser asociados a un emisor dando la posibilidad de establecer reglas de filtrado de paquetes similares a un Cortafuego.

En el ambiente del comercio virtual los bancos pueden implementar de igual manera una forma de chequera o dinero electrónico.

Como se puede ver en este pequeño espectro de posibles aplicaciones, la tecnología es aplicable a cualquier ambiente que necesite identificar a sus usuarios de forma inapelable y que además requiera la obtención de pruebas referidas a la conformidad de las partes en algún tipo de transacción o contrato electrónico, por lo que se justifica cualquier esfuerzo en su investigación y desarrollo.

1.4 Definición de objetivos

1.4.1 Objetivos Generales

Los objetivos generales del proyecto son:

- Hacer un estudio profundo y comprender las características de una PKI, la tecnología de firma digital y el marco jurídico nacional desarrollando para dar el soporte a esta tecnología.
- Proponer una metodología de implementación de un sistema de certificación digital.
- Realizar el diseño e implementación de prototipos PKI que permitan complementar el estudio teórico.
- Realizar la implementación de un prototipo de servicio bancario que aproveche las características de la PKI implementada y utilice las características de confidencialidad, integridad, autenticidad y no repudio de la firma digital.

1.4.2 Objetivos Específicos

Los objetivos específicos para el proyecto de PKI son:

Para comprender las características de una PKI:

- Definir conceptos como criptografía, firma digital, certificados digitales y funciones de resumen.
- Describir características y funcionamiento de una infraestructura de Claves Públicas y sus componentes.

- Describir los estándares y protocolos que rigen una infraestructura de Claves Públicas.
- Analizar el marco jurídico nacional y el de otros países de la región, sobre documentos electrónicos y firma digital.

Para diseñar una PKI:

- Definir un modelo de la Infraestructura de Claves Públicas.
- Definir los tipos de algoritmos de encriptación a utilizar en la generación de las claves.
- Diseñar una autoridad certificadora y si es necesario una o varias autoridades de registro.
- Definir la configuración de la Autoridad certificadora.
- Definir usos e información de los certificados digitales.

Para diseñar los prototipos:

- Definir funcionalidades de los prototipos.
- Definir un modelo de funcionamiento para cada prototipo.
- Definir requerimientos en cuanto a plataforma, servicios, seguridad y herramientas a utilizar.

CAPITULO II

COMERCIO ELECTRONICO

2.1 Preámbulo

El objetivo de este capítulo es proporcionar una visión acerca de los comienzos del comercio electrónico su desarrollo y algunas proyecciones, sin dejar de lado un rápido vistazo a los inicios de Internet, también se explora algunos de los problemas que afectan a Internet y al comercio virtual, como son los niveles de seguridad de este entorno, así como la delincuencia virtual, lo que lleva a describir algunas de las herramientas utilizadas para resolver estos inconvenientes. Todos antecedentes que sirven para ayudar a comprender mejor las implicancias que el problema presentado tiene y demostrar el valor del estudio aquí desarrollado.

2.2 Introducción

Internet ha supuesto una revolución sin precedentes en la historia de la humanidad, en el mundo de la informática y de las telecomunicaciones, la invención del telégrafo, teléfono, la radio y los computadores sentaron las bases para la integración de las múltiples capacidades que posee Internet, las que nunca antes habían sido experimentadas por la humanidad.

Internet es una oportunidad de difusión mundial, un mecanismo de propagación de información y un medio de colaboración e integración entre los individuos y sus computadores; También es una forma de esparcimiento, es un televisor, una radio, una consola de juegos; Es también una manera de educarse y aprender, es una escuela, una biblioteca, una universidad; Se ha convertido también

en una forma de comerciar y transar bienes o servicios ya que se ha transformado en un banco, un comercio, una tienda, etc. En definitiva se ha involucrado en todas las actividades de las personas.

Hoy en día una de estas actividades, la de comerciar, está teniendo un explosivo crecimiento, cada vez más personas descubren las ventajas de realizar sus negocios en línea, desde la comodidad de sus casas o desde el trabajo, pero con esto también han surgido algunas preguntas y dudas por parte de los usuarios referentes a la seguridad de realizar sus actividades por Internet, y que de no ser respondidas en forma clara, sólo les inhibirá el deseo de una mayor utilización del mundo virtual.

Estas preguntas se refieren por ejemplo a: ¿Es realmente seguro comprar a través de Internet?, ¿Es seguro introducir un número de tarjeta de crédito en un formulario de una página Web?, ¿Se utilizarán los datos introducidos de forma adecuada?.

Todo estas preguntas y otras, están referidas sin duda a la seguridad y confidencialidad de la información, además de la legalidad de este tipo de transacciones.

Durante los últimos años ha aumentado también la preocupación de las empresas por el tema, con el consecuente crecimiento de las inversiones en seguridad de éstas para contrarrestar las falencias en el área, todo para dar garantías a sus clientes y responder a las interrogantes anteriormente planteadas, tratando así de fomentar la masificación de los negocios en línea.

Pero toda esta revolución y preocupaciones que hoy nos afectan tuvieron su origen ya hace algún tiempo con el nacimiento de las redes de comunicaciones, que no está de más recordar.

2.3 Internet

Internet es una red global de computadores compuesta por muchas otras redes más pequeñas y basadas en distintas arquitecturas tanto topológicas como funcionales, las que permiten el transporte de datos electrónicos a través de ellas.

Sus albores se remontan a los años de la guerra fría aproximadamente 1960, en donde el miedo a un ataque con artefactos nucleares con capacidad de destruir los centros de control informáticos de armas creó la necesidad de implementar una red que pudiera ser empleada desde cualquier lugar.

En aquel entonces, el problema de la comunicación en un hipotético entorno de devastación, se convirtió en un punto estratégico de la defensa, en el que se planteaba la posibilidad de comunicar con éxito a las autoridades y organismos de defensa norteamericanas tras recibir un ataque con bombas atómicas. Se necesitaba entonces de una red de comando y control enlazado. Otra de las dificultades planteadas era ¿Cómo se iba a controlar esta red?, Ya que cualquier entidad central o núcleo sería el primer objetivo a alcanzar por un misil del enemigo, el centro sería el primer lugar a derribar.

Fue entonces cuando ARPA⁴ rama científica de las fuerzas armadas estadounidenses, inició la implementación de una red con las características ya mencionadas y anunció el diseño de una red de computadores que podría sobrevivir

⁴ Advanced Research Projects Agency.

a cualquier tipo de ataque, nace entonces ARPANET⁵, red de orientación exclusivamente militar, los principios de esta red eran simples, se asumiría que ésta era poco fiable y su diseño estaría enfocado para trascender su propia falta de eficiencia, todos los nodos serían iguales ya que todos tendrían la posibilidad de crear, enviar, y recibir mensajes, los que se dividían en paquetes y cada paquete se podría dirigir por separado, éstos deberían encontrar una ruta a su destino obviando cualquier interrupción en la red, estos paquetes saldrían de un nodo fuente específico y terminarían en un nodo destino, donde cada uno recorrería la red según principios particulares y la ruta no tendría importancia, sólo importarían los resultados finales, o sea, que llegaran a su destino. Como se ve la seguridad no era prioritaria.

En un comienzo esta red contó con pocas máquinas, utilizadas sólo por usuarios académicos e investigadores de ARPA junto con otros órganos de gobierno de los Estados Unidos, los que comenzaron a darle mayor uso, la red fue creciendo de forma exponencial y llegó al punto que su protocolo estándar para la transferencia de datos, el NCP⁶, quedó obsoleto.

Así en 1974 nace el protocolo TCP/IP como una solución al problema de tráfico, protocolo de más alto nivel y más sofisticado. ¡He aquí los comienzos de Internet!.

Posteriormente la red continuará su evolución hasta que un grupo de estudiantes universitarios descubre uno de los principales servicios de Internet, el Web, y programan el primer navegador para éste, el Mosaic, que permitía tener acceso a imágenes y documentos de texto desde las máquinas conectadas a la red.

⁵ Advanced Research Projects Agency Net.

⁶ Network Control Protocol.

Posteriormente en los años 80 ARPANET se separa de la red militar que la originó, formando MILNET⁷, de modo que al no contar ya más con fines militares se puede considerar este momento como el nacimiento de la Internet que hoy conocemos.

2.3.1 Funcionamiento

Internet funciona basada en una arquitectura cliente-servidor, donde cada computador es un cliente, si su objetivo es acceder a algún tipo de información y es un servidor en el caso contrario o sea cuando el objetivo sea entregarla. Para comunicarse cada computador usa un estándar, el protocolo TCP⁸, que regula las peticiones de información entre clientes y servidores.

Este protocolo define la manera en que la información será dividida en un caudal de pequeños paquetes y posteriormente enviada a través de Internet, también se encarga de que al llegar a su destino estos paquetes sean reensamblados de forma apropiada y de controlar los posibles errores producidos durante el trayecto, por lo que permite la interconexión de cualquier tipo de computador que hable en este idioma. Otra de sus características es el de ser un protocolo público, es decir no existe una única compañía responsable que lo desarrolle o lo guarde en secreto, más bien todo lo contrario. Además el protocolo puede utilizar casi cualquier método existente de transmisión siendo esto una de las razones de la expansión de Internet.

2.4 El E-Comercio

Una vez que Internet comenzó a hacerse común para la mayoría de la gente y se logró poner al alcance de las masas, se empezó a pensar en ella, principalmente

⁷ Military Network.

⁸ Transfer Control Protocol, Conjunto de protocolos que se denominan bajo el más importante de ellos.

por parte de las empresas, como en una plataforma en que se podían desarrollar otros servicios distintos a los de solamente comunicar y compartir información de carácter libre, lo que permitiría además optimizar los procesos de estas empresas con un consecuente ahorro en sus costos y tiempos de procesamiento.

Por ende estas organizaciones, descubrieron Internet como un medio de concretar negocios, dando así los primeros pasos a lo que hoy llamamos e-comercio, éste se puede definir como el procesamiento digital de datos en actividades orientadas al comercio de bienes y servicios susceptibles de ser negociados bajo condiciones electrónicas.

Esta actividad virtual vio la luz como respuesta a la necesidad de automatizar los procesos de transacciones por parte principalmente de las entidades financieras a través de sus redes privadas, aprovechando las ventajas que para ello proporcionaban los emergentes enlaces de comunicación, lo que se denominó como EFT⁹. Posteriormente comienza a extenderse el uso de las transacciones electrónicas a otras compañías generalmente grandes empresas, bajo la forma de mensajes electrónicos, así aparece lo que se conoce como la mensajería electrónica o EDI¹⁰ que corresponde a un estándar de transmisión de formularios de datos entre aplicaciones para la normalización del formato de mensajes y su procesamiento automático, ya que las aplicaciones de otra forma no se entenderían, todo esto nuevamente sobre redes privadas de comunicación.

Actualmente con la masificación de Internet y el desarrollo del WWW¹¹ gracias a la creación de herramientas como el HTML¹² y los navegadores Web, sumado al aumento del número de usuarios conectados, debido a la disminución en los costos

⁹ Electronic Fund Transfer.

¹⁰ Electronic Data Interchange.

¹¹ World Wide Web.

de conexión por la competencia entre los ISP¹³ y la baja de precios en computadores personales, permitió el acceso a las empresas más pequeñas a las comunicaciones en línea, comenzando a florecer portales y servicios con la finalidad de captar nuevos clientes, vender productos o prestar servicios al público en general, originando un nuevo tipo de economía “La Economía de la Información” o “Economía Digital”.

Esta nueva economía está cambiando la forma tradicional de conducir negocios, de trabajar, educar y tantas otras actividades. Lo que ha provocado una nueva revolución comparable tal vez al cambio provocado en el siglo XVIII por la revolución industrial. Mantenerse al margen de este proceso hoy es muy difícil para una empresa que desee permanecer en el tiempo, ya que al involucrarse en el e-commerce otras empresas relacionadas con ésta, la forzarán a cambiar sus estrategias de negocios y su logística.

Las ventajas del comercio en línea para las empresas son variadas, como la posibilidad de aumentar la competitividad, al disminuir costos, crear nuevos servicios, personalizar sus relaciones con los clientes y alcanzar un nivel de desempeño alto que por medios tradicionales no se lograrían.

Como ejemplo de las empresas beneficiadas con esta tecnología están los bancos, los que han descubierto estas ventajas y las posibilidades que les ofrece Internet, ya que los costos de las transacciones bancarias realizadas a través de este medio son los más bajos que existen actualmente.

¹² Hiper Text Markup Language, Lenguaje para escribir páginas Web.

¹³ Internet Service Provider, Empresas proveedores de acceso a Internet.

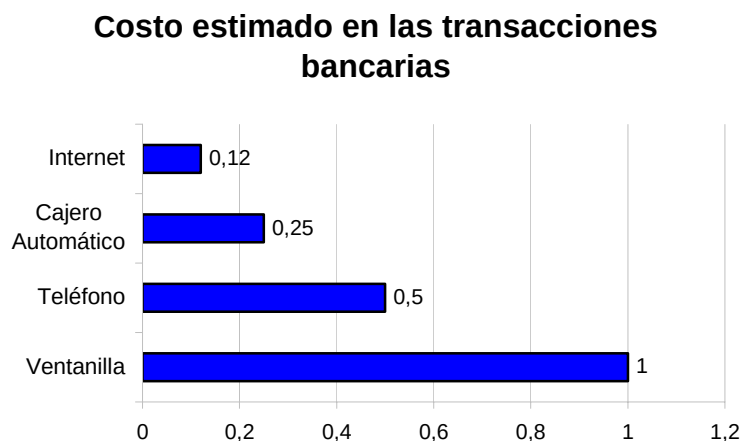


Figura 1: Costo transacciones bancarias en Europa Fuente: Booz Allen & Hamilton.

Además los costos y requerimientos de inversión para preparar e implementar un sitio virtual en el Web que preste servicios bancarios, son mucho menores que los requeridos para las operaciones mediante ventanillas, cajeros u otros medios.

Las posibilidades que ofrecen las operaciones bancarias por Internet son variadas, ejemplos pueden ser consulta de estados de cuenta, transferencias de fondos, inversiones, depósitos, pago de cuentas e impuestos, etc. Existe una larga lista de actividades que pueden realizarse con el simple movimiento de un ratón.

2.4.1 Proyecciones del e-Comercio

La situación actual de desarrollo del comercio electrónico en Chile se presenta basado principalmente en tres etapas:

Primero se centró en la expansión de los accesos a Internet a través de conexiones vinculadas al mundo académico, especialmente universitario. Posteriormente se desarrolló el contenido local por parte de los medios de comunicación tradicionales. Y por último, la llegada de los portales Web.

Este continuo desarrollo permitió durante el año 2000 por ejemplo, que el acceso a Internet en el país alcanzará al 9% de la población -correspondiente al mayor porcentaje en Latinoamérica- dentro de los factores que permitieron esta situación están el descenso de los costos de acceso, la exposición comunicacional del fenómeno de Internet, el aumento en el desarrollo de contenidos locales y la mayor conectividad de las empresas. El número de usuarios en promedio fue de 1.4 millones de usuarios, y alcanzó los 1.8 millones en diciembre de ese año, en 2 años el número de usuarios creció 10 veces y poco más del 10% de éstos eran compradores regulares por Internet, o sea unas 175 mil personas cuyo promedio de compras alcanzaba US \$200 al año¹⁴.

USUARIOS INTERNET Y HÁBITOS DE CONSUMO							
	1999	2000	2001	2002	2003	2004	2005
Nº Usuarios	750.000	1.400.000	1.824.192	2.372.169	3.018.642	3.773.303	4.527.963
% compradores	12%	13%	15%	18%	21%	25%	27%
Nº Compradores	90.000	175.000	273.629	426.991	633.915	943.326	1.222.550
Compras promedio (US \$)	140	204	272	337	382	387	411
Población (millones)	15,007	15,195	15,392	15,592	15,795	16	16,208
% Población con acceso	5%	9%	12%	15%	19%	24%	28%

Tabla 1: Usuarios Internet y hábitos de consumo Fuente: CCS.

En total las compras por Internet alcanzaron US \$35,7 millones en el 2000 con un aumento de un 184% respecto de años anteriores. La participación de los e-Tailers¹⁵ locales registró ventas por el 57% del total, y su participación sigue un contexto creciente considerando que prácticamente un 100% de las ventas en 1998 fueron por importaciones desde sitios norteamericanos. El número de sitios nacionales de e-comercio detallista creció 10 veces entre 1999 y el 2000.

PROYECCIONES COMERCIO B2C							
	1999	2000	2001	2002	2003	2004	2005
TOTAL MILLONES DE DÓLARES	12,6	35,7	74,4	143,7	242	365,3	502,1
E-TAILERS LOCALES	2,6	20,4	45,3	91,4	160,8	249,3	349

Tabla 2: Proyecciones Comercio B2C en Chile Fuente: CCS.

¹⁴ Por debajo todavía de los estándares de países desarrollados.

¹⁵ Comerciante detallista que centra sus actividades en Internet.

Los negocios entre empresas por otro lado, se han constituido en el eje del comercio electrónico en el país, a partir del 2000 se ha producido un acelerado desarrollo de este segmento, que ha dado origen a una mayor penetración del uso comercial de Internet, en el 2001, el 61% de las empresas contaba con alguna forma de acceso a Internet y el 11% había ya desarrollado su propio sitio Web.

Porcentaje de Empresas con Conexión a Internet y Sitio Web (a marzo 2001)		
Tamaño	Internet	Sitio Web
Micro	57,60%	8,50%
Pequeña	77,20%	21,10%
Mediana	92,70%	35,70%
Grande	97,20%	62,70%
TOTAL	61,40%	11,20%

Tabla 3: Porcentaje empresas conectadas a Internet Fuente: CCS.

De acuerdo a la Cámara de Comercio de Santiago, el comercio entre empresas alcanzó los US \$426 millones en el 2000, 5 veces por sobre el valor de las transacciones del año anterior, la migración de los procesos de adquisición a Internet ha sido el principal motor de este crecimiento.

Ahora considerando la evolución en el desarrollo de sistemas transaccionales y la disposición de las empresas al uso comercial de la red en los próximos años, se proyecta un rápido crecimiento en este segmento. Por lo que para el 2005 se esperan transacciones por cifras superiores a los US \$11.800 millones explicadas en un 95% por los negocios entre empresas y se estima que el comercio electrónico canalizará un 2% de las ventas minoristas en el mismo periodo.

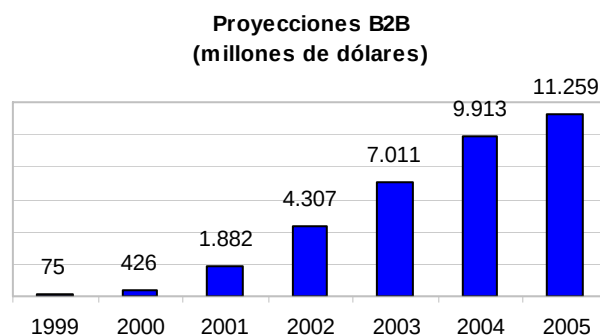


Figura 2: Proyección transacciones B2B Fuente: CCS.

Adicionalmente se consideran actividades empresas-gobierno, distintas a la compra y venta de bienes y servicios, como son el pago de impuestos por medios electrónicos, los que se espera haciendan a US \$2100 millones para el año 2004. Otro aspecto dentro del comercio electrónico es la actividad publicitaria la que el año 2000 aumentó a poco más de US \$2 millones y que a partir de ese entonces crecerá a una tasa promedio del 100% anual, hasta alcanzar US \$36 millones el año 2004.

2.5 Seguridad del Entorno Virtual

El comercio tradicional se basa en relaciones de confianza entre comprador y vendedor, sus garantías se fundan en el conocimiento mutuo de las partes además del soporte legislativo que los estados dan a esta actividad.

Pero el comercio sobre Internet presenta un conjunto de problemas de seguridad a solucionar, dados principalmente por una de sus características más potentes y que la han hecho tan popular, la de ser una plataforma abierta a la que todos pueden tener acceso y donde no existe un ente superior que la dirija. Dentro de estos problemas de seguridad está la exposición de datos confidenciales a la apropiación y al fraude realizados por personas que ven en ello la posibilidad de obtener rápidos beneficios mediante el perjuicio a otros.

Un informe acerca del comercio electrónico en el Reino Unido destaca las características de seguridad de éste, y señala que la seguridad en Internet es el principal aspecto que frena el desarrollo del comercio electrónico, especialmente en el mercado empresa-cliente, la preocupación tiene que ver con la transmisión de los detalles de las tarjetas de crédito por redes públicas como Internet, principal forma de pago a través de este medio y la posibilidad que la información caiga en malas manos.

Por esto todas las empresas además de pensar en los beneficios y ventajas que les ofrece Internet al permitirles llegar a un sector más amplio de la población, deben concentrarse también en el impacto que tienen las interrupciones de sus actividades debido a las violaciones de seguridad. Lo que conlleva a la necesidad de implementar un buen esquema de seguridad que permita el intercambio y almacenamiento de información sin comprometer su confidencialidad e integridad y sin perder la necesaria interacción de los negocios en línea. Esto debería ser una de las principales preocupaciones, si es que las empresas desean explotar las oportunidades de crecimiento y desarrollo que ofrece Internet, ya que un usuario no estará dispuesto a ingresar información confidencial o interactuar con un medio en el que no confíe.

Por lo tanto una empresa que no vea la seguridad como una de sus principales estrategias en el mundo de los negocios electrónicos, estará arriesgándose a perder mucho de su valor al perder la confianza de sus clientes y por lo tanto su reputación.

2.5.1 Amenazas

Dentro de la floreciente sociedad digital han aparecido también actividades ilícitas -ya que Internet reúne características que la convierten en un medio idóneo para cometer actos ilegales básicamente debido a la gran cantidad de datos de fácil acceso y cómoda manipulación que se acumulan en ella-, que son denominadas “delitos informáticos” los que pueden definirse como una acción humana que se realiza en un entorno informático y que pone en peligro un interés jurídicamente protegido, causando perjuicio a personas sin que necesariamente se beneficie el autor, el que es imputable de culpa por haber realizado tal acción y que es sancionado con una pena [15]. Otras definiciones menos técnicas, señalan a los delitos informáticos como actitudes ilícitas en que se tiene a los computadores como instrumento o como fin.

En la actualidad se usan los computadores tanto como una herramienta de apoyo a las actividades humanas, o como un medio eficaz de conseguir un enorme caudal de información en minutos o segundos, lo que hasta hace unos años sólo podía conseguirse luego de largas búsquedas en las que el ser humano jugaba un papel determinante, todos estos indiscutibles beneficios también tienen algunos inconvenientes. La manipulación fraudulenta de los computadores con ánimo de lucro, la destrucción de programas y datos, el acceso y utilización indebida de información son algunos de los delitos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños, los que generalmente suelen ser mayores que en los delitos tradicionales y también suelen ser superiores las posibilidades de que no sean descubiertos.

Por esto, los sistemas de información y sus datos se han transformado en objetos muy preciados, entre éstos los que presentan mayor atractivo para la consumación de este tipo de actos fraudulentos son los sistemas de pago, donde es más fácil convertir transacciones dolosas en dinero por lo que las empresas bancarias y de seguros están más expuestas que otras.

En cuanto a las características estos delitos están el que son más bien acciones ocupacionales y de oportunidad las que generalmente son consumadas en segundos y que además presentan grandes dificultades para su comprobación por su carácter técnico. Una característica ineludible en estas actividades ilegales es el perfil de sus autores, los que en su mayoría cuentan con un alto grado de especialización técnica, siendo éstos delincuentes de cuello y corbata, los que aprovechando sus conocimientos y generalmente sus puestos de trabajo cometen sus fechorías. En cuanto a las motivaciones para realizar estas acciones delictivas se pueden mencionar el ganar ventajas económicas ante competidores mediante el sabotaje, obtener cuantiosas sumas de dinero o aquellas que no tienen nada que ver con la obtención de capital sino de obtener notoriedad o fama.

La mayoría de estos actos caen dentro de ciertas clasificaciones bien definidas como son:

- **Engaños**

Por ejemplo el costo de crear sitios virtuales es pequeño, además la facilidad de copiar una página Web hacen sencillo crear sitios ilegítimos que suplanten a organizaciones establecidas. Con esto se da la posibilidad a estafadores de obtener el número de tarjetas de crédito de forma ilegal al ofrecer escaparates virtuales falsos.

- **Sabotajes**

Tienen relación con aquellas conductas orientadas a causar daños en el hardware o software de un sistema. Los métodos utilizados son muy variados y se pueden diferenciar en aquellos que causan daños físicos y los que causan daños lógicos, o sea aquellos que producen como resultados la destrucción o alteración de los datos contenidos en un sistema informático.

- **Publicación y modificación de información no autorizadas**

Este grupo de conductas afecta la esfera de privacidad mediante la acumulación y divulgación indebida de datos contenidos en sistemas informáticos y se refiere a la obtención, utilización o modificación en perjuicio de un tercero de datos reservados de carácter personal que se hallen en archivos electrónicos.

- **Accesos no autorizados**

Se refiere al uso ilegítimo de contraseñas y la entrada en un sistema informático sin la autorización del propietario, puesto que los bienes que se acostumbra a proteger con contraseñas son lo suficientemente importantes como para que el daño producido por su violación sea considerado como delito.

- **Estafas electrónicas**

La proliferación de las compras virtuales permite que aumenten también los casos de estafas, como ventas de productos que nunca llegan al consumidor o donde los productos recibidos no se cancelan, otro ejemplo son las transferencias electrónicas de fondos no autorizadas.

En todo caso, como se ve estos delitos no son nuevos sino que son los antiguos crímenes consumados ahora mediante medios electrónicos y apoyados por las nuevas tecnologías, los que muchas veces pasan desapercibidos y permanecen impunes ya que pueden ocultarse tras incontables enlaces que en muchas ocasiones sobrepasan las fronteras físicas de los países o se desvanecen tras el clic de un ratón sin dejar ningún rastro, esto como consecuencia de la debilidad de los sistemas de rastreo y la dificultad de recabar pruebas -como llegar a un culpable si basta con presionar un botón para que las pruebas desaparezcan -, además que muchas veces los entes públicos y la justicia no están preparados para enfrentar este tipo de crímenes principalmente por la falta de legislación o por no tener la capacidad o los medios técnicos para investigar dichos actos.

Por esto la proliferación de estos delitos hace a la sociedad cada día más escéptica a la utilización de tecnologías de información lo que trae como consecuencia el obstaculizar el desarrollo y generación de nuevas oportunidades de negocios por falta de apoyo de la sociedad que temerosa desprecia las oportunidades que estas herramientas ofrecen.

2.5.2 Estadísticas de Seguridad

Desde hace algunos años existe una entidad que realiza estudios periódicos sobre seguridad informática y crímenes cometidos mediante la utilización de computadoras, esta entidad es el CSI¹⁶ quien anualmente realiza un “Estudio de Seguridad y Delitos Informáticos” en el que encuesta a profesionales de seguridad de agencias del gobierno y grandes corporaciones estadounidenses.

¹⁶ Computer Security Institute.

Este estudio tiene como objetivo el elevar el nivel de conocimiento en seguridad así como ayudar a determinar el alcance de los delitos informáticos en los Estados Unidos.

La mayoría de sus encuestados trabaja en grandes organizaciones por ejemplo el 24% de éstos cuenta en sus organizaciones con más de 10.000 empleados y un 12% de los mismos tiene entre 500 y 9999 empleados, el 37% de los encuestados del sector comercial reporta por ejemplo ganancias sobre US \$1 billón y un 8% ganancias entre US \$501 millones a US \$1 billón.

Entre lo más destacable del estudio están las estadísticas de infracciones a la seguridad informática, donde se muestra el porcentaje de las empresas que en distintos años han reportado violaciones de seguridad, por ejemplo el 2002 el 60% de los encuestados detecto transgresiones de seguridad de sus sistemas.

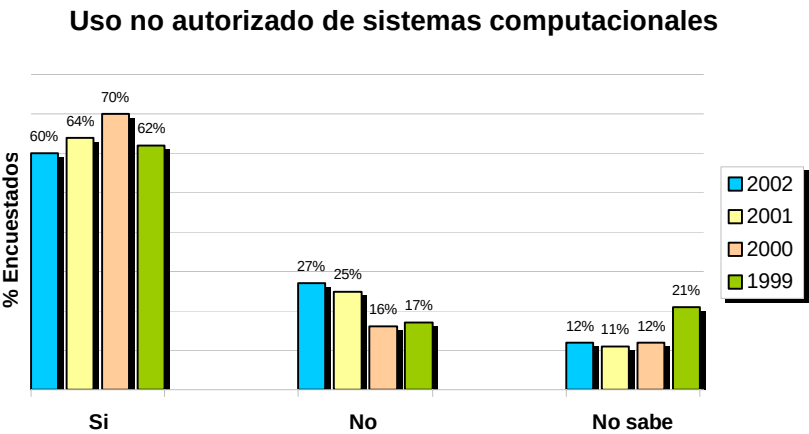


Figura 3: Uso no autorizado de Sistemas últimos 12 meses Fuente: CSI.

Otro punto interesante se refiere a los sistemas o tecnologías de seguridad más utilizados por los encuestados, entre los que destacan los cortafuegos y antivirus.

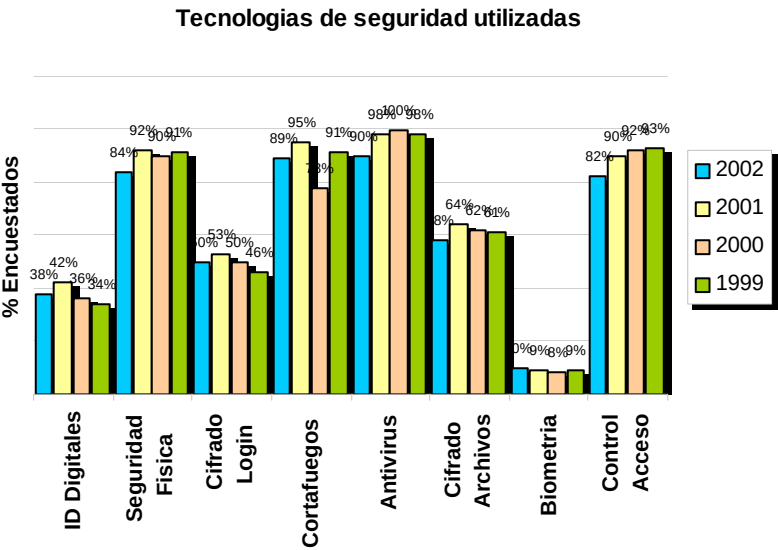


Figura 4: Tecnologías de seguridad utilizadas Fuente: CSI.

Llama la atención eso si que el 89% de los encuestados utilice cortafuegos y que el 60% de éstos halla reconocido penetraciones de sus sistemas como se puede ver en el grafico de violaciones de seguridad, anteriormente señalado.

En cuanto a los puntos desde los cuales se realizan los ataque a los sistemas computacionales se destaca el crecimiento que ha tenido Internet como origen de éstos.

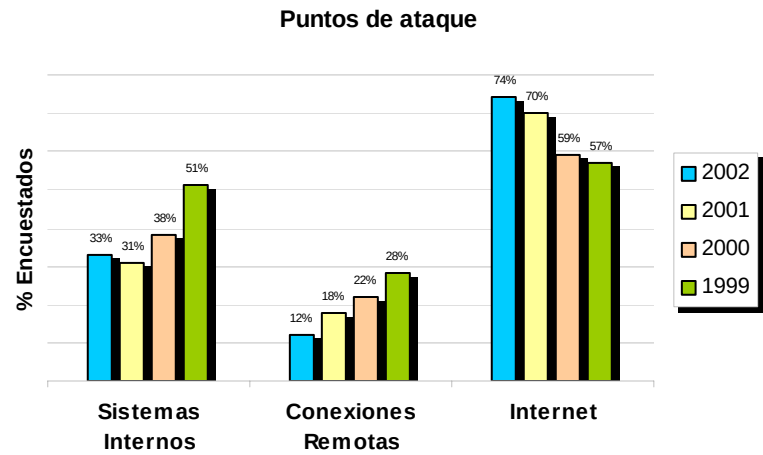


Figura 5: Orígenes más frecuentes de ataques Fuente: CSI.

En este estudio se establece también que en 1997 el 20% de los encuestados reconoció el robo de información, el año 2000 el porcentaje fue el mismo, el 2001 hubo un incremento al 25%, el año más bajo fue 1998 donde un 18% de los encuestados reconoció estos sucesos. En cuanto a las perdidas financieras tenemos que, en 1997 veintiuno de los encuestados cuantificaron sus perdidas y que el monto de perdida más alto fue de US \$10 millones, el promedio fue de US \$954.606 y el total reportado fue de US \$20.048.000.

En el 2002 por su parte, veintiséis de los encuestados reconoció perdidas, de los cuales la mayor alcanzó los US \$50 millones, el promedio fue de US \$6.571.000 y el total de perdidas alcanzó los US \$170.827.000.

Lo extraño de esto es que si el robo de información permaneció casi constante ¿Porqué las perdidas aumentaron de forma tan considerable? Una explicación puede ser la utilización de métodos más selectivos de búsqueda por parte de los atacantes, donde el objetivo principal es la información más valiosa.

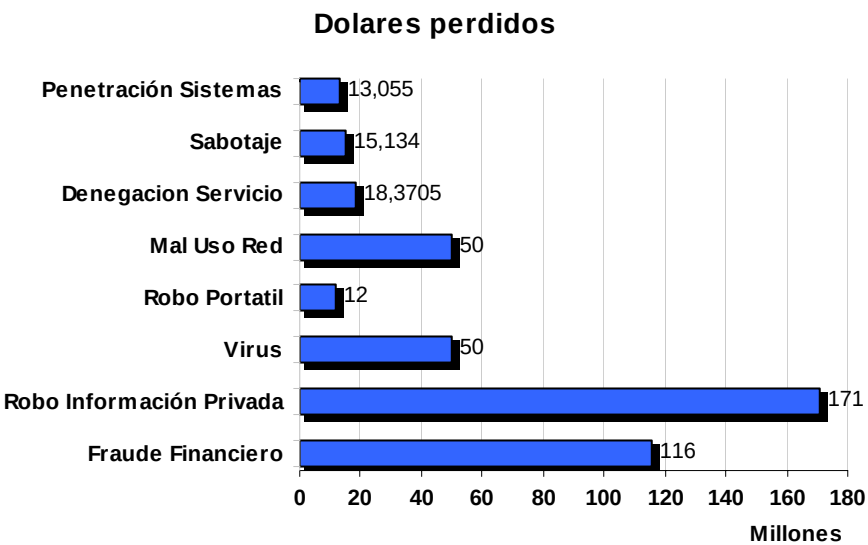


Figura 6: Dólares perdidos en el 2002 por tipo de ataque Fuente: CSI.

Otro punto interesante es el de las pérdidas por fraudes informáticos, donde el año 1997 veintisiete de los encuestados reconocieron pérdidas por este hecho, y el monto más alto alcanzó los US \$2 millones, el promedio fue de US \$957.384 y el total fue de US \$24.892.000.

El año 2002 por su parte, el monto más alto reportado fue US \$50 millones, mientras que el promedio fue US \$4.632.000, alcanzando un total de US \$115.753.000.

Dentro de los ataques más comunes mencionados se encuentran los virus y gusanos informáticos como por ejemplo "I love you", "Red Code", "Nimda", "Melissa" y "SirCam" por mencionar algunos de los más destructivos.

Otra interesante tendencia del estudio son los orígenes más comunes de los ataques dentro de los cuales destacan los llamados domésticos, donde los empleados descontentos con sus organizaciones realizan ataques a los sistemas aprovechando los conocimientos de los mismos.

En cuanto a sí los servicios Web de estas organizaciones habían sufrido ataques, la mayoría de los encuestados que respondió mencionaron que no, aunque el porcentaje a lo largo de los años muestra un decrecimiento constante. Otro hecho importante es el porcentaje no menor que desconoce si un hecho de estas características les había sucedido. Otro hecho destacable es que de todos los que respondieron positivamente, en su mayoría habían recibido 10 o más incidentes, los que en mayor proporción fueron realizados desde fuera de las organizaciones.

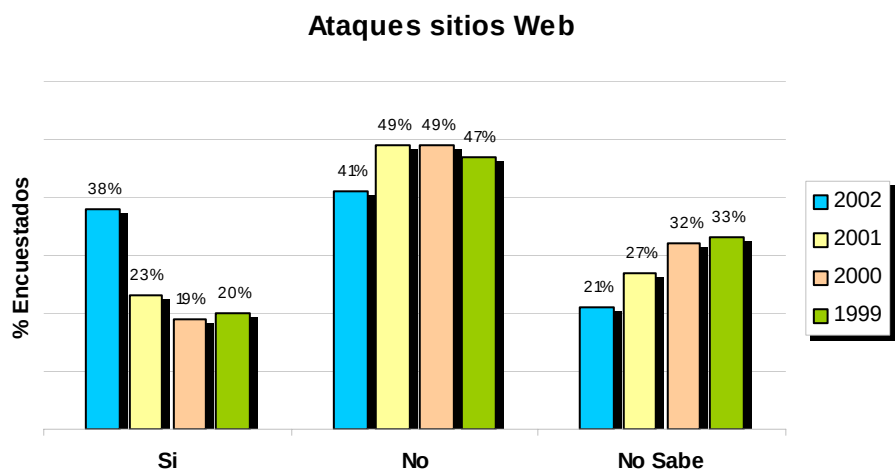


Figura 7: Organizaciones que han detectado ataques a su sitio Web Fuente: CSI.

Con respecto al tipo de ataques sufridos, éstos corresponden mayormente a vandalismo y denegación de servicios.

Por otro lado, en cuanto al tema de reportar o no los incidentes, en los primeros años de la encuesta sólo el 17% de quienes sufrieron serios ataques los reportaron, en 1999 el 32% respondió que habían reportado los incidentes, el 2000 el porcentaje de quienes reportaron intrusiones cayó al 25%, el 2001 el porcentaje se elevó alcanzando al 36% y por último en el 2002 el porcentaje se mantuvo relativamente constante en un 34%. La tendencia es entonces al silencio en cuanto a la ocurrencia de estos hechos. Las razones principales para esto son la negativa publicidad que representa para las organizaciones la ocurrencia de estos eventos y la posibilidad que la competencia tome ventaja de los mismos.

Como se puede ver el Cibercrimen ha aumentado y se ha diversificado, las cantidades de dinero perdidos debido a estos actos también han crecido de manera considerable. Lamentablemente las tendencias mostradas no son las más auspiciosas, lo que está creando conciencia en las organizaciones respecto a la

importancia de tomar mayores medidas de seguridad para protegerse en este nuevo mundo virtual.

2.6 Herramientas y Protocolos de Seguridad

Después de haber visto las amenazas que enfrenta el e-comercio para su desarrollo, se hace necesario analizar también las herramientas desarrolladas para dar solución a estos problemas o por lo menos disminuir sus efectos negativos.

El enfoque clásico de seguridad para un sistema de información, exigía un ordenamiento y custodia estricta de la información según su sensibilidad e importancia, este enfoque ya no es posible en la práctica en el mundo digital puesto que el aprovechamiento de la información consiste en la distribución de ésta, lo que lleva a plantear la necesidad de sustituir estos enfoques tradicionales por soluciones innovadoras basadas por supuesto en las nuevas tecnologías. Estas soluciones por ejemplo implican el uso de criptografía y de instrumentos nuevos de autenticación y control de acceso, entre otros. Además para poder garantizar que las infraestructuras de información sean seguras y confiables no sólo se debe exigir el uso de estas herramientas sino también su correcto despliegue.

Algunas de estas herramientas ya existen y están lo suficientemente maduras para su utilización, la dificultad radica en que los usuarios las desconocen en su mayoría o no están concientes de las ventajas de su uso debido básicamente a que no se quiere enfrentar con la debida anticipación los desastres y también a no tener una percepción clara de las implicancias que tiene el dilema de la seguridad informática.

Sin duda la primera herramienta de seguridad a considerar debiera ser el documento ISO¹⁷ 7498 que describe el modelo de referencia OSI¹⁸, y que además presenta una arquitectura de seguridad según el cual para proteger las comunicaciones de los usuarios es necesario dotar a los sistemas de los servicios de autenticación, control de acceso, confidencialidad, integridad y no repudio. Actualmente existen varios sistemas que implementan varios de estos servicios.

2.6.1 Métodos de Control de Acceso

Estos consisten en identificar a los usuarios de los sistemas, hasta hace algún tiempo los métodos tradicionales en el área de autenticación o control de acceso a los recursos se abocaban a imposibilitar el acceso a la información confidencial, manteniendo un perímetro de seguridad entorno a los datos para mantener fuera a los intrusos, este tipo de herramientas de carácter defensivo se ha ido cambiando debido a las actuales necesidades por otras que permitan el acceso a la información de las organizaciones pero de manera controlada para permitir una mayor interactividad necesaria para el comercio en línea.

Existen diversas formas de permitir o denegar el acceso a lugares o sistemas de información, entre los cuales se mencionarán los más utilizados.

- **Contraseñas**

Dentro de los métodos utilizados para identificar usuarios y controlar el acceso a sistemas informáticos el más simple y de más bajo costo es el de la contraseña¹⁹ asociada a un nombre de usuario. Los inconvenientes con este tipo de autenticación son que el usuario podría tener que manejar muchas claves dependiendo de los

¹⁷ International Standard Organization.

¹⁸ Open System Interconnection.

¹⁹ También llamado de secreto compartido

sistemas en los que esté involucrado, y si estas claves son muy complicadas le será difícil recordarlas por lo que deberá usar algún medio para almacenarlas con el consecuente peligro de su extravío.

Los ataques a este tipo de seguridad se fundan principalmente en adivinar la contraseña sobre la base de la prueba y error o método de fuerza bruta, probando combinaciones posibles de letras, números, caracteres especiales, etc. Este ataque es bastante eficiente debido a las características de las contraseñas utilizadas por la mayoría de las personas.

- **Biometría**

Otro método de identificación de usuarios es a través de la biometría o sea basado en las características físicas únicas de los individuos que son imposibles de repetir y que no cambian con el tiempo o las circunstancias. Dentro de éstas está la huella digital, el iris del ojo, la mano, la voz, etc. Sus ventajas radican en que son intransferibles, el usuario transporta su clave siempre lo que hace imposible perderla u olvidarla y no necesitan gestión por parte del usuario como cambiarlas cada cierto tiempo. El inconveniente para la utilización masiva de este método en sistemas informáticos es que necesita de electrónica adicional lo que implica un alto costo.

- **Tarjetas Inteligentes**

Es un método bastante usado en el acceso a lugares físicos no así en el mundo digital debido también a los costos, las tarjetas pueden ser magnéticas o con chips, las primeras sólo tienen memoria y se necesita un lector magnético, las otras poseen un procesador interno que les permite tener un grado de inteligencia por lo que éstas últimas necesitan lectores especiales, algunas de estas tarjetas también

están asociadas a un PIN²⁰ que debe ser ingresado para acceder a las funciones de la tarjeta.

2.6.2 Kerberos

Es un protocolo o sistema de autenticación por Ticket²¹ y fue diseñado en el MIT²² para verificar la identidad de los usuarios de una red digital, así como para distribuir las claves secretas de sesión que permitan a los usuarios de la red establecer comunicaciones seguras.

Este sistema de autenticación está basado en la criptografía y en un protocolo de distribución de claves a cada usuario y servidor. Kerberos tiene también una base de datos que contendrá las claves de ambos. Este protocolo trata de mejorar los esquemas de seguridad intentando por un lado que el cliente necesite identificarse para ser autorizado a comunicarse con un servidor -y que esta autorización venga de una maquina confiable- y por otro lado eliminar la divulgación de la información privada del usuario como es su contraseña.

El protocolo provee dos servicios fundamentales, el de autenticación AS²³ y el de Tickets TGS²⁴, el primero tiene como función autenticar inicialmente a los clientes y proporcionarles un Ticket para comunicarse con el servidor de Tickets, que proporciona a los clientes las credenciales necesarias para comunicarse con un servidor final que es quien realmente ofrece el servicio. Además el servidor posee una base de datos de sus clientes -usuarios y programas- con sus respectivas claves conocidas únicamente por dicho servidor y por el cliente al que pertenecen.

²⁰ Número Identificador Personal.

²¹ Información cifrada por un servidor confiable que permite acceder a la estación que lo recibe y a los servicios de aplicación en entornos cliente servidor distribuidos.

²² Massachusetts Institute of technology.

²³ Authentication Service.

²⁴ Ticket Granting Service.

El protocolo es un proceso en el que diferentes elementos colaboran para conseguir identificar a un cliente que solicita un servicio ante un servidor, éste se realiza en tres etapas que funciona de la siguiente manera:

- I Login. Inicialmente el cliente o usuario necesita obtener las credenciales necesarias para acceder a otros servicios. Para ello cuando un usuario se conecta a un sistema escribe su nombre de usuario, de la misma forma que en un sistema habitual, la diferencia está en que se envía el nombre de usuario al servidor de autenticación Kerberos para solicitar un Ticket que le permita comunicarse posteriormente con el servidor de Tickets. Si el usuario es conocido, el servidor de autenticación retorna un mensaje que contiene una clave para la comunicación con el servidor de Tickets y un Timestamp²⁵ cifrado con la clave del cliente, junto con un ticket para la comunicación con el servidor de Tickets, cifrado con la clave secreta del servidor de Tickets.
- II Ahora en la maquina del cliente, se intentará descifrar este mensaje con la clave que se le solicitará al usuario, si ésta es correcta entonces el usuario podrá obtener la clave de sesión entre el cliente y el servidor de Tickets ya que un cliente podrá descifrar este mensaje sólo si conoce su clave, una vez obtenida esta clave de sesión el cliente la guarda para una comunicación posterior con el servidor de Tickets y borra la clave de usuario de la memoria, de esta forma el modelo consigue que la clave de usuario nunca viaje por la red.
- III Obtención de Tickets. El cliente ya posee una clave de sesión para comunicarse con el servidor de Tickets y el Ticket necesario para hacerlo cifrado con la clave del servidor de Tickets. Cuando el cliente necesita acceder

²⁵ Estampilla de tiempo.

a un determinado servicio es necesario que disponga de un Ticket. Por lo que lo solicita al TGS enviándole un autenticador que el propio cliente genera, el Ticket del servidor de Tickets y el nombre del servicio al que desea acceder junto con un indicador de tiempo. Cuando el TGS recibe el ticket comprueba su validez y si todo es correcto retorna un mensaje que contiene una clave para la comunicación con el servidor al que se desea conectar y un Timestamp cifrado con la clave de sesión del par cliente-servidor de ticket, junto a un Ticket para que el cliente y el servidor se puedan comunicar cifrado con la clave secreta del servidor al que se quería conectarse originalmente. De esta manera el cliente sólo podrá obtener la clave de sesión entre cliente y servidor, si conoce la clave de sesión entre cliente y servidor de ticket.

- IV Petición de servicio. Tras obtener el ticket para comunicarse con el servidor, el cliente ya está preparado para solicitar el servicio deseado, para ello presenta la credencial autenticada ante el servidor final, que es el que presta el servicio. Ahora el cliente se comporta de la misma forma que cuando solicito un ticket al servidor de ticket, envía el ticket y una petición que puede ir cifrada si el servidor lo requiere.

Aunque se trata de un sistema robusto, éste no carece de problemas de seguridad e implementación, lo que ha impedido la expansión de su utilización. Entre estos problemas se puede mencionar que cualquier programa que lo utilice debe ser modificado para funcionar correctamente, o sea en el fondo se debe disponer del código fuente de la aplicación que se pretende “Kerberizar”. La gran centralización que presenta el sistema se transforma en otro inconveniente ya que para el correcto funcionamiento se debe disponer en todo momento del servidor que alberga al sistema Kerberos, si esta maquina falla la red se inutiliza, ya que toda la información

de seguridad reside en la base de datos que contiene las claves y si se compromete ésta la red entera está amenazada. Otra dificultad es el uso de Timestamp lo que obliga a que las maquinas que ejecutan servicios autenticados mantengan sus relojes sincronizados.

2.6.3 SET

El protocolo SET²⁶ fue desarrollado por Visa y MasterCard con la asesoría de empresas como RSA, Microsoft, IBM entre otras, con la finalidad de salvaguardar las transferencias y pagos con tarjeta de crédito a través de Internet u otras redes abiertas.

Este protocolo está basado en la criptografía de clave pública y firma digital. Y lo que hace es emular el proceso de pago con tarjeta de crédito del comercio tradicional en el mundo del comercio electrónico, la novedad en este protocolo es que hace intervenir al banco dentro del esquema a diferencia de otros sistemas que aseguran la comunicación sólo entre dos entidades, un cliente y un servidor.

El protocolo SET permite:

Confidencialidad, ya que la información de pago se cifra para que no pueda ser espiada mientras viaja por las redes de comunicaciones.

Autenticación, ya que todas las partes involucradas en la transacción pueden verificar mutuamente sus identidades mediante certificados digitales, de esta forma el comerciante puede asegurarse de la identidad del titular de la tarjeta y el cliente de la

²⁶ Secure Electronic Transactions.

identidad del comerciante, por su parte los bancos pueden así mismo comprobar la identidad del titular y del comerciante²⁷.

Integridad, garantizando que la información intercambiada como el número de tarjeta no podrá ser alterada durante su transporte a través de la red. Para esto hace uso de firmas digitales en las ordenes de pago y los pedidos.

Intimidad, debido a que el banco emisor de la tarjeta de crédito no puede acceder a la información sobre los pedidos del titular, por lo que queda incapacitado de crear perfiles de compra de sus clientes, además la transacción se cierra entre el banco y el comprador por lo que el comerciante no ve ni puede conservar los datos de la tarjeta.

Verificación inmediata, antes de completarse la compra se realiza una verificación inmediata de la disponibilidad de crédito y de la identidad del cliente.

No repudio, ya que los certificados digitales asocian la identidad del titular de la tarjeta y del comerciante con las entidades financieras y los sistemas de pago de Visa Y MasterCard.

En este esquema participan varias entidades entre las cuales están:

El Emisor de la tarjeta de crédito del cliente, quien extiende su crédito y es responsable de la facturación y servicio al consumidor, este puede ser el banco del cliente o la entidad que avala la tarjeta, Visa o MasterCard.

El Banco del comerciante, que forma la relación con éste, procesando las transacciones con tarjeta y las autorizaciones de pago.

²⁷ Esto permite además que no sea necesario el número de tarjeta ya que el cliente puede ser identificado mediante el certificado digital.

El Cliente o titular de la tarjeta emitida por el banco o por una de las empresas Visa o MasterCard.

El Comerciante, que vende productos o servicios y que acepta el pago por medios electrónicos.

La Pasarela de Pagos, mecanismo mediante el cual se procesan y autorizan las transacciones del comerciante, permite la comunicación directa a través de Internet entre el comerciante y las redes bancarias, esta pasarela puede pertenecer a una entidad financiera o a un operador de medios de pago.

La Autoridad de Certificación, quien certifica las claves del titular de la tarjeta, del comerciante y de los bancos mediante los certificados digitales. Estas pueden ser entidades independientes autorizadas como bancos o la empresa que avala las tarjetas de crédito.

El protocolo admite una serie de diferentes opciones, pero básicamente consta de los siguientes pasos:

- I El comerciante pide a su banco un certificado digital para comerciante y lo instala en su sitio Web.
- II El comerciante contrata un servicio de Pasarela de Pagos que conecte su sitio Web con la red bancaria y entidad de certificación.
- III El cliente que quiere comprar en Internet solicita un certificado digital para consumidor y lo instala en su computador personal.
- IV El cliente entra al sitio Web del comerciante con la decisión de comprar algún artículo, comunicándose en forma cifrada de acuerdo con un protocolo de encriptación.

- V El cliente genera dos textos, uno es el texto del pedido y el otro un texto con la orden de pago. Envía al comerciante los dos mensajes firmados digitalmente²⁸, los datos del pedido (básicamente identificación del comerciante, productos y fecha) y la orden o instrucciones de pago del cliente (número de tarjeta de crédito, banco emisor, cantidad, etc.) que no puede leer el comerciante, además de la relación que une el pedido con la orden de pago. Esto reduce los riesgos de abusos y fraudes ya que el comerciante no puede ver información como el número de la tarjeta de crédito empleado por el comprador y el banco no se entera de los hábitos de compra de su cliente.
- VI El comerciante luego verifica la firma del pedido y envía la orden de pago (que no ha podido leer) con su firma digital al banco a través de la pasarela de pagos. Se crea entonces una petición de autorización de pago que se envía a la pasarela de pagos, incluyendo el importe a ser autorizado, el identificador de la transacción y otra información relevante, todo esto correctamente cifrado y firmado.
- VII La pasarela de pagos comprueba la autenticidad del comprador, la integridad del mensaje y la relación existente entre el pedido y la orden de pago.
- VIII Si todo está correcto la pasarela envía al banco del comerciante la orden de pago y solicita la autorización para realizarlo.
- IX El banco del comerciante comprueba entonces la orden de pago y autoriza el cargo del importe de la compra.

²⁸ Firma especial denominada firma dual, ya que para su confección se utilizan ambos documentos.

- X Una vez informado el comerciante de la autorización procede al envío de los artículos al cliente, después de la entrega física del producto pide el importe de la venta a la pasarela de pagos.
- XI Entonces la pasarela de pagos pide al banco del comprador la transferencia del importe de la venta al banco del comerciante, completándose de esta manera la transacción. Todo este proceso se realiza cifrando los mensajes que son enviados a las distintas entidades involucradas en el sistema.

El protocolo SET especifica el formato de los mensajes, las codificaciones y las operaciones criptográficas que deben usarse. No requiere un método particular de transporte de manera que los mensajes SET pueden ser transportados sobre HTTP en aplicaciones Web, correo electrónico o cualquier otro método.

Algunos inconvenientes de este protocolo y causa principales del porque no ha experimentado una mayor utilización es debido a que algunos ISP no soportan SET, además la obtención del certificado por parte del comerciante involucra un costo y la duración de una transacción SET es mayor que en otros sistemas.

2.6.4 SSL

El SSL²⁹ es un protocolo muy utilizado y de carácter abierto que desarrolló la empresa Netscape para proporcionar seguridad durante la transmisión de datos, este protocolo fue aceptado como un estándar Web para la autenticación y encriptación de las comunicaciones en un sistema cliente-servidor asegurando un canal de comunicaciones entre éstos.

Este esquema es típicamente utilizado entre navegadores y servidores Web sobre todo en los sistemas de pago por Internet que utilizan tarjetas de crédito. Esta

capa de seguridad, basada en la encriptación de las comunicaciones, se ubica sobre el protocolo TCP/IP en el modelo OSI y puede correr bajo protocolos de aplicación como HTTP, FTP, LDAP y TELNET, lo que lo hace más flexible que otras soluciones de seguridad. Esta herramienta sólo sirve para comunicaciones bidireccionales y está basado en la aplicación conjunta de criptografía asimétrica³⁰ y simétrica lo que lo convierte en protocolo híbrido en cuanto a encriptación, además utiliza certificados y firmas digitales.

SSL proporciona algunas de las funciones necesarias que una solución de seguridad debe tener para el comercio electrónico actual, como son:

Confidencialidad, mediante conexiones cifradas, ya que aunque la información caiga en manos incorrectas, ésta será indescifrable.

Autenticación del servidor, ya que el usuario puede asegurarse de la identidad del servidor al que se conecta, opcionalmente puede autenticar al cliente para que el servidor conozca la identidad del usuario con el fin de decidir si le permite el acceso a áreas protegidas.

Integridad de los mensajes, ya que detecta modificaciones en la información después que ésta viaja por la red.

El protocolo SSL está basado en dos subprotocolos o capas, el Record Protocol y Handshake Protocol, el primero se encarga de la compresión, encriptación, integridad y serialización de los mensajes; el segundo gestiona la conexión inicial, los algoritmos a utilizar, autenticación de las partes y la clave de sesión.

²⁹ Secure Socket Layer.

³⁰ Utiliza dos claves relacionadas, una para cifrar y la otra para descifrar.

En su primera versión, SSL no soportaba autenticación, sólo soportaba encriptación e integridad de mensajes. La versión dos por su parte soportaba autenticación sólo del servidor, mientras que SSL 3.0 soporta tanto autenticación del cliente como del servidor además de los otros servicios.

En sus primeras versiones también utilizaba claves de tan solo 40 bits de longitud, la que actualmente llega a 128 bits debido a que los computadores modernos ya tiene la capacidad suficiente para descifrar claves de longitud menor a ésta, sin embargo contrario a lo que se podría pensar, no se puede aumentar el largo de la clave todo lo que se quiera ya que esto haría mucho más lento el funcionamiento de los servicios que implementen el protocolo.

SSL funciona de la siguiente manera:

- I El cliente se conecta a través de su navegador a un servidor que soporte SSL y envía una solicitud para iniciar una comunicación o sesión segura.
- II El servidor envía una respuesta si soporta o no SSL.
- III El cliente y el servidor comienzan a negociar la conexión SSL e intercambian información de seguridad, a esto se le llama “Handshake”, donde se hace la autenticación del servidor y opcionalmente del cliente, se determinan que algoritmos de criptografía serán utilizados³¹, el identificador de sesión, los algoritmos de compresión y se genera una clave secreta por parte del navegador del cliente, para ser utilizada durante el intercambio de mensajes en la comunicación SSL.

³¹ El algoritmo utilizado será el más fuerte que soporte tanto el servidor como el cliente.

- IV Después de verificar la identidad del servidor y de la generación de la clave aleatoria -distinta para cada sesión-, ésta se cifra con la llave pública del servidor y es enviada a éste en caso que el Handshake tenga éxito.
- V El servidor y el cliente pueden ahora intercambiar información de forma segura utilizando la clave secreta acordada en la sesión, adicionalmente cada vez que el servidor o el cliente deseen enviar un mensaje al otro se genera un resumen del mensaje utilizando un algoritmo denominado Hash, el que también se cifra y se envía para la verificación de la integridad del mensaje.

Un sitio Web seguro mediante SSL se reconoce por una imagen de un candado³² que aparece en esquina inferior izquierda de la página Web. La mayoría de los navegadores Web son compatibles con el protocolo SSL y una característica a destacar es la capacidad de encriptación de la comunicación la que puede ser de 56 o 128 bits dependiendo del navegador del cliente y del certificado digital instalado en el servidor Web.

El protocolo SSL versión 3.0 no está exento de algunas deficiencias por lo que se busco un nuevo protocolo que permitiera transacciones seguras por Internet, sobre todo teniendo en cuenta que SSL es propiedad de Netscape. El resultado fue el protocolo TLS³³ que permite una compatibilidad total con SSL siendo un protocolo público estandarizado.

TLS busca integrar en un esquema tipo SSL al sistema operativo a nivel de la capa TCP/IP del modelo OSI, para que el efecto "Túnel" que se implemento con SSL sea realmente transparente a las aplicaciones que se están ejecutando.

³² Caso del Navegador Web Internet Explorer.

³³ Transport Layer Security.

2.6.5 S-HTTP

El protocolo S-HTTP³⁴ fue desarrollado por Enterprise Integration Technology y al igual que SSL permite tanto el cifrado de documentos como la autenticación mediante firma y certificados digitales, pero se diferencia de SSL en que se implementa al nivel de la capa de aplicación del modelo OSI, protegiendo los datos y no un canal de comunicaciones.

Se puede identificar rápidamente una página Web servida con este protocolo porque la extensión de la misma pasa a ser “.shtml” en vez de “.html” como en las páginas normales. El mecanismo de conexión mediante S-HTTP comprende una serie de pasos parecidos a los usados en SSL, en los que el cliente y servidor se intercambian una serie de datos formateados que incluyen los algoritmos criptográficos, longitudes de claves y algoritmos de compresión a usar durante la comunicación segura.

Bajo este protocolo, un cliente solicita un documento, le dice al servidor que tipo de cifrado puede manejar y le dice también donde puede encontrar su clave pública, si el usuario de esta clave está autorizado a acceder al documento, el servidor responde cifrando el documento y enviándoselo al cliente, que usará su clave privada para descifrarlo y mostrárselo al usuario.

A diferencia de SSL el protocolo S-HTTP es escasamente utilizado y además está integrado con HTTP ya que está diseñado específicamente para soportar este protocolo, por lo que asegura solamente este tipo de transacciones, negociando los servicios de seguridad a través de cabeceras y atributos de página.

³⁴ Secure Hiper Text Transfer Protocol.

2.6.6 S/MIME

El correo electrónico es uno de los servicios más antiguos de Internet y es uno de los sistemas de comunicación más vulnerables a los ataques de seguridad, actualmente se ha vuelto una herramienta imprescindible a nivel profesional, siendo uno de los elementos de mayor crecimiento en Internet.

Sin embargo su asignatura pendiente ha sido por largo tiempo la seguridad, ya que por sus características no es suficiente sólo cifrar las conexiones por las cuales se transmite el correo, si no que es necesario firmar y cifrar el mensaje en sí. De esta manera el mensaje podrá transitar por líneas inseguras y estar a salvo también de los administradores de los sistemas donde se guarden los mensajes.

Para cumplir con esto, se creó el protocolo S/MIME³⁵ que es una extensión del protocolo MIME creado para que los correos electrónicos tuvieran la capacidad de enviar archivos de todo tipo anexados al texto del mensaje.

El protocolo S/MIME fue una propuesta de la empresa RSA³⁶ y está basado en los estándares de criptografía pública creados por esta empresa, proporciona seguridad en el intercambio de mensajes mediante correo electrónico y uno de sus objetivos era ser fácilmente integrable en las aplicaciones de correo ya existentes.

Este estándar permite la confidencialidad, autenticación, integridad y no repudio, ya que trabaja con certificados y firmas digitales, por lo que necesita de autoridades de certificación para la emisión de certificados. También permite la utilización de listas de revocación de certificados que se utilizan para anular la validez de los mismos y tiene la capacidad de envolver tanto al mensaje como su firma en un sobre de datos cifrado.

2.6.7 PGP

El PGP³⁷ es un paquete de seguridad para el correo electrónico que fue desarrollado por Philip Zimmerman, es un programa de firma electrónica de código abierto, mientras Zimmerman controlaba su producción el gobierno de los EE.UU. le prohibió su exportación basándose en intereses militares, una vez que Zimmerman vendió su producto se dejó de liberar el código fuente eliminándose las barreras para su exportación.

El paquete presta servicios de encriptación, autenticación, compresión de datos y firma digital, utiliza para esto algoritmos como el RSA, IDEA, MD5 y para la compresión de texto el algoritmo ZIP.

Para enviar un mensaje encriptado por ejemplo, ambas partes deben tener el software PGP y deben intercambiar sus claves públicas, el proceso funciona de esta forma:

- I El usuario A desea enviar un mensaje a otro B, el usuario A entonces mediante PGP aplica un algoritmo al mensaje obteniéndose un resumen de éste, el que se encripta con la clave privada de A.
- II Luego se concatena el mensaje con el resumen y el resultado es comprimido mediante otro algoritmo.
- III Ahora el usuario A, escoge una frase que será utilizada por PGP para generar una clave aleatoria, ésta se utiliza para cifrar el mensaje comprimido.

³⁵ Secure Multipurpose Internet Mail Extension.

³⁶ Administradores de los derechos del conocido algoritmo de cifrado asimétrico RSA.

³⁷ Pretty Good Privacy.

- IV La clave es a su vez cifrada con la clave pública del usuario B y se concatena la clave cifrada con el mensaje que está comprimido y encriptado.
- V Ahora cuando el usuario B recibe el mensaje descripta la clave utilizando su clave privada.
- VI Luego con la clave recién obtenida descripta el mensaje y lo descomprime para posteriormente separar el mensaje del resumen encriptado.
- VII Seguido de esto se descripta este resumen con la clave pública del usuario A.
- VIII Ahora se le aplica nuevamente el algoritmo de resumen al mensaje original, para compararlo con el resumen que venía concatenado a éste, si éstos son similares se comprueba que el mensaje no fue alterado y que quien lo envió fue efectivamente el usuario A.

```

-----BEGIN PGP SIGNED MESSAGE-----

-----
Un problema en el tratamiento de cookies en el componente ASP.NET puede
dejar vulnerables a un ataque de desbordamiento de búfer a determinadas
aplicaciones desarrolladas bajo el entorno .NET de Microsoft.
-----
-----BEGIN PGP SIGNATURE-----
Version: PGP 6.5.2

iQCVAwUBPQDysetaAupcB1VZAQEw/wP8D1oTH/dbprB/+SslZjuH09N3013g8/2m
2R/LRXwQY1TM8NbKZGbBQovJ/esbuVsGXhQPqBizS8HHkAoZINXKKpCjpk02vHfw
WTdEJtyMLA1X1pkGOvb2pTCU46TP0nOdyv62j9IFeKFNUMhSzChddyDXKz2NWTH
jdoWFO6KAkA=
=P0Xc
-----END PGP SIGNATURE-----

```

Figura 8: Mensaje firmado mediante PGP.

La Figura muestra un mensaje que ha sido firmado mediante PGP, en el nuevo texto va indicado el comienzo del texto original, posteriormente se especifica

el comienzo y fin de la firma, que encierra en su interior el resumen del documento cifrado con la clave privada del emisor.

El problema con el PGP es que cualquier usuario puede crear un par de claves privada y pública o varios pares si lo requiere, pero al momento de enviar su clave pública a otros usuarios éstos no tiene la certeza de si quien les envía la clave, es realmente quien dice ser, ya que falta una tercera parte de confianza que certifique que esa clave pública pertenece realmente al usuario que así lo declara, dándose la alta probabilidad de suplantación de identidad.

2.6.8 WTLS

El protocolo WTLS³⁸ está orientado a proporcionar seguridad en medios inalámbricos como son las comunicaciones a través de teléfonos celulares, éstos utilizan el protocolo WAP³⁹ para desplegar información tipo Web en sus dispositivos, ya que está optimizado para ser utilizado en canales de comunicación de banda estrecha.

El WTLS define como la seguridad de Internet se extiende al mundo de las comunicaciones inalámbricas y tiene un impacto para la Internet móvil similar al que tiene el SSL para la Internet por cables, abriendo nuevas posibilidades al comercio electrónico inalámbrico. El protocolo se ha diseñado siguiendo una serie de criterios similares a los de SSL y TLS para de esta forma crear una plataforma segura inalámbrica.

³⁸ Wireless Transport Layer Security.

³⁹ Wireless Application Protocol.

Dentro de los servicios que proporciona el protocolo están:

La confidencialidad, al encriptar la información enviada entre el celular y el servidor.

La integridad de los datos, ya que asegura que los datos intercambiados entre celular y servidor no han sido modificados y no están corruptos.

La autenticidad del celular y del servidor de aplicaciones ya que cuenta con varios servicios para esto.

El funcionamiento de la comunicación entre el mundo de las señales de radio y el de los cables, se debe a que la Internet inalámbrica utiliza una maquina intermedia, llamada Gateway WAP que transforma las señales de radio en señales eléctricas las que se dirigen posteriormente a través de Internet.

Para la comunicación de forma segura con la Internet tradicional, más específicamente con los servidores Web, el Gateway utiliza los protocolos de seguridad tradicionales como es el SSL, asegurando integridad, privacidad y autenticidad con este servidor.

En el otro extremo de la comunicación el Gateway toma los datos cifrados con SSL y los traduce para su envío a través de las redes celulares que utilizan el protocolo de seguridad WTLS. En esencia el Gateway WAP realiza la función de un puente entre los dos protocolos de seguridad.

La necesidad de este cambio entre SSL y WTLS es impuesta por la naturaleza de las comunicaciones inalámbricas, ancho de banda reducido con alta latencia⁴⁰. Por esto, dado que SSL se diseño para computadores de sobremesa con capacidad

⁴⁰ Tiempo necesario para un paquete de información viaje desde la fuente hasta su destino.

de proceso superior a la de un teléfono móvil si se intentara incluir SSL en estos teléfonos, aumentarían sus precios para poder adaptarlos, frenando así el crecimiento de la tecnología WAP.

2.6.9 IPSec

Es un conjunto de estándares para la ampliación del protocolo de Internet, como una forma de ofrecer servicios de seguridad estándar sobre redes TCP/IP, proporciona servicios de seguridad a la capa IP del modelo OSI y todos los protocolos superiores basados en IP, TCP, UDP y otros, combinando algoritmos de cifrado, algoritmos de resumen y certificados digitales.

Entre las ventajas de IPSec destacan que está apoyado en estándares del IETF⁴¹ y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada.

IPSec se puede integrar a la versión actual del protocolo IP y lo que es más importante viene por defecto en la siguiente versión de este el IPv6, otra característica destacable es su carácter de estándar abierto y aunque establece ciertos algoritmos comunes por razones de interoperabilidad permite integrar algoritmos criptográficos más robustos que puedan ser diseñados en el futuro.

Dentro de IPSec se distinguen los siguientes componentes:

Dos protocolos de seguridad, IP AH⁴² e IP ESP⁴³ los que proporcionan los mecanismos de seguridad para proteger el tráfico IP. El protocolo AH es un procedimiento para garantizar integridad y autenticación de los datagramas⁴⁴ IP,

⁴¹ Internet Engineering Task Force.

⁴² Authentication Header.

⁴³ Encapsulating Security Payload.

⁴⁴ Agrupamiento lógico de información enviada como una unidad a través de una red.

mientras el objetivo principal de ESP es proporcionar confidencialidad para lo cual especifica el modo de cifrar los datos que se desean enviar y como se incluirán estos datos en el datagrama.

Un protocolo de gestión de claves llamado IKE⁴⁵ permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP, este protocolo no se limita a IPSec ya que es un protocolo estándar de gestión de claves que puede ser útil a otros protocolos.

El protocolo cuenta con dos modos de funcionamiento, el primero es el modo Transporte en que el contenido del datagrama son los datos de la capa de transporte o sea datos TCP o UDP lo que requiere que ambos nodos de la comunicación entiendan IPSec y el segundo modo es el de Túnel en que el contenido es un datagrama IP completo, este modo se usa cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

Dentro de las principales ventajas de este estándar se encuentran la transparencia para los demás dispositivos presentes en la red y para las aplicaciones, ya que éstas no necesitan modificaciones debido a que no se enteran de la existencia de criptografía intermedia como es en el caso de SSL debido a que el protocolo trabaja al nivel de IP. Entre los servicios de seguridad ofrecidos están la integridad, autenticación del origen de los datos, confidencialidad, detección de repeticiones de paquetes, control de acceso y no repudio.

Como se ha podido ver en este capítulo Internet ha crecido de manera increíble y ha logrado alcanzar la mayoría de las actividades humanas, también se ha podido vislumbrar sus potencialidades sobre todo para el comercio y las proyecciones de crecimiento que éste posee en el mundo digital. Sin embargo

también han quedado claras las variadas amenazas que éste debe enfrentar y las herramientas actuales que intentan dar solución a estos peligros. A continuación se describirán las bases sobre las cuales se implementan estas herramientas de protección, lo que nos acercará un poco más a solución que esta tesis plantea como mejora a la seguridad de aplicaciones Internet.

⁴⁵ Internet Key Exchange.

3.1 Preámbulo

Este capítulo tiene como fin mostrar la base de la mayoría de los servicios y protocolos de seguridad utilizados en el entorno electrónico. Estos se fundan sobre técnicas y procedimientos de los que se mostrará una pequeña visión, la que contempla la definición de criptología prosiguiendo con una descripción de sus orígenes hasta los avances logrados en la actualidad, revelando las principales características, clasificaciones, funcionamiento y utilidades de los algoritmos de cifrado. Lo que servirá para ir adentrándose en el mundo de las Infraestructuras de Claves Públicas y la firma digital que es lo que interesa aclarar en este trabajo de tesis.

3.2 Introducción

Como ya se ha visto en los capítulos anteriores, uno de los retos más importantes para el futuro del mundo digital es el poder transmitir mensajes de forma segura. Será por lo tanto la protección de dicha información una de las claves del futuro de las comunicaciones, lo que permitirá el desarrollo de nuevas aplicaciones y servicios en entornos públicos como Internet.

No es desconocido el crecimiento de las redes y sus interconexiones, donde cada día más usuarios se unen e interactúan, circulando por la llamada “Autopista de la Información” y convirtiéndose en flamantes habitantes de un nuevo mundo virtual

repleto de información. Pero así como se comparten datos y accesos a los sistemas, también se comparten muchos riesgos asociados a la seguridad.

Como se vio en el capítulo anterior, ya desde sus inicios y por su concepción Internet ha sido un medio inseguro para la transmisión de información de carácter confidencial debido a que en su diseño original sólo se pensaba en la eficiencia del transporte y no tenía mayor prioridad la seguridad.

Por esto, en este medio es difícil poder confiar, ya que nos relacionamos con personas invisibles, donde además los mensajes pueden permanecer en el ciberespacio por tiempo indefinido sin que se tenga conciencia de ello, ni de donde pueden ser almacenados. Al mismo tiempo existen muchos programas desarrollados para monitorear y analizar el tráfico que se conduce a través de las redes, por lo que el peligro de que éstos sean utilizados de forma irresponsable es muy alto.

Los objetivos entonces son, como ya se ha mencionado en los capítulos anteriores, mantener la confidencialidad de los datos almacenados, procesados y transmitidos; mantener la integridad de éstos, para darles inmunidad en contra de los posibles intentos de manipulación; asegurar la identidad del origen y destino de la información y garantizar el no repudio de las actividades virtuales. Esto no es fácil ya que no contamos en la red con los medios que utilizamos habitualmente en el mundo real como son las cajas fuertes o guardias de seguridad. Pero no todo está perdido, todavía hay esperanzas de conseguir los objetivos propuestos y poder emular las herramientas de seguridad del mundo físico.

Pues bien, la criptografía es una excelente forma para lograrlo, ya que permite mantener la información lejos de los ojos de los curiosos y delincuentes, debido a que es la única manera de mantener las cosas en secreto y por tanto de conservarlas seguras.

3.3 Historia

La criptografía es una ciencia considerada como antigua ya que el intento de ocultar información disfrazándola con un código secreto para obstaculizar su conocimiento se remonta al nacimiento de la civilización y es tan antigua como la invención de la escritura.

En los albores de la civilización los egipcios ya apelaban a ella, ya que los sacerdotes empleaban la lengua hierática⁴⁶ para ocultar información, incomprensible para el pueblo que hablaba la lengua demótica.

Ahora bien, se considera el nacimiento puntual de la criptografía durante la guerra entre Atenas y Esparta en el siglo V AC, donde los mensajes eran alterados o cifrados mediante la inclusión de símbolos innecesarios, los que desaparecían al enrollar el papel del mensaje en un rodillo de longitud y grosor apropiados llamado "Escítala" con lo cual el mensaje podía leerse con claridad. Los Romanos por su parte en el siglo I AC empleaban el Cifrado Cesar, el que consistía en cambiar cada letra por la que ocupaba tres lugares más adelante en el alfabeto.

Más adelante en el siglo XV León Batista Alberti se destaca en el criptoanálisis y crea la primera maquina de criptografía dotada con dos discos concéntricos que giran independientes consiguiendo con cada giro un alfabeto de transposición, este es considerando por muchos el padre de la criptografía. En el siglo XVI Girolamo Cardano empleo una tarjeta perforada que había que colocar sobre le texto para poder leer un mensaje cifrado. En ese siglo también Blaise de Vigenére publicó el "Traité des Chiffres" donde recopila los diversos métodos de cifrado empleados en su época y crea el método Vigenére, método clásico de cifrado por sustitución, el que

⁴⁶ Conocida también como jeroglífica.

utilizaba una clave secreta para tales propósitos. Durante sus campañas militares y en sus documentos diplomáticos Napoleón también utilizó la criptografía y apeló a los métodos Richelieu y Rossignol donde la regularidad de las letras era evitada mediante la asignación de números a grupos de una o más letras.

Pero el máximo desarrollo de la criptografía se consumó en el periodo de guerra del siglo XX, ya que existía entonces una gran necesidad de comunicaciones militares y diplomáticas seguras. Así los alemanes construyeron la maquina Enigma para ocultar sus mensajes, ésta se componía de tres cilindros por los que rodaba cada letra, cuando un elemento cifrado pasaba por el primer cilindro, éste giraba una posición, cuando el primer cilindro giraba veintiséis veces⁴⁷ el segundo cilindro lo hacia una, cuando el segundo cilindro giraba otras veintiséis veces rotaba entonces el tercero. Mediante estos movimientos, la codificación cambiaba con cada letra que entraba a la maquina. Aun poseyendo la maquina no era posible descifrar el mensaje si se desconocía la posición inicial de los cilindros. Los alemanes además disponían de una posición inicial para cada día, que servía para codificar y decodificar los mensajes de esa jornada. Con esto los altos mandos aliados necesitaban desesperadamente descifrar el código secreto de Enigma y para este fin se constituyo un equipo de criptógrafos dirigido por Alan Turing, los que idearon Colossus, una maquina descifradora que para algunos es el esbozo del primer ordenador de la historia y el nacimiento de la informática, junto con considerar a sus creadores como los primeros Hackers del mundo.

Otro ejemplo dentro del mismo contexto bélico es el de los norteamericanos, que en plena segunda guerra mundial interceptaron un mensaje cifrado enviado desde Tokio a la embajada nipona en los Estados Unidos, éstos denominaron al

⁴⁷ El número de letras del abecedario.

sistema de cifrado “código púrpura”, el sistema fue roto por William Friedman y un grupo de criptoanalistas mediante la utilización de la maquina Magic creada para tal fin. Esta maquina jugó un papel fundamental en la derrota de los japoneses a manos de los norteamericanos.

Posteriormente y con el desarrollo de la informática se ha dado un gran salto en el estudio de los sistemas criptográficos. En 1975 Diffie y Hellman establecieron las bases teóricas de los algoritmos de clave pública, ya que hasta entonces no se concebía un sistema de cifrado que no fuese de clave secreta, a partir de esta época entran al juego del cifrado y descifrado los computadores, los que toman ahora el protagonismo.

3.4 Criptología

Esta palabra proviene del griego Kryptos y Logos que significan estudio de lo oculto. Y se entiende por Criptología a la ciencia que trata o estudia los problemas relacionados con la seguridad y los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes, un emisor y un receptor.

Esta ciencia está dividida en dos grandes ramas, la primera es la Criptografía⁴⁸, parte de la criptología que estudia como ocultar efectivamente los mensajes mediante claves y también del diseño de criptosistemas. La segunda es el Criptoanálisis, oponente de la primera, que trata de descifrar u esclarecer los mensajes rompiendo así el criptosistema. Por esto, cada progreso en una de estas ramas obliga al esfuerzo y sustitución de las técnicas empleadas por la otra, ya que

⁴⁸ Del griego Kryptos y Grafía que significa escritura oculta.

cuando el criptoanalista⁴⁹ rompe o descifra un código, el criptógrafo debe sustituirlo por otro más seguro.

Pero la criptología moderna no es algo mágico ni espontáneo, ésta descansa sobre tres importantes campos teóricos.

- **La teoría de la información**

Está basada en las condiciones técnicas de la transmisión de mensajes y el análisis sociológico de la comunicación, realizadas por Claude Shannon⁵⁰ y Warren Weaver respectivamente, además de artículos posteriores en los que se presenta una fundamentación matemática de la teoría de la comunicación y su aplicación a criptosistemas de clave secreta, los que abordan temas como la cantidad de información de un mensaje, la optimización de códigos, compresión de la información y codificadores perfectos.

- **La teoría de los números**

Tiene una estrecha relación con la criptografía ya que en ésta se basan sus algoritmos. En una definición bastante reducida corresponde a la rama de las matemáticas que se ocupa de las propiedades y relaciones de los números. Entre los tipos de números que estudia están los números primos⁵¹ y las características de su divisibilidad⁵², los números enteros y la aritmética modular cuya propiedad de tener operaciones inversas permiten el cifrado y descifrado en algunos criptosistemas.

⁴⁹ No confundir los procedimientos del criptoanálisis con descifrar un mensaje, este último es habitual y se realiza con la clave de cifrado del mensaje.

⁵⁰ Publicó "A Mathematical Theory of Communication".

⁵¹ Números solo divisibles por uno y por ellos mismos.

⁵² Muy importancia en la criptografía asimétrica.

- **La teoría de la complejidad algorítmica**

Tiene como objetivo estudiar los requisitos que deben cumplir las técnicas criptográficas para ser seguras y se refiere a uno de los más modernos vínculos entre la computación y las matemáticas abarcando los problemas referidos a la capacidad de los algoritmos computacionales de realizar una tarea determinada en un tiempo de computo razonable⁵³.

Además de apoyarse en estos tres campos teóricos la seguridad de los sistemas criptográficos yace sobre dos conceptos más, la “Difusión” y la “Confusión”, ya que la redundancia del lenguaje entrega muchas pistas que permiten utilizar técnicas estadísticas para romper algunos tipos de cifrados.

El propósito de la Difusión de la información es distribuir o repartir en el texto cifrado las propiedades estadísticas que se encuentran dentro de los mensajes en claro, esto se puede conseguir a través de permutaciones, que consisten en separar lo más posible los caracteres que se encuentran juntos en el mensaje original, desestructurándolo completamente.

El propósito de la Confusión por otra parte, es ocultar la relación entre el texto claro y el cifrado, este objetivo se puede conseguir por ejemplo mediante sustituciones que consisten en reemplazar los caracteres del texto original por otros caracteres o símbolos distintos en el texto cifrado.

Ambas técnicas, la difusión y la confusión, proporcionan fortaleza a los criptosistemas de manera independiente, sin embargo utilizadas conjuntamente pueden dar lugar a sistemas muy difíciles de romper. El ejemplo más característico

⁵³ Existen dos clasificaciones, los algoritmos con tiempo de ejecución o complejidad polinomial y los con tiempo exponencial.

de estas técnicas es el sistema de encriptación DES, éste realiza permutaciones que proporcionan Difusión y sustituciones que proveen la Confusión.

3.5 Importancia Estratégica y Legal

Aunque la criptografía no parece revestir mayor importancia para algunas personas, es pieza clave en algunos debates de países más desarrollados y se ha convertido para algunos gobiernos en un foco de atención muy importante, ya que con este tipo de herramientas se produce un choque de intereses entre el derecho a la privacidad de las personas y el deseo de los cuerpos de seguridad referente a que no exista información a la que no se pueda tener acceso.

Por ejemplo en EE.UU. por un lado están los defensores de la privacidad y por otro el FBI que gracias a las escuchas ordenadas judicialmente y presentadas como pruebas han permitido solucionar innumerables casos policiales y obtener millones de dólares en multas, lo que se hubiera imposibilitado si se utilizara masivamente la encriptación de la información por parte de los delincuentes.

Debido a esto, algunos países tienen directamente prohibido dentro de sus legislaciones el uso de la encriptación de mensajes y en otros está fuertemente controlado como en EE.UU. donde se impide la exportación de programas cifradores al considerarse una herramienta tan estratégica como cualquier arma de tecnología avanzada⁵⁴. Otros países en cambio permiten el uso de este tipo de herramientas pero desean que se les incluya una puerta trasera para poder intervenirlos y así poder descifrar los mensajes cuando se considera justificadamente necesario.

⁵⁴ Como quedo demostrado en la segunda guerra mundial con el uso de las maquinas Enigma y Colossus.

3.6 Criptosistemas

Todo sistema criptográfico consta de ciertos componentes básicos y características definidas para ser considerado como tal.

Entre sus componentes tenemos:

- **El espacio de mensajes**

Es el conjunto de los posibles textos en claro. Los elementos de este conjunto se denominan mensajes, teniendo en cuenta que nos referimos a mensajes legibles. Estos se forman a partir de un alfabeto, mediante reglas sintácticas y semánticas del idioma en que se originan.

- **El espacio de textos cifrados**

Es el conjunto de todos los posibles mensajes cifrados, el alfabeto de los textos cifrados puede ser el mismo o distinto del utilizado para los mensajes en claro y el tamaño de éstos puede ser mayor que sus respectivos textos en claro.

- **El espacio de claves**

Corresponde al conjunto de posibles claves utilizadas en los procesos de cifrado y descifrado, son una pieza fundamental en la criptografía.

- **Una familia de transformaciones de cifrado**

Es el procedimiento que convierte el texto claro en un texto cifrado.

- **Una familia de transformaciones de descifrado**

Corresponde al procedimiento que permiten reconstruir el texto en claro a partir del cifrado.

Adicionalmente la información dentro de un criptosistema fluye de tal manera que relaciona a todos estos componentes desde un ente transmisor a uno receptor. El punto débil del criptosistema está ubicado en el medio de transmisión, el que por naturaleza es inseguro y donde un intruso podría intentar acceder a la información que se transmite.

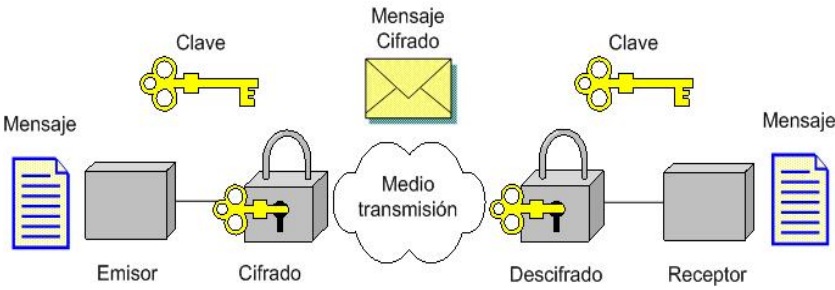


Figura 9: Esquema Criptosistema.

Con respecto a los requisitos que deben satisfacer los criptosistemas para poder ser utilizados están:

- Debe ser imposible recuperar a partir del texto cifrado, el texto original y/o la clave⁵⁵. Se debe considerar cumplida esta tarea si la complejidad del proceso para obtener el texto original es lo suficientemente costoso en tiempo y recursos.
- Todo sistema criptográfico debe estar compuesto por dos tipos distintos de información, las claves de carácter privado y los algoritmos de tipo público⁵⁶.
- Las transformaciones de cifrado y descifrado deben ser computacionalmente eficaces y eficientes, para todas las claves. El algoritmo de cifra como su inverso debe ser rápido y confiable, su aplicación no debe suponer un retraso excesivo ni ninguna distorsión en el funcionamiento del sistema de información.

⁵⁵ Principio de Kerckhoffs descrito en su libro “La Criptografía Militar”.

⁵⁶ Este principio de Kerckhoffs ha quedado obsoleto en manos de los sistemas criptográficos de clave pública.

- La seguridad del criptosistema debe depender exclusivamente del secreto de las claves y no del secreto de las funciones de cifrado y descifrado.

Unido a esto se puede comentar un requisito adicional, que las funciones de cifrado y descifrado pueden y deben conocerse públicamente, de hecho este conocimiento es beneficioso pues pone a prueba la fuerza de los sistemas de cifrado por parte de la comunidad especializada, lo que permite descubrir debilidades o darle validez para su aplicación práctica.

Con respecto a la seguridad de un criptosistema, ésta depende de su fuerza que se define como el grado de dificultad que supone romperlo⁵⁷. Romper un criptosistema significa que un criptoanalista puede reconstruir el texto en claro a partir del texto cifrado.

Esta reconstrucción en todo caso no es imposible, ya que no existe un sistema invulnerable, porque con los recursos y el tiempo suficiente prácticamente todo sistema puede ser roto, por lo que generalmente no se busca un sistema totalmente inviolable sino que sea imposible de romper computacionalmente hablando como por ejemplo que dada la tecnología actual de microprocesadores, el tiempo que tome romper el sistema sea superior a 50 años.

3.7 Clasificación de Métodos Criptográficos

Inicialmente se puede hacer una clasificación de los criptosistemas de acuerdo a un orden cronológico, que está claramente dividido por la aparición de los computadores. Una vez más éstos aparecen como el engranaje principal de cambios, esta vez para permitir el avance y progreso de la criptografía. Los métodos

⁵⁷ Se refiere a poder descifrar los mensajes sin conocer la clave.

criptográficos se dividen entonces en la criptografía clásica antes de la aparición de los computadores y la criptografía moderna posterior a ésta.

3.7.1 Criptografía Clásica

Los métodos clásicos de criptografía son aquellos desarrollados hasta la primera mitad del siglo XX. Son técnicas desarrolladas para cifrar mensajes escritos a mano o en maquinas de impresión y se puede considerar como tales a todos aquellos criptosistemas anteriores al uso sistemático de los computadores en la criptografía. Dentro de sus características fundamentales está la simplicidad y facilidad de recordar sus algoritmos y claves, ya que fueron creados pensando en su aplicación al campo militar donde los mensajes debían poder cifrarse y descifrarse de modo sencillo junto con poder recordar los métodos fácilmente, esto sin duda también los hacía muy vulnerables.

Estos procedimientos clásicos se basan principalmente en la sustitución y en la transposición para alterar del orden lógico de los caracteres del mensaje, mezclando bajo cierta ley las palabras o frases del texto en claro.

3.7.1.1 Sustitución

El método de sustitución consiste básicamente en reemplazar los caracteres del mensaje inicial por otros, los nuevos caracteres pueden ser de cualquier tipo: letras, símbolos, dígitos, etc. Los caracteres iniciales siguen estando en el orden preestablecido pero salvo que se conozca la equivalencia entre los nuevos caracteres y los antiguos, el mensaje es ilegible.

Se pueden considerar dos tipos de sustitución:

- **Equivalencia entre alfabetos carácter a carácter**

A cada letra del alfabeto ordinario se le hace corresponder un símbolo de otro alfabeto. El mensaje se cifra cambiando las letras por su equivalente, si a la letra “A” le asignamos el símbolo “@”, en el mensaje cifrado tendremos siempre una @ en lugar de la A.

- **Equivalencia entre alfabetos utilizando una clave**

Difiere del anterior en que una vez establecida la correspondencia entre los alfabetos, la asignación de caracteres se realiza teniendo en cuenta la posición del carácter en el mensaje, por ejemplo si el mensaje es “secreto” y la clave es “23”, el mensaje cifrado se consigue adelantando dos letras la primera y tres la segunda, dos letras la tercera y tres la cuarta y así sucesivamente, el mensaje cifrado⁵⁸ quedaría “uheugwq”, como se ve la letra “e” aparece como “h” y la segunda vez como “g” con lo que ya no hay una correspondencia uno a uno, esto se conoce como el método de Vigenére.

Dentro de los métodos clásicos por sustitución, nos podemos encontrar con:

- **El Cifrado de César o Mono alfabético Simple**

Es extremadamente sencillo y fue empleado por los romanos para encriptar sus mensajes durante las campañas militares, de ahí el nombre de cesar, ya que fue en su reinado donde nació. Este consiste en reemplazar cada letra de un texto por

⁵⁸ Nótese que los caracteres del alfabeto del texto claro y cifrado no necesariamente deben ser los mismos.

otra que se encuentra a una distancia determinada. Se sabe que César empleaba una distancia de tres.

Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto César	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Mensaje	E	I	H	a	c	k	e	r	A	c	e	c	h	a
Cifrado	H	ñ	K	d	f	n	h	u	D	f	h	f	k	d

Tabla 4: Ejemplo cifrado sustitución de Cesar.

▪ Sistema de Sustitución Poli alfabética

Es un método que emplea más de un alfabeto de sustitución. Esto es, se emplean varios alfabetos diferentes, para después elegir un alfabeto distinto para la sustitución de cada carácter según una secuencia establecida.

Este sistema es algo más complejo que los anteriores y resulta difícil descifrar mensajes cuando se emplean más de diez alfabetos.

Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto 1	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
Alfabeto 2	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
Alfabeto 3	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Mensaje	E	I	H	a	c	k	e	r	A	c	E	c	h	a
Clave	S	O	L	S	O	L	S	O	L	S	O	L	S	O
Cifrado	W	z	R	s	q	u	W	g	L	u	s	n	z	o

Tabla 5: Ejemplo cifrado sustitución polialfabética.

Para descifrar un mensaje entonces se debe en principio conocer la correspondencia entre los alfabetos y la clave. Aunque cuando el mensaje es lo suficientemente largo se puede utilizar la técnica de análisis de frecuencia para descifrarlo.

3.7.1.2 Transposición

Los métodos de transposición consisten en una reordenación de los símbolos del mensaje original de modo que éste resulte ilegible. Si un mensaje consta de N letras se podrá transponer de N! formas⁵⁹. La reordenación se puede realizar desde un modo simple, escribiendo el mensaje letra a letra pero al revés o utilizando complicados esquemas matriciales.

Dentro de los métodos clásicos de transposición podemos encontrar:

- **Transposición por columnas**

En este sistema se dispone el texto por filas de una determinada longitud, rellenándose el final de la ultima fila con un carácter cualquiera. El texto cifrado se obtiene leyendo la matriz resultante por columnas. La clave es simplemente el número de columnas utilizado.

“El Hacker Acecha”

E	l	H
A	c	k
e	r	A
c	e	c
h	a	x

Tabla 6: Cifrado de transposición por columnas.

⁵⁹ N factorial, N!=1×2×...×N.

Entonces el mensaje cifrado seria: "EaechlcreaHkAcx"

- **Sistema de Cifrado Inverso**

Este es quizás una de las formas más simples de cifrar. Consiste en invertir el orden de la frase, posicionando la primera letra en el último lugar de la frase y así sucesivamente.

"El Hacker Acecha"

El mensaje cifrado quedaría "ahcecA rekcaH IE"

Como se ha podido ver los métodos criptográficos clásicos emplean la misma clave para cifrar y descifrar un mensaje y si bien estos métodos se pueden combinar para formar técnicas seguras han demostrado ser ineficaces ante la potencia de calculo de los computadores modernos, para los cuales es trivial la resolución de estos criptosistemas.

Por esto han surgido nuevos métodos, más seguros, algunos basados también en claves secretas cuya computación es mucho más compleja.

3.7.2 Criptografía Moderna

Los métodos modernos se desarrollan con la aparición de los computadores y basan su funcionamiento en la utilización de potentes y complejas herramientas tanto de hardware como de software. Utilizan también claves secretas de gran longitud para controlar una compleja secuencia de operaciones, que pueden incluir tanto transposiciones como sustituciones de los datos.

Estos sistemas al estar basados en complejas transformaciones matemáticas deben disponer de una gran memoria y alta capacidad de procesamiento para poder

cifrar la información. La principal diferencia de los sistemas criptográficos modernos respecto de los clásicos está en que su seguridad no se basa en el secreto del sistema, sino en la robustez de sus algoritmos, siendo el único secreto la clave empleada para el cifrado.

Estos sistemas se pueden dividir además en aquellos de clave pública y de clave privada. Ambos sistemas tienen características bien diferenciadas, lo que permite su uso para diferentes fines, de hecho ambos tipos de sistemas suelen combinarse para llevar a cabo distintas acciones y lograr la mayoría de los objetivos de seguridad⁶⁰.

3.7.2.1 Números Aleatorios

Otra de las características que vale la pena destacar de estos sistemas criptográficos es la utilización de los números aleatorios, pilares sobre los que se sostienen, ya que la utilización de éstos es vital para su seguridad. Estos entregan secuencias numéricas, donde el siguiente elemento no se puede predecir sobre la base de los anteriores, ya que todos tienen igual probabilidad de ser escogidos, lo que en estadística se define como independientes⁶¹. Aunque en los computadores esto no es tan real ya que si un generador de números aleatorios se ejecuta bajo las mismas condiciones varias veces, las secuencias de números serán similares, por esto se les llaman números pseudo aleatorios ya que son generados por una función que aparenta tales características.

⁶⁰ Confidencialidad, Integridad, Autenticidad y No repudio.

⁶¹ Ejemplo clásico es el lanzamiento de una moneda ideal al aire.

3.7.2.2 Cifradores de Bloque y de Flujo

Dependiendo de la manera en que aplicamos el cifrado y particularmente como se trata la información antes de ser cifrada, los criptosistemas modernos pueden clasificarse también en cifradores de bloque y cifradores de flujo.

Los cifradores de bloques antes de proceder al cifrado agrupan parte de la información en bloques de tamaño fijo, normalmente varios bits. En cuanto a los cifradores de flujo, consideran el mensaje a cifrar como un flujo de bits y cifran cada elemento individualmente en forma secuencial.

3.7.2.3 Sistemas de Cifrado Simétrico

Estos sistemas son también llamados de clave única, ya que utilizan la misma clave tanto para cifrar como para descifrar un mensaje, por lo que la clave debe ser compartida por el emisor y el receptor de éste. En el esquema simétrico para poder mantener la efectividad, la clave debe ser mantenida en secreto por ambos entes, ya que el nivel de seguridad depende exclusivamente del nivel de protección de la clave⁶².

Estos sistemas han tenido muy buena aceptación ya que permiten hacer computaciones elevadas y se caracterizan por ser altamente eficientes con relación al tamaño de su clave, además de ser rápidos y robustos.

En este tipo de sistemas la confidencialidad y la autenticidad⁶³ se obtienen al mismo tiempo, ya que cuando se descifra un mensaje usando la clave privada, el hecho de que ésta sea tan sólo conocida por el emisor y el receptor garantiza entre comillas las dos propiedades:

⁶² Por ello también se llaman de clave privada.

⁶³ Condicionado a que la clave no sea conocida por más personas.

- Que el mensaje no es legible para nadie más, o sea confidencialidad.
- Y dado que el texto descifrado es legible, sólo hay un emisor posible, aquel que conoce la clave privada, o sea autenticidad del mensaje⁶⁴.

El problema fundamental de este tipo de criptosistemas es la generación, almacenamiento y sobre todo el intercambio de las claves, debido a que éstas se distribuyen en entornos no seguros⁶⁵. Por tanto las claves deben intercambiarse de un modo eficiente, pues es en ello donde descansan todas las características de seguridad de estos sistemas.

Problema adicional es el que cada pareja de usuarios necesitará compartir una clave distinta, por lo que el número de éstas aumentaría cuadráticamente con el número de personas involucradas, por ejemplo si existen N usuarios, cada usuario necesita $N-1$ claves distintas para comunicarse con el resto. Así pues el total de claves involucradas si todos los usuarios están conectados es de $N*(N-1)/2$ o sea del orden N^2 .

En los últimos años se han diseñado una gran cantidad de sistemas criptográficos simétricos, siendo el más conocido DES a pesar de no tener las mejores propiedades.

3.7.2.3.1 DES

El algoritmo DES⁶⁶ fue diseñado por IBM y es utilizado extensamente dado que se ha convertido en un estándar al estar reconocido por las agencias norteamericanas. El origen de DES se remonta a la década de los setenta debido a

⁶⁴ Esta autenticidad es relativa ya que no existe un único posible emisor, sino al menos dos.

⁶⁵ Si existiera un entorno seguro la criptografía y este trabajo no serían necesarios.

⁶⁶ Data Encryption Standard.

una petición realizada por el NBS⁶⁷ a distintos fabricantes de criptosistemas para encontrar un estándar de protección de datos.

Los requisitos que debía cumplir el estándar de cifrado eran:

- Contar con un nivel de seguridad computacional alto.
- Estar especificado en todos sus detalles de forma entendible.
- Su seguridad no debe verse comprometida si se hace público el algoritmo.
- Su implementación en dispositivos electrónicos debía ser de bajo costo.
- Debía poder implementarse en hardware.

Por esos tiempos IBM disponía de un sistema denominado LUCIFER basado en una clave de 128 bits. Este fue sometido a pruebas por el NBS y tras ser analizado por expertos de la NSA⁶⁸ y reducir su clave a 56 bits, fue aceptado y nombrado DES.

Con respecto a su funcionamiento, éste se basa en la combinación de permutaciones y sustituciones realizadas sobre bloques de información de 64 bits, utilizando una clave secreta de 56 bits⁶⁹, sobre cada bloque se repite el mismo proceso 16 veces.

Inicialmente a cada bloque se le aplica una permutación mediante una tabla denominada IP, para producir difusión en los bits. Al finalizar el algoritmo se aplicará nuevamente una tabla pero esta vez será la inversa de la ya mencionada.

⁶⁷ National Bureau of Standards en la actualidad denominado National Institute of Standards.

⁶⁸ National Security Agency.

⁶⁹ En realidad son 64 bits porque cuenta con 8 bits más para la corrección de errores pero que no añaden fortaleza.

Posterior a la permutación inicial, se divide cada bloque en dos de 32 bits L_0 y R_0 , las operaciones de cifrado se realizan sólo en la parte derecha de cada una de las etapas, en las que se combina mediante una función XOR⁷⁰ cada bloque L_i producido en la etapa anterior con el resultado de aplicar una función al bloque R_i , K_{i+1} dando lugar al bloque⁷¹ R_{i+1} .

$$R_{i+1} = L_i \oplus f(R_i, K_{i+1})$$

$$L_{i+1} = R_i$$

En una ultima etapa, no se produce el intercambio de las partes y al bloque concatenado $L_{16} R_{16}$ se le aplica la permutación inversa con la tabla IP ya mencionada, lo que deshace la permutación inicial para dar lugar a la salida cifrada.

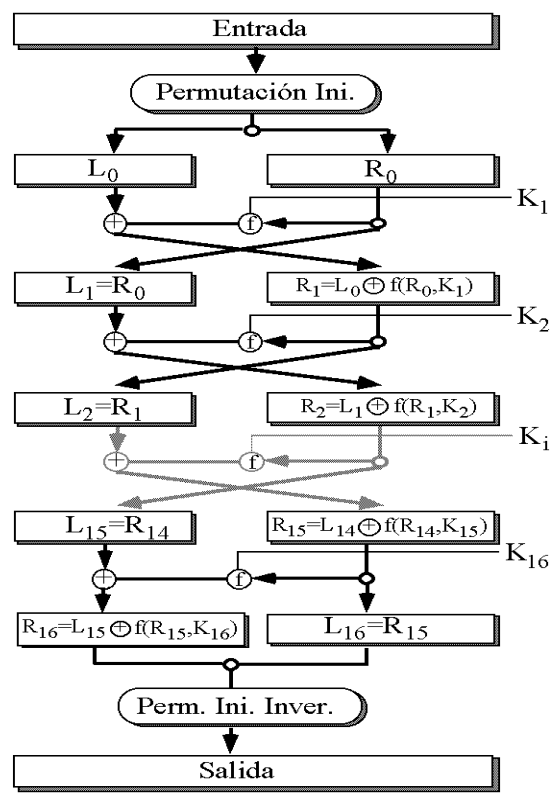


Figura 10: Diagrama funcionamiento DES.

⁷⁰ Función en el álgebra de Boole que corresponde al OR exclusivo.

⁷¹ Las subclaves K_i de cada iteración cuyo tamaño corresponde a 48 bits, se generan a partir de la clave de 56 bits.

La función f se basa entre otros mecanismos en una serie de tablas P-boxes⁷² y S-boxes⁷³ cuidadosamente elegidas para garantizar la seguridad y para que puedan utilizarse tanto para el cifrado como el descifrado. De esta manera el algoritmo DES es reversible, es decir, puede aplicarse el mismo proceso tanto para el cifrado como para el descifrado utilizando la misma clave.

En la actualidad no se ha podido romper el sistema DES desde la perspectiva de poder deducir la clave simétrica a partir de la información interceptada. Sin embargo en 1998 con el método de fuerza bruta y un solo computador la EFF⁷⁴ rompió en menos de tres días una clave DES. Para ello probó más de 88000 millones de claves por segundo durante 56 horas hasta hallar la clave que cifraba el mensaje.

Lo anterior quiere decir que es posible obtener la clave del sistema DES en un tiempo relativamente corto por lo que actualmente una clave de 56 bits es altamente vulnerable, esto lo hace inseguro para sistemas de alta seguridad, por lo que en los últimos años se han estado haciendo intentos de encontrar un sustituto, pero por la inercia de su aplicación el proceso ha sido muy lento.

La opción más común que se ha elegido para suplantar a DES ha sido usar lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave, esto ha tomado la forma de un nuevo sistema de cifrado que se conoce actualmente como Triple DES o TDES.

⁷² Tablas de permutación.

⁷³ Tablas de sustitución.

⁷⁴ Electronic Frontier Foundation.

3.7.2.3.2 TDES

Debido a que el sistema DES se considera actualmente poco práctico -por la corta longitud de su clave- y para poder continuar utilizándolo, se creó Triple DES. El funcionamiento de Triple DES consiste en aplicar tres veces el sistema DES con claves de 56 bits distintas, con esto se consigue una longitud de clave de 128 bits. Esto se basa en que DES tiene una característica matemática particular, lo que implica que si se cifra el mismo bloque dos veces con claves diferentes, se aumenta el tamaño efectivo de la clave.

El funcionamiento de Triple DES es el siguiente, se le aplica al documento a cifrar un primer cifrado DES mediante la primera clave K_1 , al resultado se aplica un segundo cifrado con la segunda clave K_2 y al resultado se le vuelve aplicar DES, esta vez con la tercera clave K_3 .

En este sistema aunque se usa una clave de 168 bits⁷⁵, se ha podido demostrar que los ataques por fuerza bruta pueden romper a TDES con una complejidad 2^{112} en vez de necesitar 2^{168} , es decir efectuar al menos este número de operaciones para obtener la clave, además de necesitar los recursos computacionales para tales efectos.

3.7.2.3.3 AES

El sistema AES⁷⁶ nace cuando el NIST⁷⁷ en 1997 convoca a un concurso internacional para definir el Estándar de Cifrado Avanzado como sucesor del ya casi obsoleto DES, de manera que el nuevo algoritmo sea capaz de proteger información hasta bien avanzado el siglo XXI.

⁷⁵ Longitud efectiva de la clave, dada por la suma de tres claves de 56 bits.

⁷⁶ Advanced Encryption Standard.

⁷⁷ National Institute of Standards and Technology.

Dentro de las especificaciones y requisitos mínimos para este nuevo estándar criptográfico, se encontraban:

- Ser de carácter público.
- Ser un algoritmo de cifrado simétrico en bloque.
- Estar diseñado de manera que se pueda aumentar la longitud de clave según las necesidades.
- Ser implementable tanto en hardware como en software.
- Los algoritmos que cumplan con tales requisitos serían juzgados de acuerdo a:
 - Seguridad o esfuerzo necesario para criptoanalizarlos.
 - Eficiencia computacional.
 - Requisitos de memoria.
 - Simplicidad, flexibilidad y requisitos de licencia.

Como consecuencia del concurso en el año 2000 resultó elegido el sistema RIJNDAEL propuesto por los criptógrafos belgas, Vincent Rijmen y Joan Daemen.

RIJNDAEL es un cifrador que opera con bloques y claves de tamaño variable y que pueden ser especificados independientemente a 128, 192 y 256 bits, la razón de esto es que aunque una clave de 128 bits es imposible de romper probando todas las combinaciones posibles con los recursos computacionales actuales, no puede asegurarse que en el futuro próximo el estado de la computación lo permita.

El número de iteraciones que realiza el sistema depende del tamaño de la clave y de la longitud del bloque, las diferentes transformaciones que realiza actúan

sobre un resultado intermedio, este resultado intermedio del cifrado se denomina “Estado”, que puede representarse como un arreglo rectangular de bytes, la clave por su parte también se representa como una matriz rectangular de bytes. La transformación que tiene lugar en cada vuelta de cifrado está compuesta a su vez de cuatro transformaciones diferentes.

Según estudios publicados no existe un mecanismo para romper el algoritmo que sea más eficiente que el método de la fuerza bruta, además el diseño de los parámetros del algoritmo, número de vueltas, número de rotaciones, valores de la S-box, etc. fueron elegidos para hacer robusto al algoritmo frente a cualquier ataque de criptoanálisis.

3.7.2.3.4 IDEA

El sistema IDEA⁷⁸ fue desarrollado por Xuejia Lay y James Massey del SFIT⁷⁹ y a pesar de que lleva solamente unos años en uso es probablemente uno de los mejores algoritmos de bloques existente. Trabaja con bloques de 64 bits y utiliza claves de 128 bits, el número de iteración que utiliza son 8 en las cuales realiza el cifrado sobre la base de operaciones XOR, suma y multiplicación de enteros, es similar a DES, pero las iteraciones son más complejas.

En cada iteración el bloque de datos es dividido en cuatro sub bloques de 16 bits, a su vez se utiliza para cada vuelta seis sub claves.

Hasta ahora este sistema no se ha roto y se cree que es resistente al criptoanálisis ya que no hay pruebas de lo contrario. Se encuentra bajo patente de Ascom-Tech, aunque se permite su uso gratuito para aplicaciones no comerciales,

⁷⁸ International Data Encryption Algorithm.

⁷⁹ Swiss Federal Institute of Technology.

está libre de restricciones y permisos nacionales lo que lo ha hecho muy popular sobre todo fuera de EE.UU.

3.7.2.3.5 BLOWFISH

Este sistema fue creado por Bruce Schneier⁸⁰ y es un algoritmo de cifrado en bloque de clave secreta, el tamaño de los bloques es de 64 bits y utiliza claves de hasta 448 bits de longitud. Requiere una fase compleja de inicialización antes de que el cifrado pueda ocurrir, es eficiente en los microprocesadores grandes ya que fue diseñado para ser rápido, compacto, simple y robusto.

El algoritmo se divide en dos partes, una parte de expansión de la clave y una parte de cifrado de los datos. La expansión de la clave convierte una clave de 448 bits en varios arreglos de subclaves completando 4168 bytes. El cifrado de los datos ocurre vía 16 iteraciones, cada iteración consiste de una permutación dependiente de la clave y una sustitución dependiente de los datos y de la clave. Todas las operaciones son XOR y sumas sobre palabras de 32 bits. Blowfish utiliza una gran cantidad de subclaves, más concretamente un arreglo consistente de 18 subclaves de 32 bits, las que deben ser calculadas antes de cualquier proceso de cifrado o descifrado de datos.

Hasta el momento ha resistido con éxito todos los ataques conocidos, por ello y por su estructura se le considera uno de los algoritmos más seguros, a pesar de lo cual no se utiliza masivamente.

⁸⁰ Autor del libro "Applied Cryptography", considerado por muchos como la Biblia en cuestiones criptográficas.

3.7.2.3.6 RC

El sistema RC⁸¹ cuenta ya con varias versiones partiendo con la RC2 que tiene su código protegido bajo secreto comercial por RSA, es un algoritmo de cifrado en bloques de 64 bits desarrollado por Ronald Rivest y su versión de exportación limita su uso a claves de 40 bits. Para este sistema existen ataques criptoanalíticos que aunque requieren de gran cantidad de texto cifrado muestran las vulnerabilidades de RC2. Hoy en día RC2 tiende a utilizarse cada vez menos en beneficio de su hermano mayor RC4.

RC4 es un cifrador de flujo de 8 bits, también es un secreto comercial, aunque su código fuente ha sido publicado en algunos grupos de discusión, forma una parte importante del cifrado en SSL.

Por desgracia la versión exportable de RC4 tiene una clave de solamente 40 bits, lo que lo hace altamente vulnerable a ataques por fuerza bruta, la versión en EE.UU. cuenta con una clave de 128 bits que lo hace más seguro.

RC5 es un sistema de cifrado en bloques, se encuentra bajo patente de RSA, es relativamente nuevo y trabaja con bloques de longitud de 64 y 128 bits, el tamaño de la clave puede variar llegando a los 2048 bits, éste realiza operaciones de suma en módulo, XOR y rotaciones, también utiliza subclaves para su funcionamiento. Se conocen ciertos tipos de ataques contra él, aunque se considera un sistema seguro.

RC6 es un cifrador de bloque que se basa en RC5 y que soporta bloques de 128 bits.

⁸¹ Rivest Cipher.

3.7.2.4 Sistemas de Cifrado Asimétrico

En 1976 Whitfield Diffie y Martin Hellman en su trabajo titulado “New Directions in Cryptography” proponen las bases de un nuevo tipo de criptografía denominada de clave pública como solución a los problemas de gestión de claves que posee la criptografía simétrica. Este tipo de sistemas también es conocido como de dos claves, donde cada usuario tiene una clave que es privada sólo conocida por él y otra que es pública que puede ser revelada a todos los otros usuarios de un sistema.

La característica más destacable de estas claves, es que están relacionadas matemáticamente siendo una la inversa de la otra. La fortaleza del sistema depende del tamaño de las claves y la imposibilidad computacional de obtener una de las claves a partir de su inversa, esta imposibilidad se basa en que no se tiene el suficiente tiempo para romper el sistema con los medios técnicos actuales.

La razón del porque a este sistema se le denomina también asimétrico es debido a que no se puede utilizar la misma clave para cifrar y descifrar un mensaje, si se cifra un mensaje con una clave se debe descifrar con la otra.

Por lo tanto si un usuario desea enviar un mensaje secreto a otro debe utilizar la clave pública del receptor para cifrar el mensaje, ya que así sólo éste podrá descifrarlo utilizando la clave privada correspondiente, que sólo el debe conocer. Este procedimiento permite garantizar la confidencialidad de la comunicación, pero no garantiza su autenticidad, dado que todos pueden tener acceso a la clave pública del receptor, por lo que cualquier usuario podría ser el emisor de un mensaje. Por lo tanto si el emisor quiere garantizar la autenticidad del mensaje, debe cifrarlo con su propia clave privada, dado que todo el mundo conoce la clave pública con la cual descifrar el mensaje. Este proceso garantiza el origen del mensaje o sea la

autenticidad⁸², pero no garantiza la confidencialidad, ya que cualquiera puede descifrarlo.

Como se puede ver este nuevo sistema logra superar las dificultades de los sistemas simétricos proporcionando algunos de los servicios de seguridad buscados y mencionados desde el principio de este trabajo. Sin embargo la confidencialidad y autenticidad en el sistema asimétrico se logran por separado, entonces para lograr ambos objetivos es necesario combinar los procedimientos de forma apropiada.

Desgraciadamente este tipo de sistema no está libre de dificultades, uno de los principales es que los algoritmos de clave pública son alrededor de mil veces más lentos que sus pares de clave privada, debido a esta razón el cifrado de la información se suele realizar mediante criptosistemas de clave privada, mientras que los sistemas de clave pública se reservan para el cifrado de la clave utilizada para cifrar la información, ya que ésta posee menos datos. Además, de necesitar enviar un archivo cifrado a varias personas es necesario generar distintos archivos cifrados, porque se debe utilizar para cada una su respectiva clave pública.

Otro de sus inconvenientes se refleja en la necesidad de poder garantizar que el par de claves pertenecen a quien dice ser el dueño de ellas, lo que no nos permite aun garantizar el no repudio.

En cuanto a las técnicas empleadas por los sistemas de clave pública para generar sus claves, éstos hacen uso de propiedades matemáticas específicas orientadas a las funciones unidireccionales⁸³ como son la dificultad matemática del calculo del logaritmo discreto, el problema de factorización de grandes números primos o el problema de la mochila.

⁸² Este proceso esboza los principios de la firma digital.

3.7.2.4.1 RSA

Dentro de los sistemas de clave pública está el RSA, que es quizás el sistema de cifrado más empleado y extendido en la actualidad. El RSA fue creado por Rivest, Shamir y Adleman, de ahí su nombre, quienes lo desarrollaron en el MIT en 1978 basados en los estudios de Diffie y Hellman. Este sistema utiliza dos claves y cualquiera de las dos puede ser pública o privada. Las claves se generan matemáticamente a partir de la multiplicación de grandes números primos y otras complejas operaciones matemáticas.

El problema a resolver y en el que se fundamenta la seguridad del sistema consiste en la factorización de un número entero grande, que es producto de dos números primos de la misma longitud. La obtención de un número, producto de dos primos es fácil, pero del conocimiento de éste es computacionalmente imposible obtener sus dos factores primos.

O sea la única forma de atacar las claves sería factorizando este número en dos primos, pero está demostrado que este proceso de factorización de grandes números primos es enormemente costoso en tiempo y recursos computacionales.

Aunque este problema no es del todo inabordable, de hecho en 1977 una revista norteamericana desafió a sus lectores a factorizar un número con 129 dígitos, durante 17 años el problema estuvo sin solución, sin embargo en 1994 un grupo de científicos y matemáticos usando tiempo de CPU donado por 600 voluntarios a través de Internet consiguieron su factorización.

⁸³ En un sentido son muy fáciles de aplicar pero intentar invertirlos se transforma en un problema intratable.

Existen dos formas principales de utilizar RSA dependiendo de la aplicación:

- Esquema de cifrado. Se usa principalmente para cifrar claves de sistemas simétricos.
- Esquema de firma digital. Se usa para autenticar mensajes, cuenta con dos partes, una denominada Proceso de Firma o cifrado y la segunda denominada proceso de Verificación de la Firma o descifrado.

La generación de las claves RSA se sostiene en una serie de propiedades teóricas de la aritmética modular y de los números enteros como son que dos números enteros son relativamente primos si no tienen factores comunes. Por otro lado la función $\Phi(n)$, se denomina función de Euler⁸⁴ y se define como el número de enteros menores que n y relativamente primos a él.

El proceso a seguir para la generación de las claves es el siguiente⁸⁵:

- I Se eligen dos números primos p y q de gran longitud⁸⁶ y del mismo tamaño, los que se multiplican formando el módulo de cifrado.

$$n = p * q$$

- II Se calcula la función de Euler $\Phi(n)$.

$$\Phi(n) = \Phi(p * q) = (p - 1) * (q - 1)$$

- III Se elige un valor e entero positivo que cumpla⁸⁷:

$$1 \leq e \leq n$$

⁸⁴ Función que tiene como entrada un número entero y entrega el número de primos relativos a este.

⁸⁵ La explicación de los algoritmos aquí citados queda fuera del alcance de la tesis

⁸⁶ Números mayores de 100 dígitos.

⁸⁷ MDC es el número más grande que divide de manera entera a los dos.

$$\text{MCD}(e, \Phi(n)) = 1$$

- IV Se calcula d, mediante el algoritmo extendido de Euclides se calcula el inverso de e en el módulo $\Phi(n)$, o sea:

$$d = \text{inv}(e, \Phi(n))$$

$$\text{ó } e \cdot d \bmod \Phi(n) = 1$$

- V Configuración de las claves:

- Se publican n y e como clave pública del usuario.
- Se guarda en secreto el valor d como clave privada.
- Se guardan en secreto p, q y $\Phi(n)$ o se destruyen.

Una vez obtenidas las claves, se está en condiciones de cifrar mensajes para lo cual se utilizan las siguientes funciones:

▪ **Cifrado**

Si se desea cifrar el mensaje M^{88} con la clave pública de un usuario se utiliza:

$$C = M^e \bmod n$$

▪ **Descifrado**

Para que el usuario pueda descifrar el mensaje debe usar:

$$C^d \bmod n = (M^e)^d \bmod n = M^{e \cdot d} \bmod n = M$$

⁸⁸ Los mensajes deben ser representados en forma numérica por ejemplo ASCII.

Como se ve, los números e y d en combinación con n se utilizan como claves de cifrado y descifrado.

RSA es sin duda uno de los sistemas más estudiados hasta el momento y por lo tanto se considera uno de los más seguros ya que ha podido superar todo tipo de controversia, por lo que es uno de los sistemas criptográficos de llave pública más usados en el comercio y en general en toda actividad que requiera para su información un alto grado de seguridad.

Sin embargo, se han estado desarrollando una gran cantidad de sistemas de clave pública con el fin de sustituir o simplemente competir con RSA, los que no han tenido gran éxito. En principio estos nuevos sistemas deben de pasar un riguroso criptoanálisis por parte de la comunidad criptográfica, la prueba es en general proporcionar al menos la misma seguridad que los sistemas existentes con similar facilidad de implementación y que basen su seguridad en problemas muy complejos.

Hasta hoy sólo los sistemas basados en el Problema del Logaritmo Discreto Elíptico han podido competir exitosamente con el sistema RSA, incluso son más prometedores que éste, ya que con sólo llaves de 160 bits proporcionan la misma seguridad que RSA el que actualmente debe utilizar claves de 1024 bits.

3.7.2.4.2 DSA

El algoritmo DSA⁸⁹ es una modificación del sistema ElGamal y fue propuesto como algoritmo estándar de firma digital dentro del DSS⁹⁰ por el NIST en 1991. Esta medida fue muy criticada sobre todo por RSA Data Security, ya que esta compañía quería que su algoritmo se convirtiera en el estándar.

⁸⁹ Digital Signature Algorithm.

⁹⁰ Digital Signature Standard.

Dentro de los inconvenientes de DSA y en los que se basaron las críticas de RSA se encuentran que este sistema es solamente un estándar para firma digital, por lo tanto no se puede utilizar en el cifrado de información y por ende para distribuir claves. Otra desventaja de DSA es su lentitud en comparación con RSA en cuanto a la verificación de la firma digital, una ventaja eso si de DSA es que al momento de generar las firmas digitales, éste realiza dicha función con mayor agilidad.

El problema matemático que plantea este algoritmo y sobre el que basa su seguridad radica en la dificultad de calcular logaritmos discretos, ya que se puede calcular A^X de forma relativamente rápida para un X grande, pero encontrar el exponente de A que permita obtener un Y conocido, cuya forma es también del tipo A^X , es prácticamente irrealizable.

Para generar las claves en este sistema se deben seguir los siguientes pasos:

I Seleccionar un número primo q tal que:

$$2^{159} < q < 2^{160}$$

II Elegir un t tal que:

$$0 \leq t \leq 8$$

III Seleccionar un número primo p donde⁹¹:

$$2^{511 + 64t} < p < 2^{512 + 64t}, \text{ tal que } q \text{ divide a } (p-1)$$

IV Seleccionar un elemento $h \in \mathbb{Z}_p^*$ (números menores que p y relativamente primos a él) y calcular:

⁹¹ Si t=8 entonces p es un primo de 1024 bits.

$$g = h^{(P-1) / q} \bmod p$$

- V Repetir hasta que $g \neq 1$
- VI Seleccionar un número aleatorio X , tal que $1 \leq X \leq q-1$
- VII Calcular $y = g^X \bmod p$
- VIII La clave pública es (p, q, g, y) y la clave privada es X .

Ahora bien, para firmar un mensaje M , se debe hacer lo siguiente:

- I Seleccionar un entero K en el intervalo $[1, q-1]$
- II Calcular $r = (g^K \bmod p) \bmod q$
- III Calcular $K^{-1} \bmod q$
- IV Calcular $s = K^{-1} \{h(M) + X r\} \bmod q$, donde $h()$ es el algoritmo SHA –1 sobre el mensaje.
- V Si $s = 0$ entonces volver al paso 1.
- VI La firma para el mensaje M es el par de entero (r, s)

Para verificar la firma se hace lo siguiente.

- I Obtener una copia de la clave pública (p, q, g, y)
- II Verificar que r y s sean enteros en el intervalo $[1, q-1]$
- III Calcular $w = s^{-1} \bmod q$, $h(M)$
- IV Calcular $u_1 = h(m) w \bmod q$, $u_2 = r w \bmod q$
- V Calcular $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$

VI Aceptar la firma si y solo si $v = r$

3.7.2.4.3 ECC

Otro sistema criptográfico de clave pública es el ECC⁹² que usa curvas elípticas definidas en un campo finito. El criptosistema ECC basa su seguridad en el mismo problema que el DSA, pero en vez de usar números enteros como los símbolos del alfabeto del mensaje a encriptar o firmar, usa puntos en un objeto matemático, llamado Curva Elíptica. Este sistema puede ser usado tanto para cifrar como para firmar digitalmente.

La ventaja más destacable que ofrecen los ECC en comparación con RSA es la longitud de la clave secreta, se puede mostrar que mientras en RSA se tiene que usar una clave de 1024 bits para ofrecer una seguridad considerable, los ECC sólo usan 160 bits para ofrecer lo mismo, así también las claves RSA de 2048 bits son equivalentes en seguridad a 210 bits de ECC. Los requerimientos de memoria y CPU para realizar las operaciones criptográficas son también bastante inferiores por lo que este sistema es muy adecuado para ambientes restringidos en recursos donde el poder de computo es reducido y requiera una alta velocidad de procesamiento y grandes volúmenes de transacciones, lo que permite su uso por ejemplo en tarjetas inteligentes y celulares.

Los ECC son bastantes seguros, aunque existen varios tipos de curva y algunos se han revelado altamente vulnerables, aun así es el mejor candidato para remplazar a las aplicaciones que tienen implementado RSA.

Su desventaja fundamental es que muchas de sus variantes están patentadas por lo que no pueden utilizarse de forma libre.

Comparación de claves y algoritmos						
Clave Simétrica	Clave ECC	Clave RSA	Tiempo para descifrarla	Maquinas	Memoria	
56	112	420	5 minutos	10000	Trivial	
80	160	760	600 meses	4300	4 GB	
96	192	1020	3 millones de años	114	171 GB	
128	256	1620	10E16 años	0,16	120 TB	

Tabla 7: Comparación fortaleza relativa de claves ECC y RSA.

3.8 Funciones Hash

Las funciones Hash o de resumen son una herramienta fundamental en la criptografía moderna y son usadas principalmente para resolver otro de los aspectos de seguridad buscados, la integridad de los mensajes.

Estas funciones son ampliamente utilizadas en conjunto con la firma digital, ya que al ser aplicadas sobre un documento de tamaño variable, producen un pequeño resumen de tamaño constante.

Las funciones de resumen deben poseer las siguientes características para ser consideradas como tales:

- Cualquier cambio en el mensaje, por mínimo que sea, debe producir un resumen distinto.
- Debe tener compresión, o sea a partir de un mensaje de cualquier longitud, el resumen debe tener una longitud fija y lo normal es que sea menor que la del mensaje.
- La función no debe poder invertirse, debe ser unidireccional para que impida obtener el mensaje original a través del resumen.
- Debe ser fácil y rápida de calcular.

⁹² Elliptic Curve Cryptosystem.

- El resumen debe ser una función compleja de todos los bits del mensaje, debe proveer Difusión.
- Debe ser computacionalmente difícil encontrar un par de mensajes M y M' de forma que los resúmenes de ambos sean iguales, a esto se le denomina resistencia a las colisiones.

Otra de las características de las funciones Hash es que pueden ser utilizadas en dos formas:

- MDC. Los MDC⁹³ sirven para resolver el problema de la integridad de la información. Al mensaje se le aplica la función Hash y se manda el resumen junto con el propio mensaje. Al recibirlos el receptor, aplica nuevamente la función Hash al mensaje y comprueba que sea igual al Hash que se envió junto con el documento.
- MAC. Los MAC⁹⁴ sirven para autenticar el origen de los mensajes, así como también su integridad, para hacer esto se combina el resumen con una clave privada y se envía el documento junto con éste. Al llegar a su destino se comprueba la integridad de la clave privada mediante la pública correspondiente, con esto se demuestra el origen del mensaje. Adicionalmente se realiza el proceso descrito para MDC.

Los algoritmos Hash no emplean claves de ningún tipo, sino que se basan en extraer una determinada cantidad de bits a partir de un texto de longitud variable, o sea cada cierta cantidad de texto elegido de forma arbitraria se procede a realizar una transformación de bits, de esta transformación se obtiene una palabra, esta

⁹³ Modification Detection Code.

⁹⁴ Message Authentication Codes.

palabra tiene una extensión de X bits preestablecidos, de esta forma el texto se hace irreconocible, al poder leer sólo números secuenciales que no guardan relación alguna entre si.

3.8.1 **MD5**

El algoritmo Hash MD5⁹⁵, fue creado por Ron Rivest y distribuido por el grupo RSA Data Security, es la evolución de su versión anterior el MD4, debido a los ataques que esta ultima versión sufrió. Este algoritmo produce un resumen de 128 bits a partir de un bloque de texto de cualquier longitud, para ello divide el texto en bloques de tamaño fijo y luego realiza una serie de operaciones matemáticas en bloques sucesivos. Es uno de los algoritmos de resumen más extendido lo cual lo hace estar presente en variadas especificaciones y aplicaciones de seguridad.

El algoritmo funciona básicamente de esta manera:

- I Un mensaje de tamaño cualquiera M se alarga hasta que sea múltiplo de 512 bits añadiendo información adicional si es necesario al final del mismo. De esta forma se tiene un mensaje en bloques 512 bits.
- II Posteriormente se inicializan cuatro vectores de 32 bits cada uno.
- III Luego a cada bloque de 512 bits del mensaje se le realizan diversas operaciones lógicas de mezcla con los vectores.
- IV La salida de estas operaciones se convierten en el nuevo conjunto de vectores con los que se realiza la misma operación con el segundo bloque de 512 bits del mensaje, y así sucesivamente.

⁹⁵ Message Digest.

V Para finalizar, el algoritmo entrega un resumen producto de la concatenación de los últimos cuatro vectores resultantes de estas operaciones.

3.8.2 SHA-1

El algoritmo SHA-1⁹⁶ fue desarrollado por el gobierno de los EE.UU. a través del NIST con la ayuda de la NSA para ser incluido en el estándar DSS. Su funcionamiento es similar al MD5 con la diferencia que SHA-1 utiliza un vector más de 32 bits, con lo que obtiene resúmenes de 160 bits, lo que lo hace más seguro y evita posibles colisiones. Esto debido a que un resumen de 128 bits tiene una complejidad algorítmica de 2^{64} lo que actualmente es muy comprometedor, con un resumen de 160 bits en cambio se obtiene una complejidad de 2^{80} , en otras palabras esto representa la dificultad o el número de operaciones necesarias para generar dos mensajes aleatorios distintos que tengan el mismo resumen.

3.8.3 RIPE-MD160

El algoritmo RIPE-MD160 es una función Hash de 160 bits diseñado por Hans Dobbertin, Antoon Bosselaers y Bart Preneel. Es una versión del MD4 pero diseñada para resistir a los ataques criptográficos conocidos, se desarrolló como reemplazo para las funciones Hash de 128 bits, MD5 y RIPE-MD, los que fueron desarrollados por Ron Rivest y el proyecto de la comunidad económica europea llamado RIPE⁹⁷, respectivamente. Existen versiones de la función RIPE-MD que ofrecen longitudes mayores a 160 bits pero éstas son opcionales.

Para finalizar este capítulo se puede comentar que son muchos los avances en la criptografía y que si bien los criptosistemas no son del todo invulnerables,

⁹⁶ Secure Hash Algorithm.

⁹⁷ RACE Integrity Primitives Evaluation.

proporcionan la suficiente seguridad como para ser utilizados en el desarrollo de herramientas de seguridad.

No quiero terminar este capítulo sin plasmar algunas interrogantes que me parecen interesantes de analizar como son: ¿Hasta donde llegará la competencia entre la criptografía y el criptoanálisis?, ¿Alguna vez uno llegará a superar definitivamente a su oponente?, ¿Qué ocurrirá al seguir aumentando el poder de procesamiento de los computadores, se seguirá aumentando simplemente el tamaño de las claves?. Tal vez el tiempo entregue las respuestas.

Pues bien una vez familiarizado con los detalles de la criptografía y sobre todo con los sistemas asimétricos o de clave pública, se está en condiciones de abordar el tema central de este estudio, las PKI.

4.1 Preámbulo

Este capítulo tiene como objetivo develar las características y secretos del tema principal que aborda esta memoria, la Infraestructura de Claves Públicas, más conocida por sus siglas en ingles PKI y que se determinó como una solución a la problemática de mejoramiento de seguridad desarrollada al principio de este documento.

Teniendo en mente este objetivo, se describen los componentes necesarios para la operación e implementación de las PKI, los servicios que éstas proporcionan y las normas o estándares que las rigen, los que juntos ayudan a cumplir los objetivos de proporcionar un entorno seguro para la administración de las claves⁹⁸ de los usuarios, además de ser un medio en el que se apoyen e implementen diversas aplicaciones que requieran altos niveles de seguridad como son sistemas de transacciones, servicios de correo y canales de comunicación seguros.

4.2 Introducción

Internet no es sólo un instrumento esencial en el comercio electrónico que ha revolucionado a todos los entes participantes de la nueva economía, sino también es un instrumento importante para diversas actividades alejadas de aquellas que tienen que ver con los beneficios económicos. Sin embargo en ambos casos la seguridad es un factor importante para así poder realizar comunicaciones confiables.

⁹⁸ Claves provenientes de los sistemas de criptografía de clave pública.

Esta red, como ya sabemos, hace posible que las comunicaciones puedan ser escuchadas y que las identidades de personas y maquinas sean susceptibles de suplantación, lo que deriva en una alta posibilidad de realizar engaños. Debido a esto las necesidades de seguridad se han visto incrementadas enormemente y por ende el uso de la criptografía también ha aumentado como medio de solución para satisfacer estas necesidades.

Dentro de esto, la protección de la información usando algoritmos simétricos es relativamente fácil en redes pequeñas, requiriendo el intercambio de claves secretas entre cada parte en la comunicación, pero cuando las redes aumentan en tamaño el intercambio seguro de claves secretas acrecienta sus costos y se hace inmanejable.

Dentro de los tipos de criptografía, como se vio en el capítulo anterior, la denominada criptografía asimétrica o pública proporciona maneras más eficientes de conseguir los servicios de autenticación y confidencialidad.

Por otro lado las funciones Hash también allí descritas nos entregan la necesaria seguridad en la integridad de los datos, pero todavía falta garantizar el No repudio de las claves asimétricas y por tanto de las acciones realizadas con ellas, ya que éstas si bien no pueden ser rotas criptográficamente, si pueden ser erróneamente atribuidas a un individuo o pueden ser descubiertas por una mala administración por parte de su propietario.

Para poder utilizar entonces este tipo de sistemas criptográficos y conseguir el No repudio de la información, se requiere de una entidad que permita certificar las claves de los entes que así lo requieran. Ya que sin esto la criptografía de clave pública no es mucho más eficiente y útil que la tradicional de clave privada, por lo que tendría sus mismas limitaciones y dificultades.

Como consecuencia, en orden a utilizar de manera exitosa la criptografía de clave pública, es que ciertos servicios como la generación de las claves, su distribución, almacenamiento y la revocación⁹⁹, entre otros, son también imprescindibles.

En el mismo sentido, la certificación de las claves públicas de un usuario debe ser realizada por una organización confiable, requisito fundamental para asegurarse de que dichas claves pertenecen al interlocutor con quien supuestamente nos estamos comunicando, el depósito de las claves en una tercera parte confiable para su distribución es otra necesidad importante. Por todo esto es que se hace absolutamente necesario una infraestructura o entorno que cuente con la absoluta confianza para los usuarios y que soporte todas estas actividades.

Este entorno es el que se denomina Infraestructura de Claves Públicas, sistemas mixtos de software y hardware basados en diferentes agentes que permiten dotar a maquinas y usuarios de identidades digitales absolutamente certificadas, la que es considerada por algunos expertos como una de las herramientas más adecuadas para el desarrollo definitivo del comercio electrónico y otro tipo de servicios que necesiten cumplir con amplios estándares de seguridad.

4.3 Firma Digital

Puesto que la naturaleza del medio que se requiere asegurar es no físico, los métodos tradicionales del mundo real como marcar con sellos y firmas manuscritas para legalizar documentos en papel ya no son útiles. En vez de eso, las nuevas marcas a implementar deben ser codificadas en información del mismo carácter que

⁹⁹ Cuando una clave se ve comprometida debe existir un método de informar a los demás usuarios que la clave ya no es válida o confiable.

los datos que se quiere sellar. Por esto, es que se han desarrollado herramientas basadas en los computadores como solución a la problemática tecnológica de firmar documentos electrónicos con el propósito de legalizarlos.

Este procedimiento se conoce como firma digital y está cobrando gran importancia en los medios de pago electrónico vía Internet como elemento de seguridad y generador de confianza, tanta fuerza es la que posee este sistema, que en la mayoría de los países ha sido avalado mediante leyes específicas que lo constituyen en una prueba ineludible de autoría de un documento electrónico, homologándolo a la firma tradicional manuscrita.

Aunque el problema de seguridad más conocido es el de la confidencialidad de los mensajes, con el auge de las comunicaciones electrónicas ha cobrado especial importancia el tema de la autenticidad, íntimamente relacionado con esto se encuentra la firma digital, que además de lo anterior, asegura que el firmante de un mensaje no puede posteriormente negar su autoría.

Para demostrar el funcionamiento de la firma digital se muestra los siguientes ejemplos:

Supongamos que una persona B y otra A comparten una clave secreta y que A recibe un mensaje cifrado supuestamente por B. Tras la recuperación exitosa del mensaje, A no tiene dudas 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 A¹⁰⁰.

Sin embargo este problema se puede resolver de manera fácil usando el cifrado de clave pública para proporcionar una firma digital.

¹⁰⁰ Por el hecho de compartir la clave secreta.

Por ejemplo, un usuario A obtiene un resumen o Hash de un documento a firmar -se utiliza un resumen del documento y no el documento mismo por el volumen de datos involucrados¹⁰¹, lo que haría el proceso de firma demasiado lento¹⁰²-, el mensaje resumido es entonces cifrado con la clave privada de A, transformándose esto en la firma digital¹⁰³, A entonces envía el mensaje junto con la firma. La firma digital puede sólo ser descifrada por la clave pública del mismo individuo.

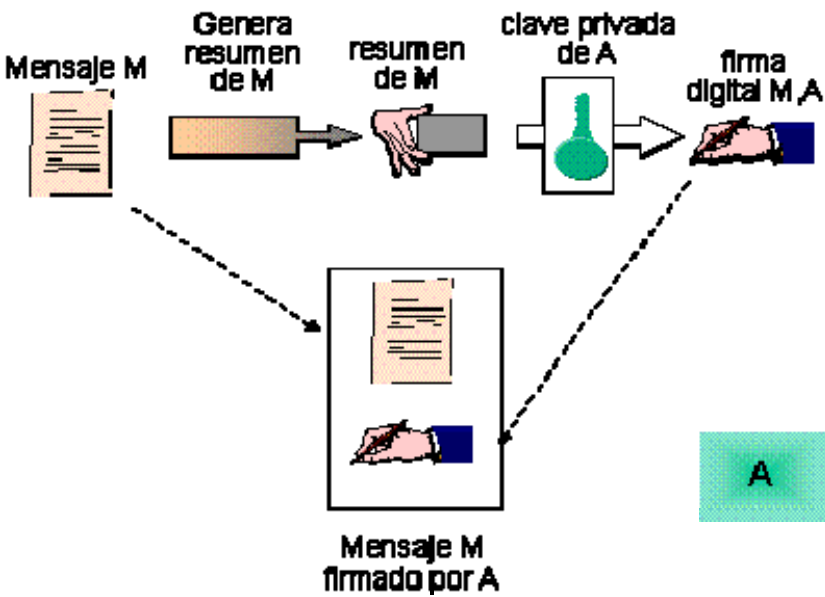


Figura 11: Esquema de generación de firma digital.

El receptor del mensaje B descifra entonces la firma digital, obteniendo así el resumen original y luego calcula nuevamente el resumen del mensaje, el valor de este nuevo resumen es comparado con el resumen del mensaje encontrado en la firma digital. Si ambos concuerdan, el mensaje no ha sido alterado en su trayectoria hacia el destinatario, ya que de ser así los resúmenes no coincidirían, esto nos proporciona la integridad del mensaje.

¹⁰¹ El resumen es único para cada documento por lo que lo representa en todos los aspectos, esto también hace a la firma distinta para cada uno.

¹⁰² Es sabido que el proceso de cifrado con el sistema de claves públicas es más lento que el sistema de claves privadas pues requieren un computo mayor.

¹⁰³ Bloque de caracteres que se anexa a un documento electrónico.

Adicionalmente, puesto que la clave pública del emisor fue utilizada para descifrar la firma, el resumen debe haber sido cifrado con la clave privada correspondiente, conocida sólo por el emisor del mensaje, lo que nos da la autenticidad.

Junto con esto, si la propiedad de las claves está certificada por un ente confiable, el emisor de un mensaje firmado con este esquema no puede desconocer su firma, ya que nadie salvo él podría haber generado el resumen cifrado con tal clave privada, lo que nos procura el No repudio.

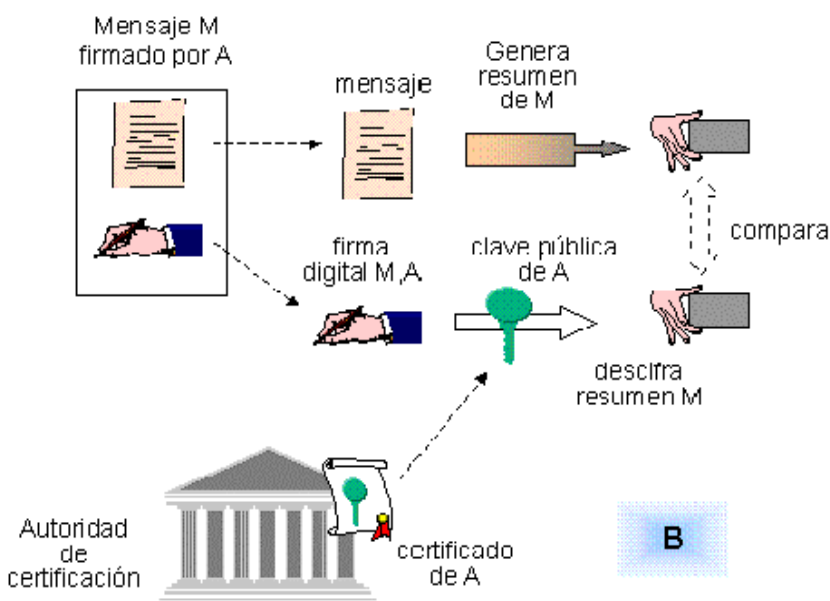


Figura 12: Esquema de verificación de firma digital.

Adicionalmente se puede cifrar esta concatenación, el documento y su correspondiente firma, con la clave pública del receptor del mensaje, en este caso B, transformándose en lo que se conoce como el sobre digital. La persona que recibe el mensaje entonces lo descifra utilizando su clave privada, lo que nos proporciona la confidencialidad.

Como vemos, hemos encontrado todos los aspectos de seguridad que se consideraban necesarios para un sistema con elevados requerimientos de seguridad.

De forma anexa se puede combinar este esquema con un estampado o firma de tiempo, lo que también puede probar que el documento existía en cierto instante determinado.

Sin embargo como ya se mencionó, la utilidad de una firma digital está limitada por la habilidad del receptor de asegurar la autenticidad de la clave usada para verificar la firma. Por ejemplo si un usuario A usa su clave privada para firmar un mensaje, otro usuario B puede verificar que A realmente lo envió, sólo si este (B) conoce la clave pública de A.

En orden a confiar sobre la autenticidad de la clave pública, B necesita obtener algo que certifique la clave de A, porque otro usuario C podría estar falsificando un mensaje de A y enviando su propia clave pública, pretendiendo ser A. Como C tendrá la correspondiente clave privada a la pública que le envió a B, éste (B) intentará verificar la firma del mensaje falso, lo que resultará en la confirmación de la autenticidad del mensaje aunque éste no venga realmente de A.

En contraste si B accede a la clave pública de A desde un origen externo confiable, y usa ésta para verificar el mensaje firmado con clave privada de C la verificación fallará, revelando la falsificación y el intento de suplantación de identidad.

En resumen si A y B son extraños y no existe un medio de comunicación que les permita identificarse de forma exacta, la única manera de autenticarse sería mediante la asistencia de una tercera parte confiable externa a ellos, que enlace sus identidades con sus claves públicas.

Para solucionar este problema surgen las Autoridades de Certificación o terceras partes de confianza, que son aquellas entidades que merecen la confianza de los demás actores en un escenario donde no existe confianza directa.

Es por tanto necesaria, una infraestructura que cierre el círculo de confianza, proporcionando una correspondencia fehaciente de las claves públicas con sus propietarios, para permitir así la autenticación de los mensajes y su imputación a una determinada persona.

4.4 Infraestructura de Claves Públicas

En la actualidad las organizaciones que ofrecen servicios en el mundo virtual, deben proporcionarlos bajo condiciones de máxima seguridad para garantizar la confidencialidad, integridad, autenticidad y no repudio de la información, que se entienden obligatorios en los sistemas informáticos modernos.

Como se describió en el capítulo de criptografía, el problema de autenticación y protección de privacidad en grandes redes fue expuesto por Diffie y Hellman cuando publicaron sus conceptos para un método de intercambio de mensaje secretos sin tener que compartir una clave secreta. Esta idea fructificó con la invención del sistema RSA, que en vez de usar la misma clave para el proceso de cifrado y descifrado de datos, usa claves diferentes.

Todas las propiedades de que goza la criptografía de clave pública, cuyo uso más común queda de manifiesto en la firma electrónica, la convierten en candidata ideal para prestar los servicios de seguridad ya varias veces mencionados en este trabajo de tesis. Cuando se desea proporcionar entonces todos estos servicios a una empresa u organización, estamos hablando de dotar a la organización de una PKI.

Ahora bien, actualmente la criptografía de clave pública es la parte fácil pero el desafío ahora es la PKI, que nos permite identificar en quien podemos confiar y bajo que circunstancias, además de si la clave pública que estamos utilizando es la correcta y si no ha sido rota.

Básicamente una PKI es una estructura funcional basada en el cifrado que debe realizar las siguientes operaciones:

- Obtención de la identificación de los usuarios¹⁰⁴.
- Validación de la identidad de los usuarios.
- Generación segura de claves.
- Gestión de solicitudes de certificación¹⁰⁵ de claves.
- Emisión y validación de certificados.
- Gestión de almacenamiento de certificados y claves.
- Gestión de publicación y distribución de certificados.
- Gestión de revocaciones y pérdida de vigencia de certificados.
- Gestión de renovación de certificados.
- Soporte de aplicaciones adicionales como: estampado de tiempo, recuperación de certificados, firma y cifrado de objetos, entre otras.
- Administración de relaciones de confianza.

Para que una PKI pueda realizar todas estas actividades generalmente incluirá elementos como una o varias Autoridades de Registro para certificar la identidad de los usuarios; una o varias Autoridades Certificadoras que emitan los certificados de clave pública; un repositorio de certificados y listas de revocación; prácticas y políticas que permitan controlar y sincronizar estos componentes además

¹⁰⁴ Todo ente que se relacione con la PKI ya sea para su certificación o la verificación de otro usuario.

¹⁰⁵ La certificación se refiere a proporcionar la identidad real de un solicitante.

de administrar el ciclo de vida de los certificados digitales desde su solicitud hasta el momento de su revocación.

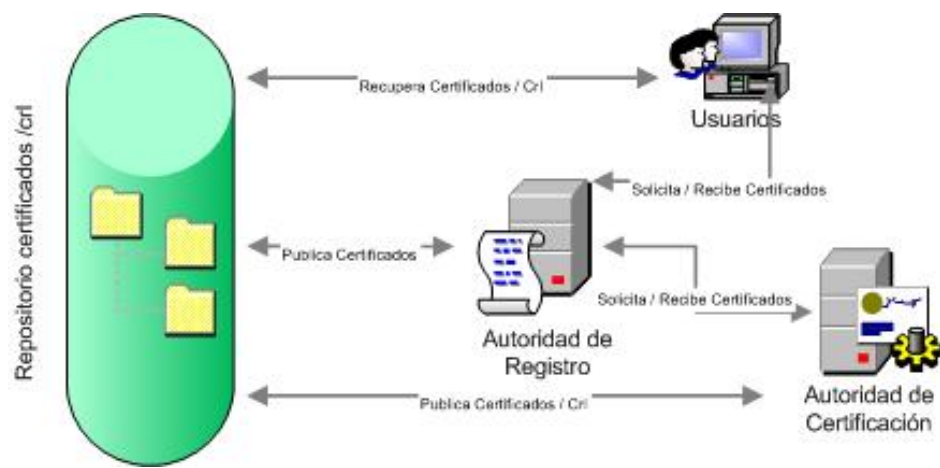


Figura 13: Esquema PKI.

4.4.1 Políticas de Certificación

Toda organización y por ende toda PKI necesita de ciertas reglas o políticas para operar de manera adecuada y para poder generar en sus usuarios la confianza en los procedimientos que ejecuta.

Estas políticas son un conjunto de normas que definen la dirección de la PKI a alto nivel, así como los procesos y principios acerca del uso de la criptografía, típicamente esto incluye definiciones de cómo la PKI maneja las claves de los usuarios junto con otra información de valor y cómo configura los elementos de control requeridos para el manejo de los distintos niveles de riesgo. Son también documentos en los que se indican los procedimientos y reglas que gobiernan a las autoridades certificadoras y las de registro, entre las que destacan, cómo se efectúan las solicitudes, cuál es la información necesaria a incluir en éstas, cómo se aceptan las solicitudes de certificación, cómo se verifican las identidades de los solicitantes, cómo se generan los certificados, cómo se renuevan y revocan los certificados y cómo se publican, entre otras cosas.

4.4.2 Autoridad de Certificación

Una CA¹⁰⁶ es la entidad dentro de la PKI que da fe o que certifica que ciertas identidades¹⁰⁷ están relacionados con las claves públicas que aparecen en los certificados que ésta emite. No se trata tan solo de una fabrica productora de certificados, sino que implica el administrarlos apropiadamente para lograr el objetivo de una correcta implementación de identidades digitales.

La CA entonces desarrolla procedimientos que verifican la identidad de un solicitante de certificado y expide un certificado digital firmado por ella y que es prueba de dicha identidad. Esta autoridad puede ser un organismo público o privado que busca llenar la necesidad de una tercera parte de confianza y que se hace responsable por la información contenida en sus certificados, ya que con su firma garantiza la validez de éstos.

Para solicitar un certificado la persona o entidad interesada debe cumplir algunos procedimientos previos, confeccionando generalmente una solicitud de certificación que debe ser presentado ante la CA¹⁰⁸, en la que deben figurar los datos del solicitante¹⁰⁹ y su clave pública¹¹⁰. También debe manifestar su voluntad de aceptar conformidad con dicha clave pública y demostrar que es el propietario real de la clave privada asociada a ésta¹¹¹.

La administración de certificados por parte de la CA implica la generación, renovación, distribución, almacenamiento, revocación, suspensión y destrucción de claves, certificados y listas de revocación de certificados.

¹⁰⁶ Certification Authority.

¹⁰⁷ Usuarios, maquinas, servidores e incluso la misma Autoridad Certificadora.

¹⁰⁸ Generalmente esta responsabilidad se le delega a una Autoridad de registro.

¹⁰⁹ Nombre, razón social, RUT, dirección, correo, etc. dependiendo del tipo de certificado solicitado.

¹¹⁰ Si las claves las generó el usuario.

¹¹¹ En algunos esquemas tanto la clave pública como la privada las genera la CA.

Asimismo la CA también es la encargada de establecer los estamentos de prácticas de certificación que especifican elementos como el tamaño de claves generadas, algoritmos utilizados, información presente en los certificados, fechas de inicio y fin de validez de éstos, uso y restricciones de las claves y certificados, forma de almacenamiento, etc. Los que deben quedar disponibles a los usuarios. Junto con esto, la CA debe proporcionar las herramientas y procedimientos además del personal responsable para el correcto registro de los datos de sus usuarios, todo basado en una serie de normas tanto tecnológicas como legales.

La CA se encarga también de firmar además de los certificados, las listas de revocación de certificados que emita. De forma conjunta debe entregar la posibilidad de recuperar las claves, certificados y listas de revocación publicándolos en un repositorio accesible a todos los usuarios, éstos son generalmente servidores de acceso libre que realizan la función de deposito de los certificados y listas revocación.

Uno de los principales desafíos de una CA radica en que la confianza de los usuarios es fundamental para el buen funcionamiento del servicio. El entorno de seguridad de la CA ha de ser muy fuerte, en particular en lo que respecta a la protección de la clave privada que utiliza para firmar sus certificados. Si este secreto se viera comprometido, toda la seguridad de la infraestructura de clave pública se vería afectada.

Una pregunta interesante a responder es ¿Quiénes pueden ser capaces de generar la confianza de los usuarios? Los principales candidatos son siempre las entidades que ya gozan de un prestigio en el ámbito de seguridad, como pueden ser organizaciones de gobierno, el SII¹¹² por ejemplo o privados como los bancos. La

¹¹² Servicio de Impuestos Internos.

alternativa a estos es establecer una entidad que se gane la reputación de confiable al construir instalaciones muy seguras y establecer procedimientos de certificación rigurosos.

4.4.2.1 Certificados Digitales

¿Cómo puede el receptor de una clave pública cerciorarse que ésta realmente pertenece a la persona que se indica?, ¿Podría alguien hacerse pasar por una identidad legítima y mirar como los demás inconcientemente le envían documentos secretos?.

La respuesta es sí, por lo que es muy importante estar realmente seguro de que la clave pública que manipulamos para verificar una firma o cifrar un texto pertenece realmente a quien pensamos. Ya que sería desastroso cifrar y enviar un texto confidencial con una clave pública de alguien que no es el receptor imaginado.

Para solucionar esto, existe el certificado digital, un tipo de pasaporte o cedula pero digital que forma una asociación entre la identidad de un individuo y su pareja de claves. Un certificado digital contiene además de la clave pública del propietario, la información suficiente para satisfacer a un tercero acerca de la correcta identidad que en él se presenta.

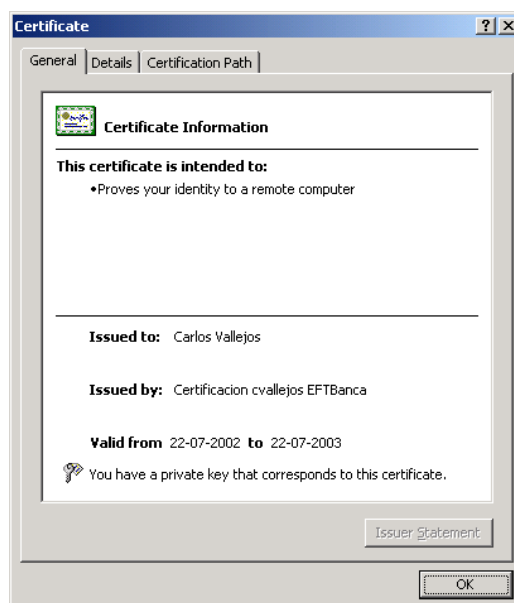


Figura 14: Certificado Digital almacenado en IExplorer.

El detalle de la información contenida en los certificados típicamente incluye:

- **Sujeto:** Nombres y apellido del sujeto que se identifica con el certificado¹¹³.
- **Emisor:** Identifica la fuente de confianza que generó el certificado.
- **Número de serie:** identifica al certificado como único.
- **Clave pública:** La clave pareja de la clave privada del sujeto.
- **Válido desde:** Especifica la fecha desde la cual el certificado es utilizable.
- **Válido hasta:** Especifica la fecha hasta la cual el certificado se puede utilizar.
- **Algoritmo de firma:** Indica el algoritmo de resumen y el sistema mediante el cual se generó la firma.

¹¹³ Puede incluir información adicional como correo electrónico, organización, localidad, etc.

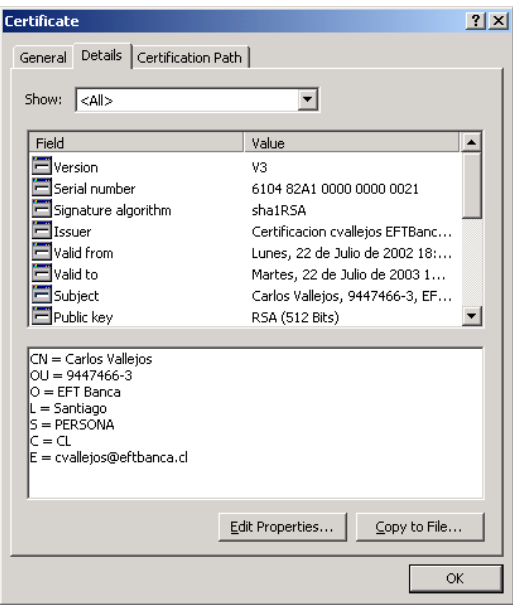


Figura 15: Detalle contenido de un certificado digital.

Con un certificado entonces, el receptor del mensaje ahora utilizará éste para verificar la identidad del propietario de la clave pública, puesto que confía en la entidad que certifica dicha identidad¹¹⁴, por lo que ahora usará la clave pública contenida en el certificado para verificar los mensajes firmados que pudiera recibir del titular del certificado.

Para aumentar la seguridad del sistema, una decisión importante que deberá tomar un usuario es ¿En los certificados de que CA confiar?, Esta decisión probablemente se basará en la reputación de la CA sobre el nivel de investigación emprendido para certificar una identidad.

4.4.2.1.1 Tipos de certificados

En la práctica una CA puede ofrecer una variedad de certificados clasificados comúnmente de acuerdo a las aplicaciones en los que se utilizarán y el nivel de investigación utilizado para confirmar la identidad del sujeto o titular.

¹¹⁴ Adicionalmente debe verificar la firma del certificado con la clave pública de la CA.

Dependiendo del uso, funcionalidad o destino que se les va a dar a los certificados, éstos se pueden clasificar en varios tipos.

4.4.2.1.1.1 Certificados de Identificación

Un certificado de identificación conecta un nombre, en este caso el del titular con una clave pública, adicionalmente en sus prácticas de certificación debe existir una declaración del tipo de investigación llevada a cabo para comprobar la identidad del titular. El nombre no necesariamente necesita ser único o igual al nombre real, el nombre o identidad digital podría perfectamente ser un seudónimo.

Desde el punto de vista de la identidad certificada, se pueden dividir en personas o servidor:

- **Certificados Persona**

Se expiden a personas físicas y es utilizado para autenticación de clientes ante servidores¹¹⁵.

Según los niveles de comprobación acerca de la identidad de las personas, éstos se pueden subdividir en clases:

- Clase 1: Corresponden a los certificados más fáciles de obtener e involucran muy pocas verificaciones de la identidad del titular.
- Clase 2: En estos la autoridad comprueba los datos por ejemplo de la cedula de identidad, permiso de conducir o el pasaporte del interesado.

¹¹⁵ Principalmente en comunicaciones tipo SSL.

- Clase 3: Adicionalmente a los controles anteriores, se verifican por ejemplo antecedentes comerciales y se solicita la presencia física para realizar la validación de esta información.

Según el uso que se hará del certificado, éstos se pueden clasificar por ejemplo en certificados de:

- Correo: Estos certificados permiten que los mensajes de correo electrónico sean firmados y cifrados digitalmente.
- Firma de Código: Son usados para identificar al autor de una aplicación o dll mediante su firma.

▪ **Certificados Servidor**

Son usados para identificar a un servidor ante un cliente y se expiden a nombre de la empresa propietaria del servidor. Vinculan generalmente la dirección Web o DNS del servidor con su pareja de claves¹¹⁶.

4.4.2.1.1.2 Certificados de Autorización

Aunque los certificados de identificación son los más populares, en el corto plazo las CA probablemente comenzarán a emitir certificados con atributos distintos a los referidos a la identidad de las personas.

Un certificado de autorización puede indicar información referente a donde reside un sujeto, o la edad de éste para comprobar su mayoría de edad en algunas transacciones comerciales, la pertenencia del sujeto a una organización en particular o si es ciudadano de algún país.

¹¹⁶ La presencia de este certificado es condición imprescindible para establecer comunicaciones SSL con un Servidor Web.

Estos certificados tienen muchos usos potenciales. Por ejemplo los profesores que intercambian preguntas de un examen sobre Internet podrían requerir que los colegas demuestren su calidad de miembro en la asociación de colegios de profesores antes de permitirles el acceso a alguna de las preguntas. Los certificados de nacionalidad por ejemplo permitirían implantar sistemas de votación electrónica que incluyan a personas de un país residentes en el extranjero.

4.4.2.1.1.3 Certificados de Transacciones

Este tipo de certificado atestigua un cierto hecho o formalidad distinto a un certificado que identifica o autoriza, un certificado de transacción no se generaría para ser reutilizado.

Por ejemplo si Alicia es abogada y Bob es su cliente, Bob puede firmar digitalmente un documento, Alicia entonces publica un certificado que atestigua que Bob lo firmó digitalmente en su presencia. El certificado puede contener el texto del documento, la firma digital de Bob y la clave pública de éste, que será firmado por la clave privada de Alicia, el certificado resultante sería evidencia que Bob puso su firma en presencia de Alicia. Este acto llevará probablemente en el futuro algún tipo de formalidad asociada quizás a un acto notarial, de hecho ya se está mencionando la posibilidad de una especialización legal denominada Cibernotario.

4.4.2.1.1.4 Certificados de Tiempo

Los certificados de tiempo o de estampado digital de tiempo permiten dar fe a través de la firma electrónica de que un documento existía en un instante determinado de tiempo, por lo que constituyen un elemento fundamental de todos los servicios de registro contractual y de protección de la propiedad intelectual o industrial que se están proponiendo actualmente en el mundo electrónico.

4.4.2.2 Listas de Revocación

Los certificados por su naturaleza y debido al papel que desempeñan no deben ser documentos imperecederos, al igual como sucede con los documentos de autenticación del mundo físico. Estos al estar basados en el uso de claves no convienen que sean válidos por periodos de tiempo muy largos, ya que uno de los principales problemas del manejo de las claves es que cuanto más vida tienen es mayor la probabilidad que algún extraño se apodere de ellas.

Además con el paso del tiempo los equipos informáticos van aumentando su poder de calculo, facilitando con ello la labor de los criptoanalistas, por este motivo los certificados digitales tienen estipulado un periodo de validez que suele ser de un año.

Por consiguiente puede ser necesario en un momento dado anular una pareja de claves, bien porque se crea que las claves estén comprometidas, o porque la persona o entidad propietaria haya incurrido en algún delito. Debido a la importancia que esto reviste es que existe la posibilidad de anular un certificado, esta revocación la lleva a cabo la autoridad certificadora a petición de autoridades judiciales o del titular del certificado, o porque la CA lo considera necesario.

Para llevar un control de los certificados revocados las autoridades de certificación utilizan lo que se conocen como Lista de Certificados Revocados o CRL¹¹⁷. Una CRL es un archivo emitido cada cierto tiempo y firmado por la CA, que contiene la fecha de emisión de la misma y una lista de certificados revocados, figurando para cada uno de ellos su número de identificación, la fecha en que ha sido revocado y opcionalmente el motivo de la revocación.

¹¹⁷ Certificate Revocation List.

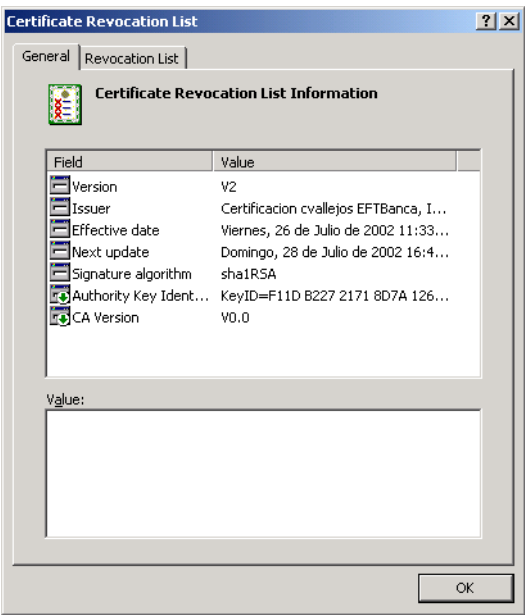


Figura 16: Lista de certificado revocados.

Los motivos más comunes de revocación son que los datos del titular han dejado de ser válidos, la clave privada del mismo se ha visto comprometida o el certificado a dejado de tener validez en el contexto para el que había sido emitido. Otras razones pueden ser que por disposiciones legales la persona asociada a un certificado ya no tenga la facultad de utilizar su clave, o que la seguridad de los sistemas de la CA se encontrasen comprometidos.

Toda CRL provee información acerca de los certificados revocados, pero estas pueden manejar varios esquemas como son contener el historial de todos los certificados revocados durante la existencia de la CA o bien pueden sólo publicar los certificados revocados desde la emisión de la ultima CRL, en todo caso ninguno de los dos esquemas está exento de dificultades.

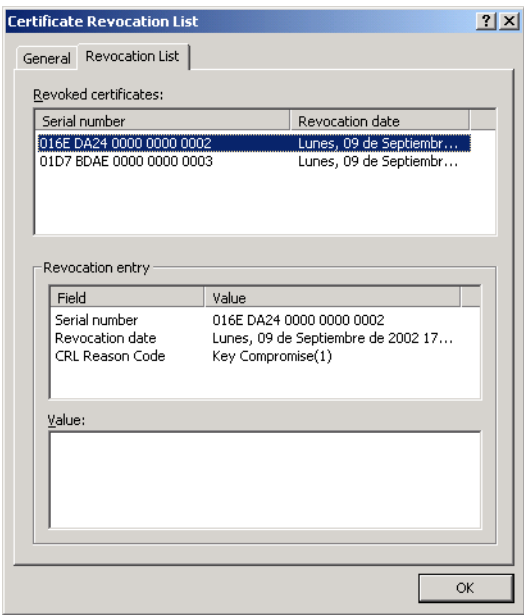


Figura 17: Detalle lista de certificados revocados.

Existen algunos problemas con las CRL, ya que éstas deben cada cierto tiempo -definido por la CA- ser actualizadas para su consulta por los usuarios. Estos generalmente deberán conservarlas en sus equipos, lo que dependiendo del universo de certificados que maneje la CA podría derivar en un problema futuro de capacidad de almacenamiento, por el tamaño que estas CRL lograrían alcanzar.

Una forma de mejorar la utilización de listas de revocación es dividir las por causa de revocación o zonas geográficas, lo que ayudaría a disminuir su tamaño y los posibles problemas de almacenamiento.

Otra de las dificultades de las listas de revocación es el lapso de tiempo entre que el certificado pierde su confiabilidad y la publicación de tal hecho en la lista de revocación, esto genera una ventana de tiempo durante la cual un certificado y su clave no válida pueden ser utilizados.

El uso de una CRL en un proceso de autenticación presenta otro problema, ya que puede resultar inadecuada en aquellas operaciones que exijan una velocidad alta de procesamiento, en estas operaciones consultar una CRL podría disminuir

enormemente su rendimiento, sobre todo si la lista de revocación a consultar tiene un tamaño muy grande.

Una solución a estos problemas los dan los servicios que implementan OCSP¹¹⁸, y que son ofrecidos por personas o entidades de confianza, estos servicios al recibir una petición de validez de un certificado responden al instante si en esa fecha y hora concreta el certificado es válido o si por el contrario está revocado. Para dar validez a la respuesta el servicio la firma con su clave privada, con lo que el usuario está seguro de la veracidad de la respuesta recibida.

4.4.2.3 Declaración de Prácticas de Certificación

Son las reglas encargadas de establecer el uso que se les confiere a los certificados, son más conocidas por sus siglas en inglés CPS¹¹⁹. Estas políticas son uno o varios documentos que establecen los procedimientos operacionales sobre cómo las políticas de certificación serán reforzadas y soportadas en la práctica por la CA, además permiten que los usuarios se sientan satisfechos acerca de la seguridad de las identidades certificadas.

Estas reglas típicamente incluyen definiciones de cómo la CA es operada; cómo los certificados son emitidos, aceptados y revocados; cómo se establecen los valores de los parámetros contenidos en los certificados dependiendo del uso que se vaya a hacer de los mismos; cómo las claves serán generadas, con qué algoritmos, de qué tamaño serán éstas, cómo serán registradas y verificadas, dónde se almacenarán y cómo quedarán disponibles a los usuarios, etc.

¹¹⁸ On Line Certificate Status Protocol.

¹¹⁹ Certificate Practice Statement

Según el estándar X.509, una Política de Certificación es “Un conjunto designado de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o clase de aplicación con requerimientos de seguridad comunes”.

Los conceptos CP¹²⁰ y CPS vienen de diferentes orígenes y fueron desarrollados por diferentes razones, sin embargo su interrelación es importante.

Un CPS es un estamento detallado por una CA de sus prácticas, que potencialmente necesitan ser entendidas y consultadas por usuarios, y aunque el nivel de detalle puede variar, los CPS generalmente son más detallados que sus definiciones de Políticas de Certificación. En todo caso Una CP puede ser expresada como un conjunto de cláusulas y un CPS puede ser expresado como un conjunto único de cláusulas con cada componente direccionando los requerimientos de una o más CP.

Por ejemplo, un CPS puede ser expresado como una combinación de:

- a) Una lista de CP.
- b) Para cada CP en a), un conjunto de cláusulas las cuales contiene estamentos que refinan la CP, completando detalles no estipulados o expresamente dejados a las decisiones de los CPS por la CP.
- c) Un conjunto de cláusulas que contienen estamentos relativos a las prácticas de certificación de la CA, sin tener en cuenta la CP.

Los estamentos proporcionados en b) y c) pueden aumentar las condiciones aplicables de la CP, pero no deben tener conflictos con ninguna de sus disposiciones.

¹²⁰ Políticas de Certificación.

Cualquiera sea la forma de expresar un CPS, éstos deben quedar disponibles para que cualquier usuario pueda consultarlos, de no ser esto posible se producen dudas acerca de la veracidad de la CA, por lo que sus certificados no serían confiables.

Con respecto a la información contenida en estos documentos últimamente han surgido algunas preocupaciones, ya que éstos describen muy en detalle el funcionamiento y operación de una CA, por lo que existen algunas corrientes en torno a su reemplazo por otros instrumentos menos informativos.

4.4.3 Autoridad de Registro

Aunque la Autoridad de Certificación en algunos esquemas es la última responsable por la identificación del usuario durante el proceso de certificación, la CA puede asignar estas responsabilidades a una Autoridad de Registro o RA¹²¹.

Esto se debe a que la presentación de los datos al momento de solicitar un certificado ante la CA puede ser dificultosa al estar ésta normalmente alejada de los solicitantes, además porque este proceso impide que la CA se aboque a su principal función que es la de emitir certificados, o debido a que con el tiempo una autoridad de certificación puede verse fácilmente desbordada si cubre un área geográfica muy extensa o muy poblada, por lo que esta medida acercará la CA a los usuarios, hará el proceso de certificación más expedito y aumentará la eficacia en la gestión de solicitudes.

Dentro de las tareas que puede realizar una autoridad de registro están:

- Validar solicitudes de certificados en base a procedimientos de identificación apropiados para los niveles de seguridad que esto requiere.

- Enviar las peticiones de generación de certificados a la CA para que ésta los firme con su clave privada.
- Recibir los certificados solicitados a la CA.
- Entregar los certificados a los solicitantes, ya sea de forma personal, correo electrónico, etc.
- Informar a los usuarios de la necesidad de la renovación de su certificado.
- Solicitar la revocación de un certificado a la CA.

Por ultimo, la función de RA puede ser cumplida por una organización o por una persona y sus procedimientos de verificación pueden ser incluso manuales. Las normas que utilice la RA para realizar sus operaciones deben también verse reflejadas en los CPS.

4.4.4 Repositorio de Certificados

Todas las PKI necesitan de una forma o sistema de hacer llegar los certificados a sus usuarios, éstas dependerán de la estructura misma del ambiente de la PKI y de sus políticas.

Existen múltiples formas de distribución y almacenamiento para los certificados y sus respectivas claves dentro de los cuales se destacan los disquetes, que son el medio más practico y económico de almacenamiento, sin embargo no el más confiable; las tarjetas inteligentes son los dispositivos mejor considerados para cumplir con esta tarea ya que son fácilmente transportables y seguros, claro que requieren de dispositivos lectores lo que las hace más costosas, existe también actualmente un medio de almacenamiento parecido a las tarjetas inteligentes, los

¹²¹ Registration Authority

Token USB¹²², que son sistemas criptográficos que se conectan al puerto¹²³ del mismo nombre para su lectura.

Como los certificados y las claves públicas correspondientes deben estar disponibles para todos los usuarios, un repositorio central será el lugar ideal para publicar los certificados y las CRL. Uno de los métodos más eficientes para implementar estos repositorios son los servicios de directorio, sobre todo cuando el número de certificados y listas de revocación a consultar es grande. Estos servicios consisten en una gran base de datos parecido a un directorio telefónico, en los que cada entrada de usuario contiene los certificados de los que es titular.

Estos servicios poseen también una estructura jerárquica donde se asocian atributos a los objetos que almacenan, lo que los hace distribuibles y coordinables, se rigen generalmente por el protocolo LDAP¹²⁴ el que permite a las aplicaciones localizar la información contenida en el servidor. También permite implementar esquemas más seguros de acceso a los datos que los que se pueden desarrollar sobre páginas Web u otros sistemas, además están optimizados para soportar un gran volumen de peticiones de lectura y búsqueda.

Estos servicios de directorios deben contar también con un esquema de seguridad para protegerlos contra accesos no autorizados, de forma que los usuarios puedan obtener de ellos de manera confiable los certificados que necesiten.

4.4.5 Jerarquías de Certificación

Cada certificado emitido por una CA debe estar firmado por ésta, ahora bien, las claves de una CA pueden a su vez ser certificadas por la misma CA o ser

¹²² Universal Serial Bus

¹²³ Viene incorporado en la mayoría de los PC modernos.

¹²⁴ Lightweight Directory Access Protocol.

certificadas por otra, este procedimiento puede repetirse consecutivamente con otras CA, formando una cadena de certificados¹²⁵ enlazados por una relación de confianza, que llega hasta una CA superior o raíz que se avala a sí misma.

Se podría pensar dado el esquema descrito en el párrafo anterior que utilizar muchas CA no es muy práctico y que para no complicarse verificando la autenticidad de una larga cadena de certificados sería mejor utilizar una sola y gran CA que certifique a todo el mundo.

Pues bien una sola y enorme Autoridad Certificadora no es lo más apropiado ni lo más razonable, ya que posiblemente en poco tiempo se vería desbordada por muchas solicitudes, revocaciones y renovaciones de certificados aun si se utilizan numerosas RA.

Otra de las razones del porque este esquema no es muy eficiente, es debido a que en el mundo existen muchas organizaciones con necesidades e intereses distintos de seguridad, aun dentro de estas organizaciones existen áreas con exigencias variadas, por lo que necesariamente deberán utilizar esquemas distintos. Por esta variedad de necesidades es muy difícil establecer también una política integral global, que deje conforme a todos los participantes de un entorno con múltiples intereses.

Otra de las dificultades planteadas al utilizar una única CA, es que de verse las claves de ésta comprometidas, todos los certificados que la CA haya emitido dejarían de ser confiables, lo que implicaría revocar todos éstos. La CA entonces a lo menos debería crear nuevas claves para sí y emitir nuevas claves y certificados para todos sus usuarios, lo que los obligaría a nuevamente repetir todo el proceso de registro.

¹²⁵ La que eventualmente podría ser muy larga.

Por todo esto generalmente se opta por la utilización de varias estructuras de menores dimensiones organizadas de manera principalmente jerárquica para resolver necesidades específicas, las que pueden tener diferentes políticas acerca de cómo la identidad de sus participantes es establecida y cómo los identificadores digitales son emitidos. Esto definitivamente trae nuevos desafíos al tener que planificar una estructura flexible e integrable a un entorno común.

La forma en que las CA se organizan es una característica de la PKI, existiendo distintos modelos, entre los que están:

- **Jerarquía plana.** En esta infraestructura existe sólo una CA en la que todos confían y sobre la que recae toda la responsabilidad.
- **Jerarquía de Autoridades.** En este modelo, el más extendido por cierto, una CA raíz certifica sólo a otras CA (hijas o intermedias), que a su vez pueden certificar a otras CA o a los usuarios, generalmente esta certificación es unidireccional o sea las CA hijas no certifican a CA superiores. La política de certificación en este caso es muy importante, ya que las autoridades hijas puede que sólo implementen una parte de la política de certificación de la autoridad madre. Este tipo de jerarquía es muy vulnerable puesto que todas las validaciones de certificados pasan por la CA raíz, lo que la convierte en posible objetivo de ataques
- **Jerarquía Cruzada.** Esta infraestructura es derivada de la anterior, pero donde las relaciones de confianza entre autoridades no empiezan obligatoriamente en la autoridad raíz, sino directamente entre CA que no se pueden considerarse subordinadas entre sí y que comparten algo en común como las políticas de certificación. Si bien este modelo es uno de los más sencillos, demuestra una falta de escalabilidad, ya que si sólo se permiten relaciones de confianza directas,

la cantidad de éstas es aproximada al cuadrado del número de CA. En todo caso este modelo es más seguro ya que las validaciones no pasan por un nodo central, ya que no existe una única CA raíz.

- **Sin estructura definida.** Es decir cada usuario es su propia CA y él decide en quien confiar y en quien no. Un ejemplo de autoridad sin estructura es PGP.

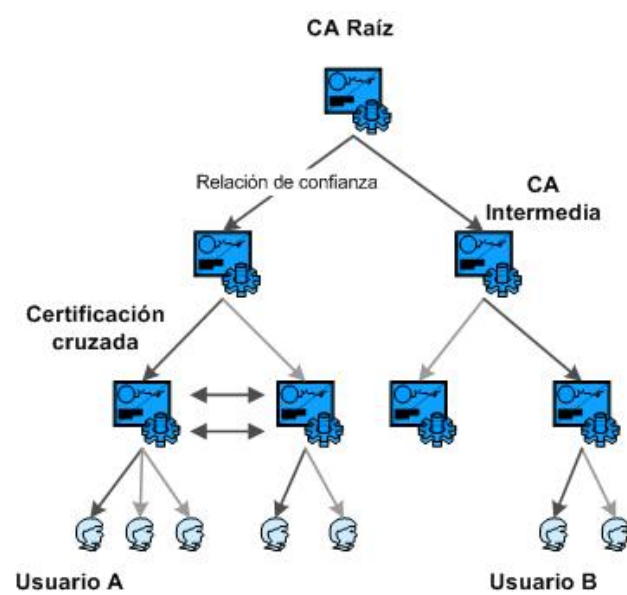


Figura 18: Jerarquía de certificación compuesta.

En general puede haber un número variable de CA entre los usuarios A y B, y para que A por ejemplo pueda validar la clave pública de B, éste debe verificar el certificado de cada CA que encuentre en el camino desde el usuario B hasta una entidad de confianza común, en este caso la CA raíz¹²⁶, este proceso se llama “validación del camino de certificación” y la longitud del camino de certificación es el número de CA entre el usuario B y la CA raíz o el número de certificados que A necesita verificar para confiar en la clave de B.

¹²⁶ En el caso que el esquema jerárquico sea unidireccional, sino deberá también verificar la ruta desde su certificado hasta la CA raíz.

La jerarquía de una infraestructura de CA es muy importante puesto que determina sus capacidades de crecimiento, utilizar varias CA mejora la escalabilidad de una PKI pero no se debe abusar ya que la longitud de los caminos de certificación deben mantenerse en un cierto rango que permita la verificación fácil y rápida de las cadenas de confianza. Lo ideal es que su longitud no exceda unos cinco certificados, ya que las aplicaciones que realicen estos procesos lo harán principalmente vía Web y al tener que validar muchos certificados verían mermado su rendimiento.

4.4.6 Estándares PKI

Las PKI deben basarse en esquemas y estándares reconocidos para poder ser aplicables de manera universal y para que sus aplicaciones sean interoperables. Estos protocolos nos permiten reconocer que es lo que significan los bits de información que se reciben desde una aplicación o que vienen en un archivo de certificados o de CRL por ejemplo, ya que ofrecen convenciones acerca de la sintaxis de los datos allí contenidos.

Para realizar sus funciones los procedimientos de distribución de certificados y CRL se basan en normas como LDAP, HTTP, FTP y X.500.

Dentro de estas especificaciones se destacan las definiciones básicas de los formatos de los objetos de una PKI mediante el protocolo X.509v3 para los certificados y CRL, así como también los estándares PKCS de RSA para los mensajes entre aplicaciones.

Otros estándares importantes son los PKIX, un conjunto de normas que permiten la interoperabilidad de las soluciones de prestación de servicios de certificación basadas en infraestructuras PKI.

4.4.6.1 X.500

El protocolo X.500, es un conjunto de estándares que definen un Servicio de Directorios, fue desarrollado por ISO y pensado originalmente para un entorno mundial. El estándar X.500 se parece mucho a una guía de teléfonos, en el que dado el nombre de una persona se puede averiguar información adicional sobre ella como localidad, organización, dirección, correo electrónico, etc.

Cada entrada del directorio X.500 tiene asignado un nombre único, que se denomina nombre distinguido o DN y para asegurarse de que este nombre permanezca único se asigna de manera jerárquica utilizando un árbol de información de directorio, en este árbol cada nodo tiene sólo un padre, excepto el nodo raíz.

A cada nodo se le asigna un nombre relativo distinguido o RDN, este nombre es único entre todos los nodos del mismo nivel, por ejemplo un computador podría tener como RDN su nombre en la red $CN^{127} = MiPC$.

El nombre distinguido completo de un nodo, se compone de todos los nombres distinguidos relativos de todos sus antepasados, Ej. $CN = MiPC$, $OU = MiUnidadOrganizativa$, $DC = MiDistrito$, $DC = MiPais$. El nodo raíz tiene una entrada para cada país los que tienen entradas para cada organización y finalmente cada organización repite esta operación para todos los elementos que desee.

4.4.6.2 LDAP

El Protocolo LDAP¹²⁸ es un estándar de comunicaciones abierto diseñado para su uso en redes TCP/IP basado en el protocolo X.500, pero que reduce la complejidad de usar éste al implementar solo algunas de sus capacidades.

¹²⁷ Common Name, identificador de objeto estándar definido por ISO.

Este protocolo define entre otras cosas: cómo un cliente de directorio puede tener acceso a un Servidor de Directorios, cómo puede realizar operaciones en el directorio y cómo puede compartir datos de éste. LDAP es un método eficiente y liviano que permite tener acceso a los servicios de directorios sin las complejidades asociadas a otros protocolos, por lo que los servidores LDAP se han convertido en el mecanismo más aceptado para almacenar certificados y CRL.

4.4.6.3 X.509

El formato o estructura de los certificados digitales de clave pública es estándar, siendo el X.509 definido por la ITU-ISO¹²⁹ el más extendido a la hora de garantizar conexiones seguras entre redes de comunicación abierta mediante certificados.

Este estándar se publicó por primera vez como parte de las recomendaciones del estándar de directorios X.500. En 1993 se revisó el estándar y se añadieron nuevos campos para soportar el control de accesos a directorios, originando la versión 2 del formato.

En la versión 3 (actualmente vigente) de X.509, los campos básicos son los mismos que en la versión 2, y los nuevos se denominan de extensión. Estas extensiones del estándar permiten una mayor flexibilidad al incluir atributos adicionales para gestionar la estructura jerárquica de las CA y la construcción de las CRL.

¹²⁸ Lightweight Directory Protocol.

¹²⁹ Organismos encargados de definir la serie de estándares sobre servicios de directorio X.500.

```

Certificate ::= SEQUENCE {
    TbsCertificate          TBSCertificate,
    SignatureAlgorithmIdentifier,
    Signature                BIT STRING
}

TBSCertificate ::= SEQUENCE {
    Version                [0]Version DEFAULT v1,
    serial number           CertificateSerialNumber,
    signature               AlgorithmIdentifier,
    issuer                  Name,
    validity                Validity,
    subject                 Name,
    subjectPublicKeyInfo    SubjectPublicKeyInfo,
    issuerUniqueID          [1]IMPLICIT UniqueIdentifier (OPT)
                           -If present, version must be v2orv3
    subjectUniqueID         [2] IMPLICIT UniqueIdentifier (OPT)
                           -If present, version must be v2orv3
    extensions              [3] Extensions OPTIONAL,
                           -If present, version must be v3
}

```

Figura 19: Formato ASN.1 certificado X.509.

El formato de los certificados x.509 v3 es el siguiente:

- **Versión:** Corresponde a la versión estándar X.509, generalmente es la 3.
- **Número de serie:** Es el número identificador del certificado, es único para cada certificado emitido por una CA determinada.
- **Algoritmo de firma:** Este campo identifica los algoritmos criptográfico utilizados para la generación de la firma digital, algoritmo de generación de claves y de resumen.
- **Fechas de inicio y fin de vigencia:** Estos campos definen el periodo de validez del certificado, generalmente corresponde a un año.
- **Propietario:** Campo con los datos que identifican al titular del certificado. Dentro de este apartado se usan una serie de abreviaturas dispuestas por el estándar X.500 para establecer la identidad del sujeto.

Código	Descripción
CN	Nombre Común
OU	Unidad Organizacional
O	Organización
L	Ciudad
S	Estado (provincia)
C	País
E	Correo Electrónico

Tabla 8: Abreviaturas para el campo identidad.

- **Emisor:** Corresponde a los datos que identifican la CA que expide el certificado, utiliza el mismo formato que el campo Propietario.
- **Clave Pública:** Representa la clave pública vinculada al titular del certificado, junto con el algoritmo que la generó y el tamaño de la clave.
- **Algoritmo de Huella Digital:** Corresponde al algoritmo con que se generó el resumen del documento.
- **Huella Digital:** Es el valor del resumen del certificado.
- **Identificador único del titular:** Este campo permite que el nombre del titular se pueda volver a utilizar en un sistema donde ya exista.
- **Identificador único del emisor:** Este campo permite que el nombre del emisor se vuelva a utilizar en un mismo sistema.
- **Extensiones:** Son la principal característica introducida por la versión 3, permite contar con información específica que puede ser definida como crítica o no. Dentro de las más importantes están:
 - **Identificador de clave de autoridad:** Permite identificar la clave pública de la autoridad certificadora que corresponde a la clave privada que ha utilizado para firmar el certificado. Esta extensión se utiliza cuando la autoridad posee varias claves para firmar.

- **Uso de las claves:** Especifica el propósito para el cual se utilizará la pareja de claves. Este puede ser firma, no repudio, cifrado de claves, cifrado de datos, firma de CRL, etc.
- **Restricción básica:** Esta extensión indica si el titular de la clave pública que aparece en el certificado es una CA.
- **Políticas de certificado:** Permite la identificación de las políticas o estamentos que rigen el uso del certificado.
- **Puntos de distribución CRL:** Especifica la localización de las CRL a utilizar para verificar el estado del certificado.

Dentro del estándar X.509 hay diferencias entre las propiedades de los campos del certificado, los que se clasifican en pertenecientes a la versión 1, campos críticos o no críticos de la versión 3 y campos modificables.

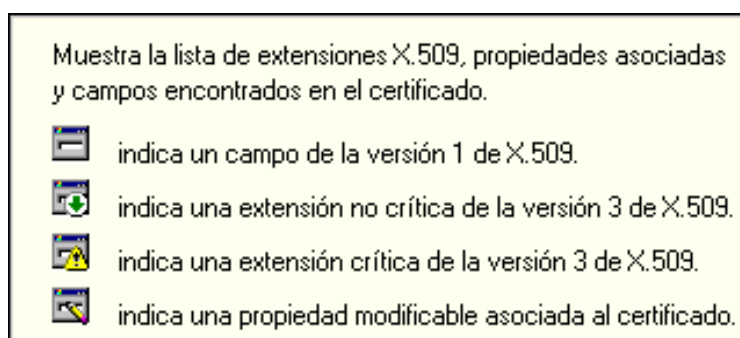


Figura 20: Propiedades campos de certificado.

El estándar X.509 establece también unas sintaxis para la Lista de Revocación de Certificados, pero no obliga a su utilización si las CA poseen otro medio de realizar la misma función, la sintaxis para las CRL actualmente es la versión 2.

```

CertificateList ::= SEQUENCE {
    tbsCertList      TBSCertList,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue    BIT STRING }

TBSCertList ::= SEQUENCE {
    version          Version OPTIONAL,
                      -- if present, shall be v2
    signature         AlgorithmIdentifier,
    issuer            Name,
    thisUpdate        Time,
    nextUpdate        Time OPTIONAL,
    revokedCertificates SEQUENCE OF SEQUENCE {
        userCertificate CertificateSerialNumber,
        revocationDate   Time,
        crlEntryExtensions Extensions OPTIONAL
                      -- if present, shall be v2
    } OPTIONAL,
    crlExtensions     [0] EXPLICIT Extensions OPTIONAL
                      -- if present, shall be v2
}

```

Figura 21: Formato ASN.1 CRL.

Para la sintaxis de las CRL el protocolo X.509 especifica:

- **Versión:** Indica la versión de la sintaxis de la CRL, si en la CRL aparecen extensiones, la versión debe ser la 2.
- **Algoritmo de firma:** Identifica el algoritmo de firma y de resumen que utiliza la CA para firmar la CRL.
- **Emisor:** Identifica la CA que ha emitido y firmado la CRL, utiliza el mismo formato x.500 de los certificados.
- **Fecha de efectividad:** Indica la fecha en que se emitió la CRL.
- **Fecha próxima actualización:** Indica la fecha en que se emitirá la próxima CRL, se puede emitir una CRL antes de esta fecha pero no es conveniente hacerlo después.
- **Certificados revocados:** Contiene la lista de los certificados que se han revocado hasta la fecha de publicación. Este campo puede aparecer vacío en el

caso en que no se hayan revocado certificados, de tener información aparece el número de serie de los certificados y la fecha en que se revocó.

- **Extensiones de certificados revocados:** Estas extensiones hacen referencia a los certificados revocados contenidos en la CRL, entregando información adicional de éstos. Entre los más importantes están.
 - **Razón de la revocación:** Indica cual fue la razón de la revocación, éstas pueden ser compromiso de la clave, compromiso de la CA, cambio de afiliación y cese de operación, entre otros.
 - **Fecha de no válido:** Indica cuando se sospecha que el certificado deja de ser válido. Un certificado puede dejar de ser válido antes de la fecha de revocación.
- **Extensiones de la CRL:** Estas extensiones dan información adicional sobre las CRL. Entre las más importantes están:
 - **Identificador de clave de autoridad:** Esta extensión permite identificar la clave pública de la CA correspondiente a la clave privada con que se firma la lista de revocación. Se utiliza cuando la autoridad posee varias claves para firmar.
 - **Número de CRL:** Contiene un número secuencial que permite a los usuarios saber el orden de emisión de las CRL, el número se incrementa en cada lista que se emite.
 - **Punto de distribución de la emisión:** Contiene una dirección que indica el punto de distribución de la CRL.

4.4.6.4 PKCS

Los estándares de clave pública producidos por los laboratorios de RSA y otras entidades, tienen el objetivo de acelerar el despliegue e interoperabilidad de la criptografía asimétrica.

Esta familia de protocolos define el formato, distribución e intercambio de las claves públicas, y permite que soluciones de diferentes fabricantes soliciten y transfieran certificados de un modo que todos se entiendan. Estos estándares actualmente se encuentran en casi todas las implementaciones de PKI existentes en el mercado.

- **PKCS #1**

Es el Estándar de Cifrado RSA¹³⁰, éste proporciona recomendaciones para la implementación de la criptografía de clave pública basada en el algoritmo RSA, cubre los aspectos de primitivas criptográficas¹³¹, esquemas de encriptación, de firma y además la sintaxis de la pareja de claves RSA.

- **PKCS #3**

Es el Estándar de Intercambio de Claves Diffie-Hellman, este estándar describe un método para la implementación de los mecanismos de intercambio de clave mediante el algoritmo Diffie-Hellman. El uso o aplicación proyectada de este protocolo era establecer comunicaciones seguras.

¹³⁰ Actualmente incluye el PKCS #2 que cubría el cifrado RSA de Hash y PKCS #4 que cubría la sintaxis de las claves RSA.

- **PKCS #5**

Es el Estándar de Criptografía Basado en Contraseñas, éste proporciona recomendaciones para la implementación de criptografía basada en contraseñas, explica como cifrar un texto mediante una clave secreta derivada de una contraseña, se puede usar para cifrar claves privadas.

- **PKCS #6**

El Estándar de Sintaxis de Extensiones de Certificado, este estándar describe la sintaxis o codificación para los certificados y sus extensiones, consiste de un certificado y un conjunto de atributos. El uso previsto de este estándar era ampliar el proceso de la certificación más allá de la publicación de la llave pública para certificar información adicional sobre el titular, está basado en una versión obsoleta de X.509 más extensiones propias¹³².

- **PKCS #7**

El Estándar de la Sintaxis de Mensaje Criptográfico, define una sintaxis general para la codificación de los datos a los que se les haya aplicado criptografía, tales como firma y cifrado digitales. La sintaxis admite recursividad y atributos arbitrarios como firma de tiempo.

El formato PKCS #7 permite transferir un certificado y todos los certificados de su ruta de certificación de un equipo a otro o a un medio extraíble. Los archivos PKCS #7 pueden utilizar varios formatos.

¹³¹ Funciones criptográficas básicas.

¹³² Cuando se publico X.509 todavía no soportaba extensiones.

- **PKCS #8**

El Estándar de Sintaxis de la Información de la Clave Privada, este estándar describe un formato para la información de la clave privada, la información de la clave privada incluye una clave privada y un conjunto de atributos.

También describe una sintaxis para las claves privadas cifradas, en las que se emplea PKCS #5.

- **PKCS #9**

El Estándar de Tipos de Atributos, define los diversos tipo de atributos usados en las extensiones de certificados, mensajes criptográficos, información de las claves privadas y solicitud de certificados definidos en los demás estándares PKCS.

- **PKCS #10**

El Estándar de Sintaxis de Solicitud de Certificados, describe la sintaxis para la solicitud de certificados, ésta consiste de un nombre distinguido, una clave pública y opcionalmente un conjunto de atributos firmados en conjunto por la entidad que solicita el certificado.

La solicitud debe ser enviada a una CA que la transforma en un certificado de clave pública X.509, la forma en que ésta devuelve el certificado está fuera del estándar, una posibilidad es un mensaje PKCS #7.

- **PKCS #11**

El Estándar de Interfaz de Criptografía en Token¹³³, éste especifica un API¹³⁴ denominada Cryptoki para dispositivos de hardware que contienen información criptográfica y realizan funciones del mismo tipo.

Define una interfaz de programación para funciones criptográficas independiente de la tecnología base del dispositivo, pero no especifica como implementar las funciones.

- **PKCS #12**

El Estándar de Sintaxis de Intercambio de Información Personal, este estándar especifica un formato para almacenar y transportar claves privadas y certificados de un usuario desde un equipo a otro. PKCS #12 es apropiado para transportar, hacer copias de seguridad y restaurar un certificado y su clave privada asociada.

- **PKCS #13**

El Estándar de Criptografía de Curva Elíptica está bajo desarrollo, éste dirige muchos aspectos de la criptografía de curva elíptica incluyendo parámetros, validación y generación de claves, firmas digitales, encriptación de clave pública y sintaxis ASN.1 para los parámetros.

- **PKCS #15**

El Estándar de Formato de Información de Token Criptográfico, es un intento por establecer un estándar el cual asegure que los usuarios puedan utilizar un mismo

¹³³ Se refiere generalmente a una tarjeta inteligente o conector similar.

¹³⁴ Interfaz de Programación de Aplicaciones.

Token en múltiples aplicaciones, actuando como un traductor entre el formato interno del dispositivo y el formato que espera la aplicación.

4.4.6.5 PKIX

El grupo de trabajo PKIX¹³⁵ definió un nuevo grupo de estándares PKI que muchos fabricantes y empresas están adoptando en lugar de los PKCS. Estos definen el formato, intercambio y distribución de claves públicas, junto con un modelo operativo para la distribución de certificados por Internet.

Son principalmente normas de gestión y administración para poder unir los diferentes componentes y servicios PKI de forma que interactúen correctamente.

PKIX define perfiles específicos para los certificados y las CRL con el objetivo de limitar la flexibilidad del estándar X.509, ya que esta flexibilidad dificulta la interoperabilidad.

4.4.6.6 OCSP

El protocolo OCSP¹³⁶ intenta dar una solución opcional al problema de verificación de revocación de certificados, se puede implementar como reemplazo o complementación de las CRL e intenta cubrir algunas de las limitaciones de éstas, ya que proporciona una validación en tiempo real de los certificados.

OCSP especifica la sintaxis de un mensaje pregunta-respuesta entre una aplicación cliente que requiere información acerca del estado de revocación de un certificado y un servidor que conozca el estado de revocación del mismo.

¹³⁵ Public Key Infrastructure X.509.

¹³⁶ On Line Certificate Status Protocol.

El esquema de funcionamiento es el siguiente:

La aplicación envía una solicitud de información del estado del certificado al servidor OCSP, el cual le envía una respuesta firmada digitalmente de bueno, revocado o desconocido.

Si el estado del certificado es bueno le indica a lo menos que el certificado no ha sido revocado de acuerdo a lo que el servidor OCSP conoce en el momento de la solicitud. Esto no necesariamente significa que el certificado esté emitido o que está dentro de su intervalo de tiempo de validez, ya que en la CRL no se publican los certificados que han terminado su vigencia.

El estado revocado indica que el certificado ha sido revocado permanentemente o de manera temporal, el estado desconocido indica que el servidor no sabe nada acerca del certificado solicitado.

4.5 Aplicaciones

En la sociedad digital actual y futura existen muchas áreas que precisan entornos de operación seguros y confiables susceptibles de funcionar en un ambiente PKI, entre éstas están:

- **Los entornos corporativos o laborales**

PKI podría apoyar los procesos de identificación de empleados, sustituyendo o complementando el esquema tradicional de identificación mediante usuario-contraseña por uno basado en Certificados Digitales.

Además ayudaría a implantar el concepto de oficina sin papeles, ya que hasta ahora los procesos informáticos todavía necesitan guardar documentación con una

serie de firmas o autorizaciones, las que podrían ser sustituida por archivos electrónicos firmados.

- **El comercio electrónico**

El intercambio de información autentica entre las partes negociadoras en un entorno Web lleva a la necesidad de establecer un nivel de protección de la información intercambiada y procesada como son pedidos, entrega de facturas, ordenes de pago, negociación y firma de contratos, entre otros. Todas estas actividades pueden ser protegidas y avaladas por una correcta implementación de PKI.

- **El trabajo a distancia**

Cuando se trabaja como parte de un equipo de teletrabajadores y dentro de un proyecto cooperativo es preciso contar con un grado de confianza en la identidad de las personas con las que se interactúa, en la autenticidad de los documentos que se intercambian e incluso en la confidencialidad de las comunicaciones, por lo que PKI puede aquí también ayudar.

- **El telediagnostico**

Los sistemas más avanzados de información medica ofrecen importantes beneficios al poder proporcionar información de carácter medico de un modo casi instantáneo.

En los sistemas actuales la información medica de los pacientes, de carácter claramente privado, se almacena en tarjetas inteligentes, por lo que un profesional de la medicina necesita confiar en la autenticidad de ella, ya que su actuar depende de

esto. Por otra parte tendrá que consultar con otros profesionales que deberán ser igualmente confiables.

- **Telebanco**

El negocio bancario necesita cada vez más acercar sus servicios al cliente y evitar la necesidad de desplazamientos a las sucursales. Para ello ya funcionan desde hace mucho las tarjetas de crédito, los cajeros automáticos, etc. Sin embargo, esto no parece ser suficiente, y se intenta llevar esos servicios hasta el mismo hogar del cliente. Esto sólo puede hacerse sobre las redes públicas actualmente existentes por lo que es absolutamente necesario incorporar soluciones que permitan asegurar las transacciones electrónicas.

4.6 Problemas de PKI

PKI no está exenta de dificultades y como toda nueva tecnología debe recorrer todavía un largo camino para lograr un alto nivel de integración y aceptación.

Los mayores obstáculos a los que se han enfrentado las empresas pioneras en la implantación de soluciones PKI para sus necesidades de negocios electrónicos han sido tradicionalmente los siguientes:

- **Falta de interoperabilidad**

Ya que el uso del estándar X.509v3 no garantiza en absoluto que dos certificados generados por sistemas desarrollados en empresas distintas sean mutuamente compatibles.

- **Costo**

Otro problema desde el principio, al no existir un mercado suficiente mente maduro de PKI, cada empresa que ofrece soluciones de clave pública posee tarifas en función de criterios diversos y cobra honorarios también dispares, de manera que la inversión en PKI puede resultar inesperadamente elevada.

- **Escalabilidad**

Cuando el número de certificados emitidos a los usuarios va en aumento, también aumenta el tamaño de las listas de revocación que deben ser consultadas cada vez que se realiza una operación que involucre certificados y firmas digitales, con lo que los tiempos de respuesta de los sistemas PKI pueden verse afectados.

- **Comprensión**

El usuario no termina por entender la tecnología, ni tan siquiera la jerarquía relacionada. Acostumbrado a autenticarse sin más que introducir un nombre de usuario y una contraseña, puede sentirse fácilmente rebasado por la complejidad de los esquemas de firmas digitales y demás funciones criptográficas. Por lo que el sistema en vez de ayudar a la gente puede que los confunda.

- **Usuarios**

Las claves de los usuarios permanecen en sus computadores los que generalmente no tienen ningún tipo de control de acceso permitiendo su uso por desconocidos o conocidos incluso, quedando de esta forma expuesta la clave privada.

La solución a esto es generalmente usar una contraseña para proteger la clave privada almacenada en estos computadores, con lo cual volvemos a generar el problema de la mala elección de la contraseña.

Basado en el mismo problema del control de acceso a los computadores de los usuarios, un extraño podría incluir en el almacén de certificados del usuario, el de una CA raíz falsa por lo que posteriormente un certificado ilegítimo podría ser considerados como veraz y por ende confiable. Incluso el extraño podría copiar cada uno de los campos de un certificado válido en otro falso -exceptuando claro la firma y la clave de éste- firmado por la CA raíz falsa con el objetivo de suplantar el certificado de otra persona, lo que para un usuario inexperto sería imperceptible.

▪ **Aplicaciones**

Muchas organizaciones que adoptan PKI ya sea porque las convencieron que era la solución mágica y definitiva al problema de la seguridad o por que detectaron la tendencia de otras organizaciones a adoptarla, se dan cuenta después de un tiempo que quieren firmar documentos, pero se encuentran con el dilema de ¿Qué firmar?, ¿Cómo firmar? Y lo más importante ¿Con qué firmar?. Esto es un problema grande en PKI, los usuarios cuentan ahora con certificados digitales pero no tiene que hacer con ellos, no existen muchas aplicaciones que utilicen PKI de forma eficiente, lo que podría resultar en que la infraestructura quede en un total abandono.

Ya se han mostrado las virtudes y defectos de la herramienta principal que se propone para mejorar las aplicaciones que se desenvuelven en entornos Internet, ahora se procederá a mostrar algunas legislaciones que avalan su utilización con lo que se concluirá la parte teórica de este trabajo, para posteriormente avocarse a la parte experimental con lo cual se espera profundizar aun más los conocimientos de esta tecnología.

5.1 Preámbulo

Las naciones históricamente han utilizado las leyes como uno de los medios de garantizar el progreso de sus actividades, entre éstas el comercio tradicional también requirió de una legislación para su regulación y desarrollo.

En la sociedad de la información y particularmente en el e-comercio las tradicionales reglas ya no son suficientes, por lo que se hace necesario la incorporación de nuevos principios que de modo sencillo organicen esta actividad.

Dentro de este ámbito, ha surgido una corriente global entorno a legislar sobre el uso de los documentos y firmas electrónicas, de la que nuestro país no ha escapado promulgando recientemente una ley respecto al tema -la que refuerza el planteamiento propuesto en este trabajo de tesis de utilizar la firma digital y PKI como solución para mejorar las condiciones de seguridad de las aplicaciones orientadas al Web-.

Debido a esto, el presente capítulo describe algunas normativas internacionales que de forma muy particular se consideraron como las más importantes en la materia, ya que algunas de ellas han sido tomadas como referentes para la definición del modelo legislativo nacional, el que por supuesto también será descrito.

5.2 Introducción

Si bien en sus comienzos Internet cimentó su desarrollo de forma libre y sin ninguna aparente regulación, hoy en día con el auge del comercio electrónico se ha hecho necesario la implementación de marcos reguladores que a través de medios legales y técnicos faciliten la realización de transacciones electrónicas, otorgando así confianza en los actos realizados a través de este medio.

Pero, ¿Por qué establecer un marco legal que fomente y facilite el uso de la firma electrónica y los documentos electrónicos?.

Una de las razones es que de nada serviría desarrollar e implementar soluciones de seguridad como la firma digital, si no hay la certidumbre para los entes que se comprometen en actos de comercio electrónico de que tales soluciones se rigen por normas que serán aplicadas en caso de conflicto.

Otra de las razones para definir una normativa en esta materia es debido al potencial que ésta presenta para apoyar el desarrollo del e-comercio, ya que al promover la confianza impulsará también el interés de las personas a participar de transacciones en este entorno, con el consecuente aprovechamiento de las oportunidades de desarrollo que este medio ofrece.

Otra razón es que las autoridades han tomado conciencia del retraso que se podría producir en las sociedades a las que sirven si no inician acciones oportunas en torno a definir un marco legal que permita la utilización de los nuevos medios tecnológicos, y mantenerse así en una situación de igualdad frente a otras naciones que ya tienen una parte del camino recorrido.

Aun más si estas innovaciones tecnológicas contribuyen a aumentar la productividad y mejorar la efectividad de los procedimientos, disminuyendo por

ejemplo costos de almacenamiento y traslado de papel al poder utilizar archivos y firmas digitales.

5.3 ¿Qué es un Documento y Firma Electrónica?

Partamos definiendo lo que no es, un documento no electrónico es aquel creado por medios manuales o mecanógrafos por consecuencia uno electrónico es aquel creado de una manera distinta a estos medios, técnicamente es un conjunto de señales o impulsos eléctricos almacenados ya sea de forma magnética u electrónica y que sólo puede ser comprendido a través de sistemas creados por el hombre que entienden este tipo de señales.

Este tipo de documentos consta generalmente de un soporte (Disquete, CD, DVD, RAM, HD), un mensaje construido basándose en un idioma, un lenguaje que corresponde a un código binario y eventualmente una firma que en este caso también es electrónica.

Por otro lado, una definición consensuada de documento electrónico, basada en distintas legislaciones podría ser la que se entiende como una expresión en lenguaje convencional que puede ser gráfica, sonora o una imagen, recogida en un soporte informático con eficacia probatoria o relevancia jurídica.

La firma electrónica por su parte no es una imagen digital de una firma manuscrita como la que está a la vista en los documentos presentados en papel, sino que su creación está basada en algoritmos computacionales y está ligada indisolublemente a cada documento firmado con una clave que es de exclusivo control del firmante, lo que hace que una firma electrónica sea distinta para cada documento al que es aplicada y permite identificar la identidad de su autor y verificar la integridad de los datos contenidos en el documento.

Para aclarar un poco más el tema, a continuación se muestran algunas definiciones encontradas en distintas normativas internacionales sobre documentos electrónicos.

- **UNCITRAL**¹³⁷: Mensaje de datos se entenderá a la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares, como pudieran ser entre otros, el intercambio electrónico de datos, el correo electrónico, el telegrama y el fax.
- **EE.UU.:** Un registro electrónico es un contrato u otro archivo creado, generado, enviado, recibido o almacenado de manera electrónica (electrónica: relacionado a la tecnología con capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas o similares).
- **México:** La información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología, se le denominará mensaje de datos.
- **Argentina:** Documento digital es la representación digital de actos con independencia del soporte utilizado.
- **Chile:** Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

Ahora que ya se tiene relativamente claro lo que es un documento electrónico, es necesario explicar algunas dificultades de éstos y que son las razones por las cuales hasta ahora no se había legislado para darles valor legal.

¹³⁷ United Nations Commission On International Trade Law.

Entre los inconvenientes de los documentos electrónicos y de la información contenida en ellos están:

- Identidad del autor de la información, es difícil identificar al autor de manera confiable.
- Integridad de la información, son fáciles de alterar sin que queden pruebas de ello.
- Confidencialidad, la información es fácil de interceptar y revelar.
- No repudio, es difícil garantizar al autor de la información.

Hasta hace algunos años no existían herramientas que pudieran resolver estos inconvenientes, pero actualmente la tecnología de firma digital, dada la madurez que se le atribuye puede garantizar a los documentos electrónicos como medios seguros y susceptibles de tener valor legal. Debido a esto, muchas naciones han considerado oportuno definir una ley que avale y fomente la utilización de esta tecnología.

Año Publicación	País
1995	▪ Ley del Estado de Utah–EE.UU.
1997	▪ Alemania, relanzada el 2001 con las normas de la UE. ▪ Italia. ▪ Comunidad Europea, Marco Comunitario de Firma Electrónica.
1999	▪ Colombia. ▪ España. ▪ EE.UU., Norma Federal,
2000	▪ Inglaterra. ▪ México. ▪ Perú. ▪ Argentina.
2001	▪ Canadá. ▪ Venezuela.
2002	▪ Chile.

Tabla 9: Cronología Leyes de Firma Digital.

Dentro de estos marcos reguladores la mayoría de los países ha discutido las normas mínimas que permitan asegurar que no se negará la existencia ni la validez legal de los documentos electrónicos ya sean cifrados o firmados.

Estas normas se han desarrollado promoviendo la adopción de principios jurídicos básicos armonizados lo más posible y basados en disposiciones internacionales como las dispuestas por la Ley Modelo de UNCITRAL¹³⁸-, pero aun así se encuentran algunas diferencias en las leyes de distintas naciones.

Evidentemente la eficacia de todas estas leyes radicará en la uniformidad de su definición, ya que si su contenido varía de forma sustancial de nación en nación, será difícil su aplicación en un entorno globalizado como es Internet, donde los negocios y las infracciones a estas leyes pueden realizarse desde cualquier territorio.

5.4 Aspectos esenciales de una Ley de Firma Digital

Antes de emplear de forma masiva cualquier herramienta nueva y sobre todo compleja se deben tomar ciertas medidas que ordenen y regulen su utilización y difusión, ya que no hay nada que desincentive más el uso de algo que el desorden y la desconfianza.

Dentro de un buen marco jurídico orientado a regular el uso de los documentos electrónicos y la firma digital, deben estar presentes -según algunos expertos- ciertos puntos importantes, como los que se describen a continuación:

- Homologar el uso y legalidad de los documentos y firmas electrónicas a sus similares en papel.
- Promover la incorporación de la tecnología en el ámbito privado y público.

¹³⁸ Comisión de Naciones Unidas para el Derecho Mercantil Internacional

- Generar políticas y leyes compatibles en el ámbito internacional para no obstaculizar la cooperación y el desarrollo económico.
- Asegurar la libre elección entre distintos sistemas que desarrollen la tecnología, ya que la imposición de una herramienta podría crear desconfianzas.
- Prevenir la mala o incorrecta utilización de esta tecnología.
- Validar la utilización de documentos y mensajes electrónicos, de las firmas digitales y entidades de certificación de claves para dichas firmas.
- Fomentar soluciones orientadas al mercado, o sea desarrolladas de acuerdo a las necesidades y demandas de los usuarios.
- Respetar los derechos fundamentales de las personas.
- Fomentar el acceso global a esta tecnología sin discriminaciones de ningún tipo.
- Establecer claramente responsabilidades y derechos de las personas que usen la tecnología.
- Fomentar otro tipo de servicios además de la expedición y gestión de los certificados digitales.

5.5 Características de las Legislaciones

Todas las normas pretenden en sus distintos cuerpos legislativos regular los nuevos servicios que se generarán a partir de la instauración de la firma electrónica, sin embargo hay algunas características que se consideran de mayor importancia y que no deben estar ausentes en una legislación.

A modo de comparación y para apreciar en que grado de compatibilidad podríamos establecer relaciones comerciales mediante esta tecnología con otros países, es que a continuación se muestra un cuadro comparativo de las principales cuestiones que deberían regular las normas legales en materia de firma electrónica y el porcentaje de legislaciones latinoamericanas que de alguna manera las mencionan.



Figura 22: Características legislaciones Latinoamericanas Fuente: CCS.

Dentro de los puntos más importantes se encuentran:

El equivalente legal de la firma electrónica a la firma tradicional o manuscrita, la que se reconoce en la totalidad de las normas.

No ocurre lo mismo con la neutralidad tecnológica (referido a que las legislaciones no estén atadas a una tecnología en particular), aunque la mayoría utiliza o se adhiere a la criptografía de clave pública lo que garantiza una cierta compatibilidad.

El tema más complicado es la homologación de los certificados emitidos por entidades extranjeras para lo que algunas legislaciones establecen la necesidad de la vigencia de un acuerdo o tratado internacional previo y el requisito de un registro de las entidades certificadoras para operar. Algunos exigen este registro y otros lo dejan a la voluntad del certificador, pero establecen diferencias entre estar inscritos y no estarlo.

En todo caso a pesar de las diferencias, existen algunos referentes muy importantes sobre los cuales se definen las leyes de documentos electrónicos y firma digital, éstos corresponden a las normas de organismos internacionales como las normas que dicta Naciones Unidas y las de las naciones pioneras en el tema, las que se consideran importantes de describir en sus aspectos más relevantes.

5.5.1 Modelo UNCITRAL

Dentro de las normativas que se toman como guía para la definición de una legislación nacional respecto al tema de firma digital, se encuentra una muy importante por lo que significa a escala mundial el organismo que la dictó.

Naciones Unidas ha producido un modelo legislativo supraestatal adaptable, que puede ser implantado de manera uniforme a las legislaciones de los distintos países, ésta fue dictada a través de la UNCITRAL o CNUDMI¹³⁹ la que ha desarrollado una estructura legal tipo o “Ley Marco” que determina los aspectos legales mínimos que debe tener una legislación sobre el tema, con el objetivo de homogeneizar las legislaciones que los países adopten y no entorpecer el desarrollo del comercio internacional.

¹³⁹ Comisión de Naciones Unidas para el Derecho Mercantil Internacional.

Esta Ley Marco nace con el propósito de resolver los problemas y conflictos relacionados con la expansión del comercio electrónico y se caracteriza por dar una solución integral y exhaustiva a este tema.

Dentro de los puntos más importantes que trata en sus artículos, están los siguientes:

- La ley se aplica a todos los casos en que se utilicen firmas digitales en actividades comerciales.
- Define conceptos como Firma Electrónica, Certificados, Firmante, Prestador de Servicios de Certificación, entre otros.
- Especifica la igualdad en el tratamiento de las tecnologías para firma electrónica, estableciendo que ninguna de las disposiciones de la ley podrá ser utilizadas para discriminar algún método de creación de firmas digitales que cumpla con los requisitos planteados en la misma ley.
- Dentro de los requisitos que plantea la ley para una firma electrónica válida o confiable están por ejemplo que los datos de creación de la firma sean exclusivos del firmante, que estos datos estaban en el momento de la firma bajo exclusivo control de éste y que sea posible detectar cualquier alteración en la firma.
- Establece que la ley debe ser interpretada en base a su origen internacional y promovida su aplicación de manera uniforme.
- En cuanto a los deberes del firmante se destacan, el actuar con diligencia para evitar que sus datos sean utilizados en forma maliciosa y que sin demora debe dar aviso a quienes pudieran confiar en la firma si los datos de creación de ésta se vieran comprometidos. Cuando se utilicen certificados digitales para corroborar

la firma digital, debe actuar con diligencia para cerciorarse de que toda la información que éstos contienen es exacta, de no cumplirse con estas disposiciones será cargo del firmante cualquier consecuencia jurídica.

- Con respecto a las responsabilidades del prestador de servicios de certificación se destacan, el actuar conforme con las declaraciones de sus normas y prácticas de certificación, cerciorarse de la exactitud de la información de sus certificados digitales, proporcionar a la parte que confía en el certificado métodos para que éste identifique la identidad del prestador de servicios y que los datos al momento de la expedición del certificado estaban bajo su exclusivo control, cerciorarse además de la validez de los datos en la fecha en que se expidió el certificado, proporcionar también medios para determinar cualquier limitación en los usos de los datos de creación de la firma o certificados, proporcionar medios para determinar si los datos de creación de la firma han sido comprometidos, proporcionar medios para determinar cualquier limitación en la responsabilidad del prestador de servicios, y medios para determinar cuales son los servicios para revocar el certificado, también se le insta a utilizar sistemas confiables al momento de prestar sus servicios, estableciéndose que serán del cargo del prestador de servicios las consecuencias del no cumplimiento de estas disposiciones.
- Para determinar si los servicios de un prestador de servicios de certificación son confiables se tendrá en cuenta por ejemplo los recursos humanos y financieros que éste emplee; La calidad de los sistemas, equipos y programas informáticos utilizados; Los procedimientos para la tramitación, solicitud y conservación de los registros de los certificados; La disponibilidad de información para los firmantes nombrados en los certificados y quienes confíen en éstos; La periodicidad y

alcance de las auditorias hechas por una entidad independiente; La existencia de una declaración por algún órgano acreditado del cumplimiento de estas disposiciones.

- En cuanto a la parte que confía en el certificado se estipula que éste será responsable por las consecuencias jurídicas de no haber verificado la validez de la firma electrónica o del certificado, y el no haber tomado en cuenta las limitaciones de éste.
- De los certificados y firmas extranjeras se establece que la determinación de los efectos jurídicos será independiente del lugar en que se halla expedido el certificado o firma digital y del lugar en que esté establecido el proveedor de servicios de certificación, y que toda firma o certificado emitido fuera del estado que promulgó la ley tendrá el mismo valor que uno emitido dentro del estado si éste posee un grado de confiabilidad equivalente, para determinar la confiabilidad de estos certificados o firmas se recurrirá a normas internacionales, y si existiere un acuerdo internacional, éste será suficiente para probar la confiabilidad de los certificados o firmas electrónicas.

Como se puede observar, la ley modelo establece normas muy generales.

5.5.2 Unión Europea

La UE por su parte, a dictado una normativa general o marco comunitario, en el que se establece un sistema común para la firma electrónica con el objetivo de regular la actividad de certificación y firma digital al interior de ésta.

Esta ley representa la tendencia actual de las legislaciones en la mayoría de los países del mundo con respecto a esta materia, las que se alejan un poco de la ley

modelo de UNCITRAL y que tienden a legislar más exhaustivamente y exclusivamente sobre los certificados y firmas digitales.

La normativa está compuesta de quince artículos y cuatro anexos en los que se establecen los objetivos del documento y sus aportes, entre sus consideraciones están:

- La comunicación y el comercio electrónico necesitan de la firma electrónica y servicios de autenticación de datos.
- La heterogeneidad en las normativas de las distintas naciones integrantes de la comunidad respecto al reconocimiento de la firma digital y organismos proveedores de servicios de certificación puede entorpecer el desarrollo del comercio electrónico.
- Un marco comunitario claro sobre firma digital impulsará el desarrollo y aceptación de las nuevas tecnologías, además la legislación de los estados miembros no debería obstaculizar el comercio al interior de la comunidad.
- Promover la interoperabilidad de los productos de firma electrónica.
- Presenta un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.
- La firma electrónica se utilizará en variadas circunstancias dando lugar a nuevos productos y servicios, los que no deben limitarse a la expedición y gestión de certificados.
- La normativa contribuye al uso y reconocimiento legal de la firma digital en la comunidad, además no define un marco reglamentario para el uso de firmas digitales dentro de un ambiente exclusivamente privado.

Dentro de los artículos del marco se puede destacar:

- El Facilitar el uso de la firma digital y contribuir a su reconocimiento jurídico.
- La Definición de conceptos como firma electrónica y firma electrónica avanzada, firmante, dispositivo de creación de firmas, certificado, proveedor de servicios de certificación, etc.
- Define los principios que deben regir con respecto al acceso al mercado por los proveedores de servicios de certificación de los miembros de la comunidad, las condiciones bajo las que operarán y como se supervisarán, entre otros.
- Especifica la aplicación de disposiciones nacionales a los proveedores y servicios que estén dentro del territorio de cada país de la comunidad.
- Establece que los estados miembros deben procurar que la firma electrónica satisfaga los requisitos jurídicos en relación con los datos electrónicos, así como la manuscrita los hace con los datos en papel y que sea admisible como prueba en procedimientos judiciales.
- Garantizar que los proveedores de servicios de certificación se harán responsables por el perjuicio causado a cualquier entidad que confíe en los certificados y sus datos; Vela también porque el proveedor de servicios de certificación consigne en el certificado los límites en cuanto a sus usos y que es responsable por cualquier daño generado por la utilización de un certificado revocado, si el proveedor no emitió información al respecto; El proveedor debe especificar también el valor límite de las transacciones para las cuales puede ser empleado el certificado y se libera de responsabilidad si el certificado es empleado para otros usos.

- De los aspectos internacionales, se velará que los certificados emitidos al público por un proveedor de un tercer país sean reconocidos como válidos siempre que el proveedor cumpla con los requisitos de la comunidad y esté acreditado por un estado miembro o que un prestador de certificación de la comunidad lo avale o que esté reconocido sobre la base de acuerdos internacionales entre la comunidad y el tercer país.
- Se vela por la protección de los datos personales y su circulación, además de que los proveedores sólo pueden recabar datos directamente del titular o por su consentimiento en la medida que sean necesarios para la emisión del certificado y que esta información no podrá utilizarse con otros fines sin la debida autorización del titular.

La directiva cuenta también con algunos anexos en los que se especifica los requisitos o contenidos de los certificados reconocidos, los requisitos a cumplir por los proveedores de servicios de certificación que emiten estos certificados reconocidos y los requerimientos de los dispositivos seguros de creación de firmas electrónicas, además de algunas recomendaciones para la verificación segura de firmas digitales.

5.5.3 EE.UU.

EE.UU. posee una reglamentación Federal a la que llama “Firmas Digitales en Actos de Comercio Nacional y Global”¹⁴⁰, que regula los actos de comercio interestatales e internacionales, estableciendo principios sobre los cuales cada estado debe dictar sus propias normas particulares.

¹⁴⁰ Existen también otras normativas sobre la materia, adoptadas por algunos de los Estados dentro del país.

El Acta establece entre otras cosas que un registro o una firma relacionado con una transacción no se le debe negar efectividad legal, validez o aplicabilidad por el sólo hecho de estar en forma electrónica y que a un contrato no puede negársele validez legal por haber utilizado en él una firma o registros electrónicos.

Con respecto a los consumidores, el Acta declara que éstos podrán establecer como válidos archivos electrónicos si cuentan con su consentimiento basados en que se les ha proporcionado claramente información respecto de los derechos u opciones de tener el archivo en otro formato que no sea el electrónico y el derecho a retirar su consentimiento.

Además se les debe informar si tal consentimiento es sólo para una transacción en particular o para todos los actos durante la relación de las partes, debe informárseles también los procedimientos para que éstos retiren su consentimiento y como pueden obtener una copia en papel de los archivos involucrados en la transacción y de los honorarios que serán cargados por tal efecto.

Previo a este consentimiento, al consumidor se le deben proporcionar los requerimientos de software y hardware para que éste tenga acceso y retenga los registros electrónicos involucrados. Si el consentimiento fuere dado electrónicamente, esto es prueba suficiente del acceso a la información en forma electrónica por parte del consumidor.

Si después del consentimiento se produce un cambio en los requerimientos de software o de hardware, creándose el riesgo que el consumidor no pueda acceder o retener los registros electrónicos, se le deberá entregar por parte de la persona proveedora de los registros los nuevos requerimientos y el derecho a retirar su consentimiento sin la imposición de ningún cargo o condición.

Esta ley también establece que las comunicaciones orales o grabaciones de éstas, no califican como expedientes electrónicos a menos que esté así expreso en una ley.

En tanto que si alguna ley o regulación requiere que un contrato u otro documento relacionado a una transacción sea retenido o almacenado, esto es resuelto reteniendo un registro electrónico del contrato, que refleje los datos dispuestos en dicho contrato y que esté disponible a toda persona que tenga facultad de acceder a éste de forma que se tenga capacidad de reproducirlo, de no ser así la validez legal de tal registro puede ser negado.

A su vez la ley reconoce a la firma digital mediante un artículo que establece que si una ley requiere que una firma o registro relacionado a una transacción sea notariado y reconocido, esta solicitud será satisfecha si la firma digital de la persona autorizada para realizar estos actos es lógicamente asociada con el registro.

También declara sobre el uso de agentes electrónicos y que las acciones realizadas por ellos como creación y envío de información, no cancelaran la validez legal de los archivos siempre que dichas acciones sean legalmente atribuibles a la persona a la que estos agentes están ligadas.

Con respecto a la influencia de este Acto en las normas locales de los Estados del país, especifica que un estatuto de estado sólo podrá modificar o remplazar la ley Federal con respecto a la ley del estado si constituye un ajuste o especifica procedimientos alternativos para el uso de registros electrónicos o firmas electrónicas y si tales procedimientos no requieren mayores efectos legales ni alguna tecnología particular.

Se especifica también algunas excepciones, como que la ley no se aplicará a un contrato u otro registro si éste es gobernado por un estatuto de carácter testamentaria o por leyes de familia como adopción o divorcio, por ordenes judiciales o en avisos de cancelación de servicios generales, de desalojo, de cancelación de seguros médicos o de vida, o cualquier documento requerido para el manejo de materiales peligrosos.

Se establece dentro de esta ley la existencia de organismos reguladores federales y estatales los que podrán emitir regulaciones sólo si son compatibles con la ley, si éstas no agregan mayores requerimientos a los ya planteados y no imponen costos irracionales sobre la aceptación y uso de registros electrónicos. Además de no requerir una normativa legal mayor a la existente, ni la aplicación de una tecnología específica para crear, almacenar o comunicar archivos electrónicos o firmas.

Dentro de las definiciones más significativas que se pueden encontrar en la normativa norteamericana se encuentran “Electrónico” que se refiere a capacidades eléctricas, digitales, magnéticas, ópticas o similares; “Agente electrónico” referido a un programa computacional u otra manera automatizada de realizar acciones sin la supervisión de un individuo; “Registro electrónico” se refiere a un registro generado, enviado o almacenado de una manera electrónica; “Firma electrónica” es un sonido, símbolo o proceso electrónico lógicamente asociado con un registro y ejecutado por una persona con el intento de firmar un archivo; “Información” se refiere a texto, datos, imágenes bases de datos o similares; “Archivo” es una información que es inscrita en un medio tangible, susceptible de ser almacenado en un medio electrónico u otro y que es recuperable.

La ley establece también un título para los “Registros transferibles”, en el cual lo define como un registro electrónico que (de acuerdo al Código Comercial Uniforme) es entregado a otra persona con el objetivo de darle el derecho de hacer cumplir tal documento (siempre que sea transferido de manera completa). También define “Control” de un registro transferible por parte de un ente si un sistema empleado para evidenciar esto establece que la persona a la cual se le quiere comprobar o atribuir el control de un documento, es realmente la persona quien emitió o transfirió el registro.

Por otro lado una persona tiene el “Control” de un registro transferible si tal registro es creado o almacenado de tal manera que una única copia del archivo existe y esta copia identifica a la persona que tiene el control y ésta es mantenida y controlada por dicha persona, además las copias y cambios no autorizados son fácilmente identificables.

Por último la ley establece la promoción al comercio electrónico y la firma digital además de instar a realizar todas las acciones necesarias para eliminar o reducir los impedimentos al comercio electrónico con el fin de facilitar su desarrollo entre los estados y el extranjero. También insta a remover los obstáculos basados en papel a las transacciones electrónicas, el permitir que las partes en una transacción determinen la tecnología apropiada de autenticación para sus transacciones, además de darles la oportunidad de probar que dichas tecnologías son válidas ante una corte o tribunal.

5.5.4 España

Se incluye la ley española por la importancia que siempre a tenido esta nación para la mayoría de los países de América, principalmente por cuestiones de historia

e idioma, lo que la transforma siempre en un nexo importante con las actividades Europeas.

España establece en su real decreto de ley, la adopción de una posición común respecto del proyecto de firma electrónica de la Comunidad Europea y que sus disposiciones permitirán al sector empresarial prestar servicios de certificación de calidad, al mismo tiempo que dan a los usuarios de estos sistemas la confianza necesaria, permitiendo su utilización y rápida difusión.

Establece así mismo sistemas de acreditación voluntarios para los prestadores de servicios de certificación y un registro de éstos en su ministerio de justicia.

En general establece en su primer título, el ámbito de aplicación de la ordenanza, que corresponde a la regulación del uso de la firma digital, el reconocimiento de la eficacia jurídica de ésta y la regulación de las empresas prestadoras de servicios de certificación.

Como la mayoría de las leyes también especifica algunas definiciones como por ejemplo firma electrónica y firma electrónica avanzada que corresponden a un dato electrónico anexo a un documento también electrónico, que permite la identificación del autor. La diferencia radica en que en la firma avanzada, los datos proporcionado para crear esta información anexa, son de exclusiva propiedad y control del autor, lo que vincula la firma únicamente a él.

Otra definición interesante es la de certificado y certificado reconocido, el primero es la certificación electrónica que vincula algunos datos de verificación de una firma con un signatario, determinando su identidad y el segundo es aquel que cumple con ciertos datos mínimos declarados en su contenido y que es emitido por

un prestador de servicios de certificación que cumple con ciertos requisitos también claramente especificados dentro de la ley.

El decreto regula de igual manera la prestación de los servicios de certificación, y establece un régimen de libre competencia, transparencia y no discriminación. También establece la utilización de la firma digital por entidades públicas y en la relación que éstas tengan con particulares, con la correspondiente subordinación a otras condiciones que serán dictadas por el ministerio de administración pública.

Con respecto a los sistemas de acreditación de los prestadores de servicios, se dispone que el gobierno podrá establecer sistemas voluntarios de acreditación, respecto de las normas que regulen estos sistemas, éstas deben ser planteadas con objetivos razonables y no discriminatorios.

Los organismos encargados de la acreditación valorarán informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que soliciten acreditación, y sólo serán entidades de evaluación las acreditadas por un organismo independiente al que se le haya atribuido tal facultad.

Se dispone también la creación de un registro con carácter público de prestadores de servicios de certificación, al que todas aquellas empresas que deseen prestar este tipo de servicios deben solicitar la inscripción previo al inicio de actividades, con el correspondiente aporte de documentación y el cumplimiento de los requisitos establecidos reglamentariamente, este registro por supuesto deberá ser actualizado de forma permanente.

Con respecto a los Certificados Reconocidos, la ley establece que éstos deben contener entre otros:

- La indicación que se expiden como certificados reconocidos.
- Los datos de identificación del prestador de servicios como su nombre, domicilio, correo, número de identificación fiscal, datos de identificación de su registro.
- La firma electrónica avanzada del prestador.
- La identificación del signatario compuesto del nombre y apellido o un seudónimo, y cualquier otro dato significativo. Previo y expreso consentimiento del titular.
- El comienzo y fin del periodo de validez del certificado, en el caso de los reconocidos no debe superar los cuatro años.
- Los límites del uso del certificado y el límite del valor de transacciones en que se vea involucrado.

Con respecto a la vigencia de los certificados, éstos quedan sin efecto de ocurrir cualquiera de los siguientes acontecimientos:

- Expiración del periodo de validez.
- Revocación por el signatario, por la persona representada por éste o un tercero autorizado.
- Por la utilización indebida del certificado a cuenta de un tercero.
- Una resolución judicial.
- Fallecimiento del signatario o representado, por incapacidad de cualquiera de ellos y por el término de la representación.

- Inexactitud grave de los datos.
- Cese de actividad del prestador de servicios, salvo que los certificados sean transferidos a otro prestador de servicios previa autorización del titular.

La pérdida de eficacia de los certificados en el supuesto caso de expiración del periodo de validez o cese de actividad del prestador del servicio tendrá lugar desde el momento en que se produjeron los hechos, en los demás casos tendrá efecto la extinción del certificado desde la fecha en que el prestador tenga conocimiento de los sucesos. En cualquiera de los anteriores sucesos el proveedor de servicios deberá publicar la extinción del certificado y responderá por cualquier daño por el retraso en tal publicación.

En lo que se refiere a los certificados emitidos por prestadores de servicios establecidos fuera de la Comunidad Europea, éstos serán considerados equivalentes si el prestador reúne cualquiera de las condiciones establecidas en el marco comunitario de la UE.

La ley establece asimismo las exigencias para los prestadores de servicios, creando una diferencia entre prestadores de servicios y los prestadores de servicios de certificados reconocidos, las obligaciones son entre otras el comprobar la identidad de los solicitantes de certificados; Poner a disposición del signatario dispositivos de creación y verificación de firmas; No almacenar ni copiar los datos con los que se crea la firma de quienes hayan contratado el servicio si éste no lo solicita; Debe informar de los precios del servicio, las condiciones y limitaciones antes de la emisión del certificado; Debe de igual modo mantener un registro de certificados emitidos y las circunstancias de la suspensión o pérdida de vigencia que quedará a disposición de quien quiera consultarlos; Al cesar sus actividades, debe indicarlo a sus clientes con dos meses de antelación.

Para los prestadores que emitan certificados reconocidos se agregan obligaciones como, indicar fecha y hora de la expedición del certificado o en la que quedo sin efecto; Debe demostrar la fiabilidad de sus servicios y garantizar la rapidez y seguridad en la prestación de éstos; Debe Emplear personal calificado y con experiencia, utilizar productos y sistemas fiables que garanticen la seguridad técnica de los procesos; Tomar medidas en contra de la falsificación de los certificados y garantizar su confidencialidad; Deben también disponer de recursos económicos para afrontar su actividad y los riesgos de posibles perjuicios o daños; Conservar registrada toda información y documentación referente a los certificados reconocidos durante quince años.

En cuanto a la responsabilidad de los prestadores de servicios establece que, éstos responderán por daños y perjuicios que causen a cualquier persona al ejercer su actividad debido al no cumplimiento de las obligaciones planteadas en la ley o por negligencia en su actuación; Las respuestas por los daños tomarán efecto sólo por uso indebido de un certificado reconocido cuando no se haya consignado en él de forma clara los límites de uso y el valor de las transacciones que pueden ser realizadas con éste.

También define el ente controlador del cumplimiento por parte de los prestadores de servicios de las obligaciones establecidas en la ley y que éste actuará a pedido de organizaciones administrativas o personas interesadas en tal acción. Se compromete también a los prestadores de servicios a entregar su colaboración en los procesos de inspección.

Con respecto a las firmas, éstas deben ser construidas mediante dispositivos seguros y para que un dispositivo tenga esta característica se exige que garantice que los datos utilizados para la generación de la firma puedan producirse sólo una

vez; Deben proporcionar seguridad razonable de que estos datos no pueden ser derivados de los datos de verificación o de la propia firma y que ésta no pueda ser falsificada; Además debe asegurar que los datos de creación de la firma pueden ser protegidos por el signatario contra la utilización por otros y que estos dispositivos no alteren los datos o documentos que deban firmar, ni que impidan que éstos se muestren al signatario antes del proceso de firma.

Con respecto a los dispositivos de verificación de firma, éstos deben cumplir con garantizar que la firma se verifica de forma confiable; Que puede establecer el contenido de los datos firmados y detectar su modificación; Que representa correctamente la identidad del signatario; Que verifica de forma confiable el certificado y que puede detectar cualquier cambio relativo a su seguridad.

Dentro de sus artículos esta ley también establece una clasificación de las infracciones, las que pueden ser muy graves, graves y leves. Dentro de las muy graves se destacan las relacionadas con el incumplimiento de las obligaciones establecidas en la ley por los prestadores de servicios que emitan certificados reconocidos.

Se cae en una infracción grave por ejemplo, si un prestador de servicios de certificación no reconocidos incumple las obligaciones establecidas en la ley para él y por este hecho causa daños o perjuicios a los usuarios o terceros; También se caen en este tipo de infracciones si se resiste a la inspección de los órganos facultados para esto y por la no comunicación del cese de actividades o la iniciación de éstas a los organismos correspondientes.

Como se puede observar esta ley establece una regulación muy exhaustiva respecto al tema.

5.5.5 Argentina

Una de las naciones más activas en el desarrollo de infraestructuras de firma digital en el ámbito latinoamericano es Argentina, por esto también se ha considerado importante revisar su legislación al momento de explorar los avances en el tema.

Su ley está definida en once capítulos y un anexo, y establece en su Capítulo de consideraciones generales, definiciones en relación a su alcance, validez y presunciones legales como autoría e integridad sobre la firma digital, entre las más importantes están:

Se reconoce la firma digital y la firma electrónica y su eficacia jurídica, la diferencia entre estas definiciones radica en que la firma electrónica carece de los requisitos legales para considerarse como firma digital, por su parte la firma digital es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo control del firmante, y que a través de ésta un tercero debe poder identificar a su autor y cualquier alteración en el documento, posterior a su firma.

De igual modo establece que cuando la ley requiera una firma manuscrita, esto podrá ser satisfecho por una firma digital, además una firma digital es válida si cumple con ser creada durante la vigencia del certificado digital del firmante, emitido por un certificador licenciado y la que es verificada por referencia a los datos indicados en este certificado.

En el Capítulo II están contenidas las disposiciones referentes a los certificados digitales, entendiéndose por tales a los documentos digitales firmados por un certificador que vincula los datos contenidos en él con su titular; Establece

asimismo que serán válidos si son emitidos por un certificador licenciado y si responden a los formatos estándares fijados por la autoridad como son:

- Contener la identificación de su titular y del certificador, periodo de vigencia y datos de identificación únicos.
- Contener una diferenciación entre la información verificada y la que no lo está.
- Contener información para la verificación de la firma.
- Contener una identificación de la política de certificación del prestador del servicio.

De igual forma establece que la fecha de vencimiento de este certificado no debe ser superior a la fecha de vencimiento del certificado del certificador; Las condiciones por las cuales serán válidos certificados emitidos por certificadores extranjeros como son satisfacer las condiciones de la ley además de estar vigente un acuerdo recíproco con la nación de origen del certificador extranjero o ser reconocido por un certificador nacional.

En su capítulo III, establece las funciones y obligaciones de los certificadores licenciados, a los que define como aquella persona que expide certificados y servicios en relación con la firma digital y que cuenta con licencia otorgada por el organismo licenciante.

Un artículo se distingue a los de otras leyes en el sentido que permite a entidades que controlan la prestación de servicios profesionales emitir certificados relacionados con esta función, las que deberán cumplir con los requisitos de certificador licenciado.

Dentro de las funciones más relevantes de los certificadores están: Recibir solicitudes de certificados firmadas; Emitir certificados de acuerdo a sus políticas; Mantener copias de los certificados y solicitudes; Revocar certificados a petición del titular, si se determina que el certificado se emitió en base a información falsa, o que sus procedimientos ya no son seguros; También especifica que deben ser publicados los certificados emitidos y revocados.

Las obligaciones de estos entes por otro lado son, por ejemplo:

- Informar las condiciones de utilización del certificado de forma comprensible.
- Mantener bajo control la protección de los datos.
- No exigir los datos de creación de la firma a los titulares.
- Utilizar sistema confiables, personal calificado y recursos suficientes para prestar sus servicios.
- Permitir el ingreso de funcionarios autorizados a su local operativo.

En el Capítulo IV por otra parte, establece los derechos y deberes de los titulares de los certificados, entre los que destacan, el derecho a:

- Ser informados de condiciones, características y valores de los servicios prestados.
- La protección de su información.
- Se les proporcione sólo los servicios pactados y a no recibir publicidad comercial por el certificador.

Algunas de sus obligaciones son:

- Mantener la seguridad y control de sus datos.
- Utilizar dispositivos de creación de firma confiables.
- Solicitar la revocación del certificado al certificador si se han comprometido los datos de creación de éste.
- Informar de cambios en los datos del certificado al certificador, entre otros.

En los capítulos siguientes se detalla la organización institucional estableciendo el diseño de un sistema de auditoria para evaluar la confidencialidad y calidad de los sistemas utilizados y una comisión asesora para la infraestructura de firma digital; Las funciones y obligaciones de la autoridad de aplicación; Condiciones de funcionamiento para los sistemas de auditoria y los detalles de la comisión asesora para una infraestructura de firma digital.

En el capítulo IX declara las responsabilidades del certificador por los daños causados debido al no cumplimiento de la ley y las excepciones por las que éstos no se harán responsables.

En sus últimos capítulos el X y XI establece las sanciones como multas o caducidad de servicios y algunas disposiciones completarías. Y por último el anexo correspondiente a los procedimientos de verificación de la firma digital y algunas definiciones.

5.6 La Normativa Legal en Chile

Nuestro país también ha considerado necesario el desarrollo de normas legislativas que avalen el uso de esta nueva tecnología, esto para no mantenerse al margen de los avances en e-comercio y no desaprovechar oportunidades de crecimiento por la pérdida de ventajas y competitividad como nación.

Nuestra ley está basada o inspirada sobre las disposiciones de la ley modelo de UNCITRAL, la normativa Europea y otras leyes más recientes como la Alemana, Italiana y Argentina.

La “Ley Sobre Documentos Electrónicos, Firma Digital y Servicios de Certificación de Dicha Firma”, establece el marco legal por el cual el estado de Chile avala esta tecnología.

Esta ley está compuesta de 25 artículos y en su primer título establece disposiciones generales como el ámbito de aplicación, el que está orientado a la regulación de la utilización de los documentos electrónicos en conjunto con las firmas digitales y los efectos legales de esto, además de la regulación de la prestación de servicios de certificación y procedimientos de acreditación, de la misma manera presenta una variedad de definiciones, dentro de las que se destacan por ejemplo:

- **Electrónico:** Característica de la tecnología con capacidades eléctricas, digital, magnética, inalámbrica o similares.
- **Certificado de firma electrónica:** Certificado electrónico que da fe del vínculo entre un firmante y datos de creación de la firma.

- **Documento electrónico:** Es la representación de un hecho, imagen o idea; creado, enviado o recibido de manera electrónica y almacenado de la misma forma.
- **Firma electrónica:** he aquí una diferencia entre dos tipos de firma una “normal” y otra “avanzada”, la primera es cualquier sonido, símbolo o proceso electrónico que permite al receptor de un documento identificar a su autor, la segunda es aquella certificada por un prestador de servicios de certificación acreditado, que vincula a los datos referidos en la firma únicamente a su autor, permitiendo la identificación de la modificación de ésta e impidiendo el desconocimiento de su autoría.

Igualmente establece que los actos o contratos realizados electrónicamente serán válidos de la misma manera que los celebrados por escrito o en soporte papel, con la excepción de aquellos actos cuya solemnidad no se pueda cumplir mediante documentos electrónicos, en los que es necesario la concurrencia personal y los referidos a los actos de familia; Con respecto a la firma electrónica, ésta tiene validez legal igual a la firma manuscrita.

El título segundo por su parte establece la regulación de la utilización de firmas y documentos electrónicos para los órganos del Estado. En el que se establece que éste también podrá utilizar la firma electrónica para realizar cualquier tipo de actos o contactos y que éstos tendrán la misma validez legal que los realizados por medios escritos, eso sí para tener el carácter de instrumento público deben ser suscritos mediante firma digital avanzada. Las excepciones son de igual forma que la solemnidad de los actos no lo permita o sea necesaria la concurrencia de la autoridad.

En relación con los actos entre privados y el Estado, éstos también podrán utilizar firma digital si los procedimientos son compatibles.

La certificación de las firmas electrónicas avanzadas de los funcionarios del Estado o de sus organismos se realizará a través de ministros de fe, que de no existir, se indicará a un funcionario para tales efectos, como alternativa se podrá contratar servicios de certificación con entidades acreditadas para esto.

El Título III se refiere a los prestadores de servicios de certificación, y serán considerados como tales las personas jurídicas nacionales o extranjeras, públicas o privadas que otorguen certificados de manera electrónica y serán prestadores acreditados los mismos, que tengan domicilio en Chile.

En cuanto a sus obligaciones se destacan, el contar con reglas sobre prácticas de certificación claras y objetivas, además de la obligación de comunicarlas a los usuarios en castellano. También debe tener un registro de certificados con acceso público, en el que debe quedar constancia de los certificados emitidos y los sin efecto.

En el caso del cese de actividades se debe comunicar de tal hecho a los usuarios o titulares de las firmas dando la posibilidad de transferir los datos de éstos a otro prestador acreditado, previa aprobación del titular. Se le obliga también a verificar la identidad del solicitante o de su representante para lo cual se requerirá su presencia en el caso de otorgarle una firma digital avanzada.

En cuanto a las responsabilidades, los daños que se ocasionen por la certificación serán de responsabilidad de los prestadores de servicios y corresponde a éstos demostrar que se actuó de una manera adecuada y sin negligencia, ahora si los certificados son usados de manera indebida, por ejemplo sobrepasando los

límites indicados para su uso, los prestadores no tendrán responsabilidad alguna. El Estado por su parte no se hará responsable por daño alguno causado por un prestador privado acreditado. Además los prestadores deberán contratar un seguro que cubra los eventuales daños causado por su responsabilidad.

Con relación a la información de los certificados digitales, en el título IV se menciona que éstos deben contener:

- Un código único que los identifique.
- La identificación del prestador de servicios, nombre o razón social, rol único tributario, dirección de correo electrónico, antecedentes de su acreditación y la firma electrónica avanzada de éste.
- Los datos de la identidad del titular como son su nombre, correo electrónico y rol.
- Los plazos de vigencia del certificado, etc.

Con respecto a los orígenes de los certificados de firma avanzada, éstos pueden ser también emitidos por prestadores no establecidos en Chile y serán equivalentes a los emitidos por prestadores del país siempre que sean homologados por éstos y siempre que cumplan con la ley vigente, de otra manera serán equivalentes si son respaldados por algún tratado internacional ratificado.

Estos certificados, tanto nacionales como extranjeros, quedarán sin vigencia ya sea por la expiración de los plazos de validez, el que no debe exceder los tres años; Por revocación por parte del prestador de servicios ya sea por solicitud del titular, su fallecimiento, resolución judicial o incumplimiento de las obligaciones por parte de los usuarios; Por la cancelación de la acreditación del prestador de servicios

o el cese de actividades de éste y siempre que no realice un traspaso autorizado de los datos a otro prestador de servicios acreditado.

El título V se refiera a la acreditación de los prestadores de servicios de certificación y por ejemplo establece que la acreditación es el procedimiento por el cual se verifica que un prestador de servicios cuenta con las condiciones e instalaciones necesarias para poder prestar estos servicios.

Dentro de las obligaciones con las que deben cumplir los prestadores de servicios están: El de demostrar la fiabilidad de sus servicios, sistemas y productos; Garantizar la existencia de un servicio de consulta de certificados emitidos; Utilizar personal especializado para llevar acabo la actividad de certificación y haber contratado un seguro para cubrir las eventuales responsabilidades por daños debidos a la realización de las actividades de certificación.

Con respecto a la acreditación del prestador de servicios, ésta se perderá a solicitud del prestador, si se disipan las condiciones que sirvieron para obtener dicha acreditación o por el incumplimiento de las obligaciones que establece la ley.

Finalmente, la entidad acreditadora velará por el cumplimiento de las obligaciones planteadas en la ley y podrá requerir la información necesaria para tales efectos a los prestadores de servicios, garantizando la confidencialidad de dichos datos.

Los derechos y obligaciones de los usuarios se resguardan en el título VI, donde se establece el derecho de los usuarios a ser informados de los costos de los procesos de certificación y medios de pago, así como de las prácticas y políticas del prestador de servicios; También tienen derecho a que sus datos se mantengan resguardados; Derecho a ser informados con anterioridad del cese de actividades del

prestador de servicios, esto para hacer valer el derecho a que sus datos sean trasladados a otro prestador si el titular lo requiere; El derecho a que su información no sea utilizada para que el prestador le proporcione más servicios de los pactados y el derecho a ser indemnizado.

Asimismo, los usuarios están obligados a proporcionar información exacta de sus datos y resguardar la seguridad de los sistemas proporcionados por el certificador.

Para la elaboración de esta ley entonces se ha tenido en cuenta los principios de: Neutralidad tecnológica demostrada por la no discriminación de distintas tecnologías ya que la norma es aplicable a cualquier entorno tecnológico; De homologación de las versiones electrónicas de firmas y documentos a sus equivalentes en papel, siguiendo así la tendencia internacional de evitar la existencia de marcos reguladores paralelos, uno para los actos electrónicos y otro para los basados en papel; Establece también la aplicación de las normas a todo tipo de actos tanto del sector público como del privado; Esta ley concuerda también con el contexto legislativo y tecnológico global, respaldando los acuerdos firmados por Chile, lo que le permite una inserción menos complicada en el comercio electrónico mundial.

Algunas consideraciones respecto a la ley son que no quedan claramente establecidos referentes respecto del tiempo y lugar en que se celebran los contratos, el concepto de documentos electrónicos originales y mensaje de datos, ni de la conservación de éstos, los que aparecen en algunas de las legislaciones revisadas.

Otra cosa que no se define claramente es que acciones aplicar en caso de un conflicto entre partes que se encuentren bajo normativas distintas, dado la globalidad del comercio electrónico.

6.1 Preámbulo

Después de haber analizado y madurado las características principales y las bases sobre las que se desempeña la tecnología de la firma digital y las infraestructuras de claves públicas, se está en condiciones de comenzar a demostrar de forma práctica la solución propuesta al problema planteado al principio de esta memoria.

Por esto, en el presente capítulo se desarrollará como tema central la definición de una metodología para la implantación de una PKI en una organización cualquiera. Para esto se presentarán algunos pasos fundamentales que se refieren principalmente a la definición de los requerimientos, el diseño de una arquitectura PKI, consideraciones operacionales y las características que deben tener los certificados y políticas de certificación.

Esta guía no pretende ser una pauta estricta acerca de los pasos o decisiones a tomar para la implantación de una solución PKI, sino ser sólo una guía en la cual apoyarse para hacer el proceso más sencillo y en la que se pueden incluir otros puntos dependiendo de las necesidades de cada organización.

6.2 Introducción

Para conducir un negocio de forma efectiva, las organizaciones deben confiar tanto en sus empleados como en sus consumidores y socios de negocios. La confianza interna implica la seguridad de las comunicaciones entre los empleados,

la confianza externa por otro lado involucra una certeza similar acerca de las comunicaciones con los clientes y socios.

Los servicios de una PKI utilizados correctamente son una excelente manera mediante la cual las organizaciones pueden asegurar ambos tipos de confianzas. Sin embargo establecer una PKI en una organización no es un proceso fácil como se podría pensar, ya que no basta con instalar una única aplicación y comenzar a disfrutar de la seguridad que ésta proporciona, tampoco se trata de tener una CA que emita certificados como una fabrica automatizada, eso claro si se habla de una PKI confiable y seria.

Desplegar un sistema de seguridad operacional no es simple, son múltiples las actividades a realizar antes de poder implementar un esquema de infraestructura de claves públicas. Es por esto, que se necesita una guía estructurada para ayudar a manejar, implementar y desplegar un sistema de seguridad robusto.

Se hace necesario entonces definir una pauta con etapas o pasos para dirigir la administración completa de la implantación de un sistema PKI. Esta pauta debe ser un apoyo a los aspectos técnicos, administrativos, operacionales y de soporte, además no debe descuidar tampoco los temas legales. Por esto se pueden ver involucradas muchas personas con distintas funciones dentro de la organización.

6.3 Planificación de la PKI

Planificar y desplegar una PKI que pueda satisfacer todos los requerimientos de seguridad de una organización no es fácil. Por esto, se necesita de una guía para la administración de la puesta en marcha del sistema de seguridad, desde la justificación del uso de PKI por la organización, al despliegue operacional, su mantenimiento y la integración de nuevos elementos.

Por consiguiente una metodología bien estructurada puede evitar muchos potenciales peligros, por lo que los riesgos se reducen y aquellos que permanecen son cuantificados en etapas más tempranas, adicionalmente esto permite reducir los costos y los esfuerzos involucrados al tener claro los servicios que son necesarios implementar y mantener.

Para implementar una PKI se presentan los siguientes pasos tentativos:

- I **Requerimientos.** El primer paso para implementar una solución PKI es entender y definir los requerimientos: ¿Qué es lo que dirige a la organización?, ¿Qué problemas de seguridad se intenta resolver?, ¿Cuáles son las necesidades de seguridad prioritarias por parte de las aplicaciones y los usuarios?, ¿Cuál es el grado requerido de mejoramiento de seguridad?, ¿Qué nivel de seguridad es el apropiado?, ¿Dónde están las debilidades del negocio?, ¿Cuáles son las restricciones legales y administrativas a cumplir?, ¿Dónde están localizados los usuarios?. No se debería intentar crear una PKI hasta no tener claros todos los requerimientos de seguridad.
- II **Arquitectura.** Una vez conocidos los requerimientos, el próximo paso es producir el modelo estructural y diseñar la arquitectura de confianza de la PKI. Esto implica determinar: ¿Cuántas CA son necesarias?, ¿Dónde se localizarán?, ¿Cómo serán manejadas?, ¿Cuál será la relación de confianza entre ellas?, ¿Habrà interoperabilidad entre CA internas y de terceros?, ¿Cuántas RA serán necesarias y que áreas cubrirán?, ¿Qué tipo de repositorios se utilizará y de que manera se integran a la CA y demás componentes?.
- III **Configuración Certificados.** Esta etapa incluye decidir: ¿Qué tipos de certificados serán usados?, ¿Se pueden emitir por lotes?, ¿Qué tan fuertes

deben ser las claves asociadas con los certificados?, ¿Cuál es el tiempo de validez adecuado y si los certificados serán renovables?. Adicionalmente este paso puede definir el uso de tarjetas inteligentes y otras opciones de almacenamiento.

- IV **Operaciones.** En esta etapa se definen los procedimientos operativos y controles necesarios para asegurar que los sistemas de seguridad de la PKI son efectivos. Los estamentos de prácticas de certificación y las políticas de certificados son parte integral de un sistema PKI, éstos proporcionan la base de la confianza y forman parte de las relaciones contractuales. Podría ser necesario construir plantillas de CPS para cada nivel en una jerarquía PKI o documentos enfocados para un público específico. En esta etapa se define también el plan de administración de certificados, lo que implica definir: ¿Cómo las solicitudes de los certificados son procesadas?, ¿Cómo los certificados son emitidos a los usuarios finales?, ¿Cómo las listas de revocación son manejadas y distribuidas? y ¿Qué estrategias se usarán para la recuperación de claves?, entre otras varias cosas.
- V **Despliegue.** Esta etapa involucra la instalación y validación de la PKI operacional y la aceptación de las pruebas realizadas. Una revisión del sistema se debe incluir para asegurar que la actual implementación mantiene todos los requerimientos planteados. La documentación de la PKI es finalizada y publicada en un lugar apropiado para completar el modelo de confianza. El plan de despliegue es seguido por la utilización de aplicaciones PKI por parte de los usuarios. Finalmente, todos los sistemas son susceptibles de cambios y una PKI no es la excepción. Se puede actualizar el sistema, mejorar el hardware y desarrollar nuevas aplicaciones. En todo caso cualquiera de estas

acciones requiere un manejo cuidadoso. Por tanto la revisión de la interoperabilidad de los nuevos elementos es clave, por lo que es necesario un eventual plan de migración.



Figura 23: Visión general metodología implantación PKI.

6.4 Requerimientos

El primer paso en la implementación de una solución de seguridad basada en PKI es entender los requerimientos: ¿Cuáles son las directivas del negocio?, ¿Qué niveles de seguridad son apropiados?, ¿Dónde son los sistemas más vulnerables?, ¿Cuáles son las restricciones a cumplir?, ¿Cuáles son los costos y beneficios involucrados?, etc.



Figura 24: Principales pasos para definir requerimientos.

6.4.1 Directivas del Negocio

El problema de negocio que se quiere resolver definirá el alcance que tendrá la PKI para integrarse dentro de una organización, resulta necesario entonces entender con claridad las directrices del negocio para el despliegue exitoso de PKI.

Si estas directrices sólo afectan a un número reducido de usuarios la instalación de PKI será limitada en el mejor de los casos. Si las directrices afectan una cantidad mayor de usuarios el despliegue deberá recibir una considerable atención corporativa para tener el éxito buscado.

Las directrices de negocios típicos que requieren una PKI están orientados a:

- **Negocios Electrónicos.** Generalmente se muestra como una necesidad de expansión de los negocios hacia el entorno electrónico, lo que se manifiesta en el interés de que las transacciones por este medio sean realmente seguras. En transacciones grandes los riesgos de pérdidas por robos pueden estimular a una organización a utilizar PKI para limitar dichas pérdidas, en transacciones pequeñas puede ayudar a resolver disputas legales disminuyendo los costos.
- **Privacidad, Integridad y Autenticidad de la Información.** Una organización puede necesitar usar Internet como una forma de comunicarse con sus diferentes sucursales o con sus socios y clientes. Estas comunicaciones con frecuencia pueden contener información confidencial contenida en documentos o correos electrónicos, por lo que sería de gran interés y valor para la organización garantizar que sus comunicaciones no puedan ser adulteradas.
- **Reducción del trabajo de oficina.** Una organización puede necesitar almacenar gran cantidad de papeles firmados durante un periodo largo de tiempo, para satisfacer disposiciones legales por ejemplo. Con el objetivo de reducir los costos

que esto implica, la organización necesita reemplazar los documentos firmados físicamente con documentos firmados de forma electrónica.

- **Menores costos en el soporte al usuario.** Los usuarios emplean varias aplicaciones las cuales requieren generalmente de un nombre de usuario y contraseña, manejar la administración de las cuentas de usuarios y contraseñas puede consumir un gran porcentaje de recursos, por lo que la utilización de certificados digitales como medio de autenticación ayudaría a disminuir la utilización de esos recursos.

Una vez entendidas las directrices y aceptado el hecho de que la organización requiere PKI, es necesario una persona que dirija el proceso de financiamiento y los esfuerzos de implementación preliminar de PKI, lo que además puede necesitar una evaluación por parte de un comité que analice el impacto en el negocio y la efectividad de los costos a largo plazo.

La decisión final de incorporar PKI puede necesitar la realización de varios pilotos de prueba para la determinación del impacto que tiene la PKI sobre las diferentes funciones del negocio o para determinar las aplicaciones con mayor rendimiento.

Por lo tanto es necesario responder además cosas como: ¿Quiénes serán los auspiciadores organizacionales de la PKI?, ¿Quién asignará los recursos?, ¿De dónde procederán los fondos?, ¿Cómo se determinarán los costos?, ¿Cómo se desarrollarán los pilotos?, etc.

6.4.2 Aplicaciones

Una vez que se han entendido las directrices del negocio, la organización puede analizar cuáles son las aplicaciones que tendrán el mayor rendimiento con

PKI. Por lo tanto antes de diseñar la PKI se debe determinar las necesidades de seguridad de cada aplicación, por lo que se podría necesitar administrar certificados para cada una de éstas.

Las aplicaciones más comunes de PKI son:

- El Correo Electrónico Seguro. El correo de Internet estándar envía un mensaje en texto plano sobre la red, permitiendo a intrusos poder monitorear los servidores de correo y la red para obtener información sensible. Otra forma de intrusión es la suplantación de identidad con herramientas que modifican los encabezados del correo, con lo que cualquier persona podría enviar información falsa en nombre de otro, incluyendo un virus. Por esto, para algunas organizaciones la seguridad en el correo es prioridad.
- Comunicaciones Seguras. PKI puede asegurar las comunicaciones en Internet y otros canales de comunicación abiertos. Por ejemplo SSL se utiliza ampliamente para garantizar la seguridad en el comercio vía Web, su seguridad se basa en mecanismos de autenticación de clave pública. Otro ejemplo son las redes privadas que se basan en servicios de seguridad IPSec, que es un conjunto de protocolos que permiten la firma y el cifrado de comunicaciones entre computadores de forma transparente para las aplicaciones.
- Transacciones Seguras de e-Comercio. Las transacciones con firma digital pueden ofrecer la seguridad de que el firmante en realidad dio origen a la transacción y que ésta no sufrió alteraciones durante su transito por la red. Es útil para contratos legales basados en documentos electrónicos.
- Firma de código. Un creciente número de aplicaciones, controles ActiveX y Applets java son bajados e instalados sobre computadores con pequeña o

ninguna notificación acerca de su autoría. Los autores de software pueden entonces firmar sus archivos para demostrar que proceden de ellos legítimamente y que no han sido modificados desde su publicación.

- Autenticación en Internet. Internet se ha convertido en un elemento clave en el crecimiento del e-comercio. Sin embargo al momento de utilizarla surgen algunas preocupaciones en relación a la confidencialidad de los datos transferidos entre clientes y servidores, la autenticación del servidor y la autenticación de los clientes.
- Autenticación inalámbrica. Un creciente número de organizaciones está implementando redes de acceso inalámbrico, lo que crea desafíos para que sólo usuarios autenticados puedan acceder a éstas, y que los datos transmitidos no puedan ser interceptados.

Si en este proceso de identificación de aplicaciones se determina además realizar cambios a las ya existentes, la organización deberá determinar cómo realizar los cambios para incorporar PKI en éstas. Crear una nueva versión que soporte PKI puede ser la mejor opción pero el costo podría ser alto.

Es necesario entonces tomar nuevas decisiones: ¿Cuáles aplicaciones usarán PKI?, ¿Cuáles tendrán mayor prioridad?, ¿Cómo se migrarán las aplicaciones existentes a PKI?, ¿Tendrán que soportar PKI las nuevas aplicaciones?.

6.4.3 Usuarios

Después de haber identificado las aplicaciones a “PKIzar”, se debe identificar los tipos de usuarios que utilizarán estas aplicaciones y para los cuales es necesario emitir certificados. Por ejemplo el uso de un certificado puede estar basado en las funciones laborales, la localización, la estructura organizacional o alguna

combinación de éstas. En todo caso, para cada uno de los grupos que se definan, se necesita determinar:

- El número de usuarios, computadores y aplicaciones que necesitan certificados. Este número puede ser tan extenso como una organización completa o tan pequeño como un único usuario.
- La localización física de los usuarios, computadores y aplicaciones que necesitan certificados. Diferentes soluciones pueden ser requeridas para usuarios remotos y para los usuarios ubicados en la oficina central de la organización.
- Número de certificados requeridos por cada tipo de usuario. En algunos casos un certificado será suficiente para satisfacer todos los requerimientos, otras veces se necesitarán varios.
- Los requerimientos de enrolamiento para cada certificado que se planea emitir, por ejemplo los objetos de identificación física que los usuarios deben presentar al momento de solicitar un certificado.

6.4.4 Niveles de Seguridad

Es recomendable también definir el nivel de seguridad que es requerido para cada tipo de usuario que utilizará los certificados. Los usuarios que trabajan con datos sensibles o información confidencial típicamente requieren niveles más altos de seguridad que otros miembros de la organización.

Grupo usuarios	Número	Localización	Aplicaciones	Nivel de Seguridad
Usuarios	45000	Interna	E-mail, firma documentos	Medio
Administradores y Desarrolladores	250	Interna	Control acceso, firma código	Alto
Servidores	50	Interna	Autenticación	Alto
Socios	35	Externa	Control acceso	Alto

Tabla 10: Tabla Ejemplo definición de requerimientos.

Una vez obtenida toda esta información el siguiente paso es diseñar la arquitectura que soporte estos usuarios y aplicaciones.

6.5 Arquitectura

Una vez que los requerimientos son conocidos, el próximo paso es producir el modelo estructural de la PKI que dará soporte a las aplicaciones y a los usuarios, y que dará capacidades de manejo a los administradores y la flexibilidad para mantener las necesidades actuales y futuras de seguridad de la organización.

Diseñar la arquitectura implica por ejemplo realizar los siguientes pasos:

- Planificar una infraestructura CA incluyendo el número, localización y tipo de CA requeridas.
- Diseñar la jerarquía de confianza de la CA.
- Diseñar la arquitectura del modelo de confianza.
- Definir los roles de la CA dentro de la jerarquía de confianza.
- Establecer una convención de nombres.
- Seleccionar la base de datos de la CA y su ubicación.
- Seleccionar el número de RA a utilizar y su distribución.
- Determinar el tipo de repositorio para los certificados y CRL, etc.

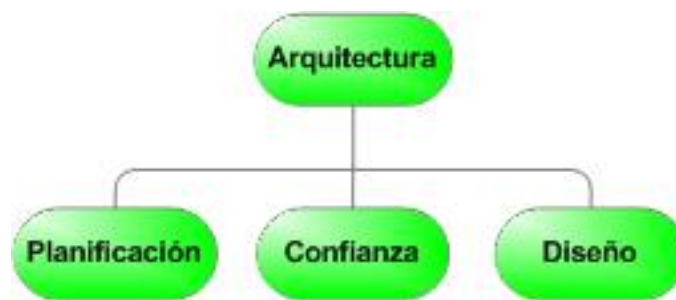


Figura 25: Principales pasos para definir la arquitectura.

6.5.1 Planificación

Antes de establecer una infraestructura de CA que satisfaga los requerimientos de certificación y las necesidades de seguridad para la organización, se necesita tomar decisiones acerca de las opciones que las CA tendrán disponibles. Planificar la infraestructura de las CA implica tomar decisiones acerca de por ejemplo:

- La localización de la CA raíz.
- CA interna v/s de terceros.
- Requerimientos de capacidades, rendimiento y escalabilidad.
- Estructura del repositorio de certificados, centralizado o distribuido.
- Modelo de administración, central o basado en roles.
- Uso de proveedores de servicios de criptografía.
- Número de CA requeridas, etc.

6.5.1.1 CA raíz

Una infraestructura CA consiste generalmente de una jerarquía de CA que confían unas en otras y que autentifican sus certificados. Dentro de esta estructura, una autoridad final debe ser establecida.

La CA raíz certifica a otras CA para publicar y administrar certificados dentro de una organización. Antes de establecer una jerarquía se debe determinar:

- Quién diseña la CA raíz en la organización. Por ejemplo, es responsabilidad de un departamento dentro de la organización o de una organización externa.
- Dónde estará localizada la CA raíz.
- Quién administrará la CA raíz.
- Si el rol de la CA raíz es sólo certificar otras CA, o también sirve a solicitudes de certificación de usuarios finales.

Después de estas determinaciones, se puede definir roles para cualquier CA adicional, incluyendo quién las administrará y que relaciones de confianza tendrán con las demás CA.

6.5.1.2 CA interna v/s de terceros

Dependiendo de la funcionalidad que se requiera, las capacidades de la organización, capacidades de sus administradores y los costos que pueda soportar ésta, se puede elegir si la base de la infraestructura CA será desarrollada internamente, a través de terceros o mediante una combinación de ambos.

- **CA interna**

Si la organización conduce la mayoría de sus negocios con socios organizacionales y quiere mantener el control de cómo los certificados son emitidos, una CA al interior de la organización es la mejor opción.

Entre las ventajas de las CA internas están:

- Permiten a una organización mantener control directo sobre sus políticas de seguridad.
- Permiten a una organización alinear sus políticas de certificación con sus políticas de seguridad general.
- Pueden ser integradas con la infraestructura de almacenamiento de la organización.
- Puede ser expandidas para incluir funcionalidades y usuarios adicionales con costos extras relativamente pequeños.

Las desventajas incluyen:

- La organización debe manejar sus propios certificados, con las complicaciones que esto pueda implicar.
- El despliegue en tiempo puede ser más largo que para una CA proporcionada por proveedores externos.
- La organización debe aceptar las responsabilidades por problemas con la PKI.

- **CA externas**

Si la organización conduce la mayoría de sus negocios con clientes o consumidores externos y desea realizar negocios con ellos mediante certificados digitales y administrar estos procesos de forma externa, las CA de terceros podría ser la opción a elegir.

Las CA de terceros permite:

- Mayores grados de confianza a los consumidores o clientes cuando conducen transacciones seguras con la organización.
- Usar tecnologías de seguridad basadas en certificados mientras se desarrolla internamente la administración de la PKI.
- Tomar ventaja del entendimiento de asuntos técnicos, legales y de negocio relacionados con el uso de certificados desde la experiencia del proveedor de la CA.

Las desventajas incluyen:

- Involucran generalmente un alto costo.
- No permite una mayor flexibilidad en la configuración y administración de los certificados.
- La CA de terceros permite generalmente sólo una integración limitada con los sistemas internos de la organización.

6.5.1.3 Rendimiento y Número de CA

Una de las cosas que se debe determinar en esta etapa es el número apropiado de CA y la mejor configuración de éstas, por lo que se necesita evaluar los factores que impactan sobre la capacidad, rendimiento y escalabilidad de los servicios PKI. Estos incluyen:

- Las necesidades de certificación o sea el número de certificados que se necesitan emitir y renovar, generalmente por día.
- Los objetivos de expansión de la infraestructura.
- El grado de relevancia de la disponibilidad de la CA.
- El esfuerzo necesario para mantener la seguridad de la infraestructura.
- El largo de las claves de la CA emisora de certificados.
- El tipo de hardware utilizado para la CA, como procesador, memoria, disco duro, etc.
- El número de clientes que se necesita soportar.
- La calidad de las conexiones de red, etc.

Para demostrar el efecto de estos factores se puede mencionar por ejemplo que un servidor CA podría necesitar emitir del orden miles de certificados por día por lo que se haría necesario un servidor con grandes capacidades de procesamiento, para las operaciones de cifrado y firma involucradas en la emisión. Esto opcionalmente implica usar un número mayor de CA más pequeñas para mejorar el rendimiento y permitir a las aplicaciones consultar las CRL más rápidamente, esto

reduce también el riesgo que la organización pueda ser forzada a revocar y reemitir todos sus certificados cuando una CA se ve comprometida.

Otro ejemplo es que para muchas organizaciones, las primeras limitantes del rendimiento de la CA son la cantidad de almacenamiento físico disponible y la calidad de la conectividad de sus clientes con la infraestructura, ya que si demasiados clientes intentan acceder a ésta sobre conexiones de red lentas, las solicitudes de todo tipo se retrasarán.

Otro factor significativo en el rendimiento es el número de roles que un servidor CA debe realizar. Si un servidor opera realizando otras funciones como la de repositorio, esto puede impactar negativamente su capacidad y rendimiento, lo que también puede complicar la administración.

Adicionalmente hay algunos componentes de hardware que impactan sobre la capacidad y rendimiento de la PKI, por lo que se debe considerar:

- Número de CPU. El poder de CPU es el recurso más crítico para el rendimiento de una CA, ya que claves de mayor tamaño requieren más recursos de CPU.
- Desempeño de discos. En general un alto desempeño de discos permite una tasa mayor de enrolamientos, ya que con largos de claves pequeños la CPU realiza menos cálculos y por tanto completa un mayor número de operaciones. Con claves más largas, la CPU necesita más tiempo lo que resulta en un número menor de operaciones de lectura-escritura en los discos.
- Capacidad de discos. El tamaño de la base de datos de la CA aumenta de forma lineal con el número de registros de certificados agregados. Por lo tanto

a mayor capacidad de discos, mayor será el número de certificados que la CA puede emitir. Se debe planificar los requerimientos de disco de forma creciente en el tiempo tomando en cuenta que cada certificado requiere alrededor de 15 KB para su almacenamiento.

Para determinar el número de CA entonces, se pueden tomar en cuenta todos estos factores y en el caso de decidir utilizar más de una CA, se debe definir:

- ¿ Cuantas CA intermedias utilizar?
- ¿Cuanta CA emisoras se necesitan?

El número de CA emisoras e intermedias a desplegar dependerá de:

- El uso de los certificados. Estos pueden ser emitidos para varios propósitos, cada uno de éstos puede involucrar diferentes políticas de emisión, por lo que usar CA separadas provee una forma de administrar cada política de forma independiente.
- División geográfica u organizacional. Se puede tener diferentes CA emisoras dependiendo de la localización física de los usuarios en la organización.
- Distribución de la carga de certificación. Se puede desplegar múltiples CA emisoras para distribuir la carga de los requerimientos de certificación en la red. Por ejemplo si los enlaces son lentos y discontinuos, se puede necesitar localizar varias CA emisoras.
- Flexibilidad. Cuando se usa más de una CA subordinada, se puede desactivar una subsección de la jerarquía de la CA sin afectar las relaciones de confianza del resto de ésta.

Cualquiera sea el número de CA que se considere, se debe siempre tener sólo el indispensable para el funcionamiento eficiente de la infraestructura. Desplegar más CA de las requeridas crea una carga innecesaria de administración e introduce áreas adicionales de vulnerabilidad.

6.5.1.4 Estructura del Repositorio

En los ambientes PKI la disponibilidad de los servicios CA son menos importantes que la disponibilidad del repositorio que almacena los certificados y las CRL, por lo tanto es importante integrar los servicios del repositorio lo mejor posible para que los certificados y las CRL sean automáticamente publicadas y los usuarios puedan acceder de forma expedita a ellos.

Muchas organizaciones ya utilizan repositorios de datos centralizados, como son los servicios de directorios accedidos mediante LDAP, puede entonces ser necesario y beneficioso que los repositorios de certificados estén integrados con estos servicios.

Si se decide publicar los certificados en un directorio o en una base de datos, se necesita adaptar los esquemas de éstos a las necesidades de publicación y seguridad de la CA.

Hay algunas preguntas a las cuales dar respuesta en este ámbito: ¿Se usarán las bases de datos existentes en la organización?, ¿Se puede ajustar la CA para utilizar servicios de directorios?, ¿Permanecerán los certificados expirados y los revocados en las bases de datos?.

6.5.1.5 Roles de Administración

Es importante definir el modelo de administración de la PKI de forma temprana, este modelo debe ayudar a mantener un criterio común para la separación de los roles de administración.

Para asegurarse que un único individuo no puede comprometer los servicios PKI, es mejor distribuir roles de administración a través de diferentes individuos en la organización.

Esto implica decidir cuales individuos realizan por ejemplo las siguientes tareas:

- Instalar y Configurar las CA, RA, repositorios, etc.
- Manejar plantillas de certificados.
- Emitir o revocar certificados de usuarios.
- Configurar y revisar archivos de auditoria.

Se puede utilizar listas o métodos de control de acceso para manejar permisos en los distintos componentes PKI y delegar tareas de administración. Por ejemplo se pueden definir roles como:

- Administrador de servicios. Configura y maneja servicios, asigna administradores de certificados y renueva certificados de la CA.
- Administrador de certificados. Emite y revoca los certificados.
- Auditor. Audita las acciones de los administradores anteriormente señalados.

La extensión de los roles depende del nivel de seguridad que se requiera, pero asignar los menos derechos posibles permite un mayor nivel de seguridad.

RoI PKI	Descripción
Administrador PKI	Configura, mantiene, y renueva la CA.
Operador de respaldo	Realiza respaldo sistema y recuperación.
Administrador Auditoria	Configura, revisa, y mantiene archivos de actividades.
Administrador Certificados	Aprueba enrolamiento de certificados y solicitud de revocación.
Administrador Usuarios	Administra usuarios y su información asociada.
Operador RA	Solicita certificados a la CA.

Tabla 11: Ejemplo roles administrativos PKI.

En esta etapa debe intervenir la directiva de seguridad de la organización, si no se cuenta con ella se debe establecer una para documentar los roles y responsabilidades de seguridad.

Acción	Operador RA	Administrador PKI	Administrador Certificados	Administrador Auditoria	Operador respaldo	Administrador Servidor local
Instalar CA.						X
Configurar CA.		X				
Configurar Política.		X				
Subir / bajar Servicio.		X				X
Renovar claves CA.		X				
Emitir / Aprobar Certificados			X			
Rechazar Certificados			X			
Revocar Certificados			X			
Renovar Certificados			X			
Publicar / Configurar CRL		X				
Configurar Parámetros Auditoria				X		X
Auditar archivos de eventos				X		X
Respalda Sistema					X	X
Restaura Sistema					X	X
Solicita Certificados	X					

Tabla 12: Ejemplo lista de acciones realizadas por roles PKI.

6.5.1.6 Proveedores Criptográficos

El hardware de algunos proveedores de servicios criptográficos puede soportar un extenso rango de operaciones y de tecnologías, por esto es importante considéralos al momento de analizar las opciones de implementación PKI.

Almacenar claves en hardware resistente a fallas es más seguro que hacerlo en discos duros o disquetes, por lo tanto, las claves almacenadas en dispositivos criptográficos pueden tener ciclos de vida más extensos. Otra ventaja de éstos es que la clave es mantenida fuera de la memoria del computador, lo que hace difícil el acceso a ella por ejemplo mediante un desbordamiento de memoria.

Si se elige hardware criptográfico para la clave privada de la CA se debe asegurar que éste permanece físicamente seguro o al menos respaldado, además no debe ser sólo manejado por un ente ya que cuando se almacenan las claves en estos dispositivos, nadie en la organización puede emitir o revocar certificados sin la tarjeta apropiada y el número correcto de identificación para acceder a ésta, esto si bien puede ser una complicación también lo convierte en el esquema más apropiado para mantener la seguridad del sistema.

Existe también hardware para generar las claves de los usuarios, el que debe ser igualmente evaluado, ya que puede ayudar en el rendimiento de las CA en el caso de que éstas tengan una alta demanda por sus servicios.

6.5.2 Modelo de Confianza

Una PKI se fundamenta sobre una jerarquía de confianza, la que provee escalabilidad y facilidad de administración. En un modelo jerárquico múltiples CA son organizadas en una relación de padre/hijo claramente establecida, en donde las CA hijas son certificadas por las CA padres.

Los tipos básicos de jerarquía a elegir para la implementación PKI son:

- **Jerarquía Enraizada o de CA Raíz.** En una jerarquía enraizada, una CA puede ser raíz y las demás son subordinadas.
- **Jerarquía en red o de Certificación Cruzada.** En una jerarquía en red, cada CA puede ser ambas, una CA raíz y una subordinada.
- **Jerarquía híbrida.** Las jerarquías híbridas combinan elementos de las dos jerarquías mencionadas anteriormente.

Además de aplicar cualquiera de estos modelos de confianza, se puede diseñar la estructura de las CA dividida por ejemplo en el uso de los certificados, en la estructura organizacional o en la localización de los usuarios.

6.5.2.1 Modelo Enraizado

En un modelo de confianza de jerarquía enraizada, una CA es el ancla de confianza y posee un certificado autofirmado. Esta CA raíz emite un certificado para cada CA directamente subordinada, las cuales a su vez emiten certificados a las CA subordinadas a ellas o a usuarios finales. Una CA subordinada es confiable sobre la base de la firma de su padre.

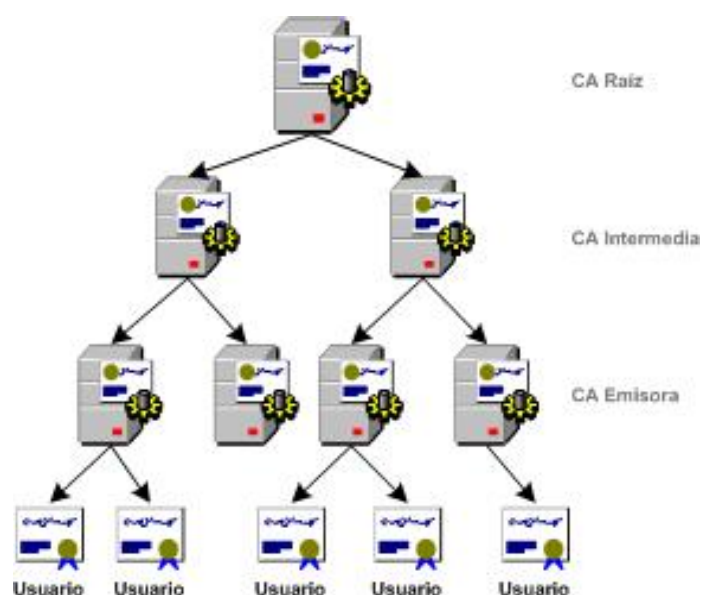


Figura 26: Modelo de confianza jerárquica enraizada.

Se pueden agregar nuevas CA en cualquier parte de la jerarquía excepto la raíz. Si se agrega una nueva jerarquía, ésta sólo necesita confiar en la CA raíz de la PKI para confiar en todas las CA subordinadas en la nueva jerarquía.

Las jerarquías enraizadas también permiten dividir los riesgos, la administración y el proceso de certificación, por lo que son más escalables y fáciles de administrar que otras jerarquías, ya que cada CA sirve un único rol.

Las jerarquías enraizadas además proveen una forma más clara de determinar si un certificado puede ser confiable, ya que la cadena de confianza siempre termina en la CA raíz, de modo que sólo la ruta a ésta debe ser validada.

La desventaja de este modelo radica principalmente en que si el certificado de CA raíz expira, todos los certificados que fueron emitidos por ésta y por sus CA subordinadas también expiran, ya que su confianza se vuelve sospechosa.

6.5.2.2 Modelo en Red

Si la organización tiene múltiples divisiones distribuidas puede que no sea capas de establecer una única raíz o ancla de confianza.

En esta situación, se puede implementar un modelo de confianza jerárquico en red, en el cual las relaciones de confianza entre las CA se establecen en base certificación cruzada. La certificación cruzada corresponde a certificados especiales que son usados para establecer confianza completa o limitada entre las CA, que de otra manera no tendrían relación.

La CA que certifica cruzado es el emisor y la CA que es certificada de forma cruzada es el sujeto. Debido a que la certificación cruzada es una subordinación lógica de una CA a otra, un modelo de confianza en red es en efecto una jerarquía, con la propiedad adicional que una CA raíz es también una CA subordinada.

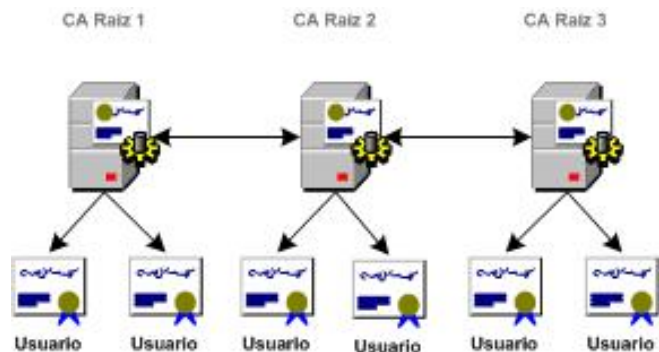


Figura 27: Modelo de confianza jerárquico en red.

La confianza en este modelo es generalmente bidireccional, lo que significa que la CA 1 emite una certificación cruzada de confianza a la CA 2 y la CA 2 emite una certificación cruzada de confianza a la CA 1. También es posible disolver la confianza en una CA revocando su certificación cruzada.

Sin embargo, la certificación cruzada no necesita ser bidireccional y una certificación cruzada de una CA no necesita la cooperación de la CA a ser

certificada. Para hacer esto, la CA crea un certificado cruzado sin el conocimiento de la CA a ser certificada, porque todo lo que necesita es el certificado de la clave pública de ésta. El proceso se conoce como certificación cruzada unilateral, donde una CA certifica cruzado a otra pero no a la inversa. La certificación cruzada permite entonces crear puentes entre PKI separadas sin que una PKI sea directamente subordinada a la otra.

El modelo de confianza de jerarquía de red es sin embargo mucho más difícil de mantener, de descubrirle problemas y de solucionarlos.

6.5.2.3 Modelo Híbrido

Algunas organizaciones pueden encontrar un modelo puramente jerárquico muy restrictivo, por que una única CA no puede servir como raíz para todas las otras. A su vez un modelo puramente de red puede ser muy complejo si se involucran muchas CA diferentes. Si se usa un modelo híbrido sin embargo, se puede certificar cruzado sólo ciertas CA y así utilizar los beneficios de ambos modelos de jerarquía.

6.5.3 Diseño Estructural

Una infraestructura consiste de una jerarquía de varias CA que confían unas en otras y que emiten y autentifican certificados. Esta jerarquía o arquitectura puede estructurarse basándose en varios factores, como son las funciones de los usuarios, el uso de los certificados, la estructura organizacional, niveles de seguridad, etc.

6.5.3.1 Basada en Uso de Certificados

Algunas organizaciones pueden basar su jerarquía en los tipos de servicios y aplicaciones para los cuales se requieren certificados. Una jerarquía basada en el

uso de certificados trabaja en organizaciones en las cuales los grupos de usuarios y computadores tiene diferentes requerimientos de aplicaciones.

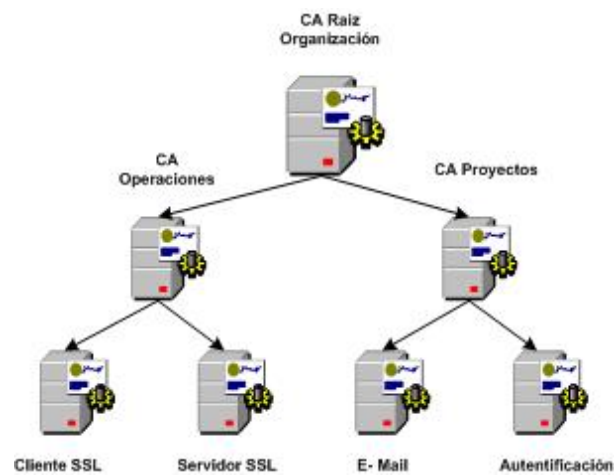


Figura 28: Estructura basada en el uso de certificados.

En una jerarquía que se basa en el uso que se le da a los certificados, las CA directamente subordinada a la CA raíz son organizadas por el tipo de servicio o aplicación que requiere certificados. Por ejemplo se puede crear una CA solamente para emitir certificados de correo electrónico y otra para emitir certificados SSL.

6.5.3.2 Basada en la Estructura Organizacional

Algunas organizaciones pueden elegir basar su jerarquía en su estructura administrativa. De esta forma las CA directamente subordinadas a la CA raíz son organizadas por el tipo de relaciones que los usuarios tienen con la organización (clientes, socios o empleados, etc.).

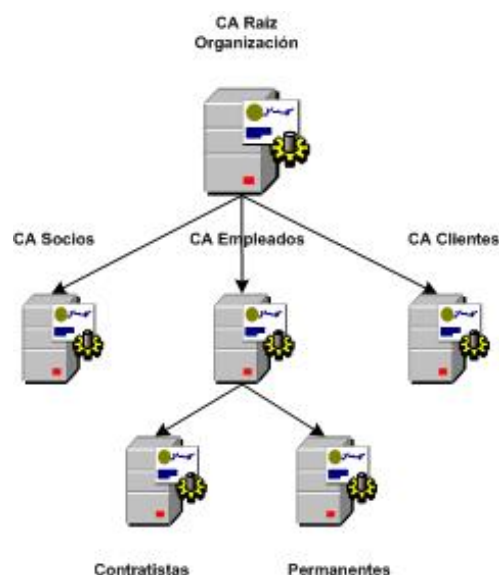


Figura 29: Jerarquía basada en la estructura organizacional.

Por ejemplo, las CA emisoras pueden ser configuradas para soportar diferentes tipos de empleados, tal como contratistas y empleados permanentes. La política de emisión puede definir entonces que las medidas más fuertes de seguridad sean aplicadas a los contratistas y empleados temporales, mientras que para lo empleados permanentes éstas podrían ser menos estrictas.

6.5.3.3 Basada en la Localización

Diseñar una arquitectura de acuerdo a la localización permite a las CA emitir certificados de forma local a usuarios que están distantes geográficamente.

Una jerarquía basada en la localización disminuye el tiempo de respuesta, permitiendo publicar información en repositorios locales más cercanos a los usuarios.

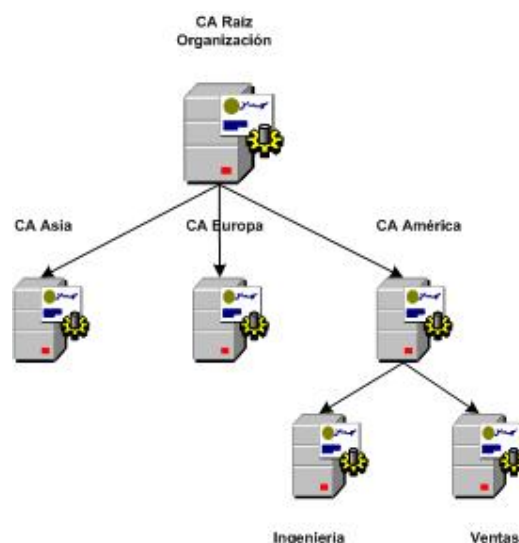


Figura 30: Jerarquía basada en la localización.

6.5.4 Consideraciones de Seguridad

Asegurar la jerarquía CA es una tarea crítica. Si un intruso puede acceder a la CA ya sea físicamente o a través de la red puede recuperar la clave privada de ésta y entonces suplantarla. Si una CA se ve comprometida, esto invalida la confianza en ésta y cualquier CA en la jerarquía que esté bajo ella. Por esta razón es importante evitar que la CA raíz esté conectada a la red.

Para asegurar la fiabilidad de la infraestructura, se puede especificar que cualquier CA intermedia o raíz que no emita certificados de forma permanente debe estar fuera de línea.

Esto minimiza el riesgo de que la clave privada de la CA llegue a estar comprometida. Aunque se debe tener cuidado si la CA emite listas de revocación o si procesa solicitudes de usuarios.

Se puede tener una CA fuera de línea de las siguientes maneras:

- Físicamente, removiendo el servidor de la red.

- Bajando el servicio de certificación.
- Apagando el servidor (la forma más segura aunque no habría posibilidad de obtener notificaciones de fallas).

Tener una CA raíz fuera de línea no reduce su importancia, además se debe mantener en un área segura con acceso restringido y usar en ella hardware confiable.

Debido a que las CA fuera de línea procesan un pequeño número de certificados, el costo administrativo al mantener una CA fuera de línea es bajo. Además la validación del certificado por el cliente no se ve afectado cuando la CA está fuera de línea porque este debe verificar la cadena de confianza y la CRL, cuya información debería estar disponible en el repositorio y la información para llegar a éste en los certificados que se quieren validar.

6.5.5 Localización de Bases de Datos

Cuando se instala una CA en la organización, se debe especificar una localización para las bases de datos y los archivos de eventos que pueda necesitar para su funcionamiento, se debe también almacenar información acerca de la configuración de la CA lo que puede ser útil como respaldo para una futura y eventual restauración.

Es buena medida localizar las bases de datos y archivos de eventos en discos separados físicamente, para mejorar la tolerancia a fallos y el rendimiento.

6.5.6 Nombres

Antes de configurar las CA en la organización, se debe establecer una convención de nombres de CA, ya que el nombre que se selecciona cuando se

configura un servidor que será una CA es reflejado en cada certificado que emite. Es importante ya que no se puede cambiar el nombre de una CA sin invalidar todos los certificados emitidos por ésta.

6.6 Configuración Certificados

Los certificados son una cadena de datos binarios, y para que una aplicación pueda utilizarlos, ésta debe saber como interpretar dichos datos.

Originalmente ISO definió el formato de los certificados y sobre la base de estas normas los certificados deben contar con cierta información en un orden específico, sin embargo el estándar ofrece distintas maneras de como la información puede ser codificada dentro del certificado, además de ofrecer extensiones opcionales.

Por tanto si dos organizaciones eligen utilizar certificados con extensiones opcionales distintas, éstas no se podrán comunicar mediante sus certificados sin un proceso de traducción, además de esto hay otras características en los certificados que deben compatibilizarse como son los algoritmos y el tamaño de las claves.

En esta etapa entonces se deben definir algunos puntos como pueden ser:

- Información contenida en los certificados a emitir. Una plantilla sería de buena ayuda, simplificando el proceso de configuración de los certificados.
- Largo de claves y algoritmos de cifrado. Los algoritmos de cifrado y largo de claves que se elijan impactan la cantidad de esfuerzo necesario para descifrar las firmas. Además los certificados utilizados en datos más sensibles deben ser protegidos con claves y algoritmos más fuertes.

- El ciclo de vida para cada certificado. El ciclo de vida es dependiente de la sensibilidad de los datos a ser protegidos, claves y algoritmos más fuertes pueden justificar ciclos de vida de certificados mayores.
- Políticas de renovación para cada certificado. Una planificación y administración adecuada de las políticas de renovación puede simplificar la administración de certificados.
- Restricciones a los certificados. Se debe limitar los usos no planificados de los certificados y asegurar que las restricciones de los CPS se mantengan.

Cada una de estas decisiones puede impactar a otras, por ejemplo un certificado para un pequeño grupo de usuarios con grandes necesidades de seguridad, puede justificar claves más largas y ciclos de vida más pequeños, además de restringir la posibilidad de renovación.



Figura 31: Principales pasos para configurar certificados.

6.6.1 Plantillas de Certificados

Puede que dependiendo de las aplicaciones utilizadas se necesite información específica en los certificados, por ejemplo los certificados para correo electrónico firmado deben contener la dirección de correo del usuario, sino las aplicaciones los rechazarán para tales usos. Se puede necesitar además incluir atributos adicionales

como el título profesional, si el usuario está firmando un documento en el ejercicio de la profesión, etc.

Existen además otros campos que definir dentro de un certificado como son el uso de las claves y el uso del certificado, los que si son establecidos como críticos y si las aplicaciones verifican esta condición impedirán el uso del certificado en aplicaciones distintas a las establecidas, por lo que los datos de dichos campos deben ser definidos con minuciosidad.

Por último para terminar de configurar las características de los certificados, se debe establecer sus restricciones y alcances, especificando en uno de sus campos la asociación a una política de certificación.

Sería entonces de utilidad definir plantillas que proporcionen el contenido por defecto para un tipo particular de certificado y que las CA pudieran emitir sus certificados basados en éstas para facilitar así el proceso de emisión.

6.6.2 Algoritmos y Largo de Claves

En cuanto a los algoritmos y el largo de las claves será necesario determinar que longitudes ofrecen la mejor opción de intercambio entre seguridad y rendimiento para el ambiente de la organización.

Si las claves serán utilizadas solo en el ámbito interno y las directivas de la organización le conceden una prioridad baja, entonces lo más adecuado sería utilizar claves pequeñas para ahorrarse algún tiempo de procesamiento.

Los requerimientos de seguridad para los certificados y sus claves se basan principalmente en:

- **Confianza en los Usuarios.** El tipo de usuario afecta el grado de confianza, por ejemplo usuarios temporales dan menos confianza por lo tanto para éstos los ciclos de vida de los certificados pueden ser menores además de requerir controles más estrictos en la renovación de sus claves.
- **Esfuerzo Administrativo.** Si la renovación de un certificado de CA por ejemplo implica un esfuerzo grande, se puede especificar un ciclo de vida más largo para los certificados de éstas y no tener así que renovarlos con tanta frecuencia.
- **Valor Comercial.** Por ejemplo certificados usados para validar datos críticos como contratos deberán tener claves más grandes y mayores restricciones en la identificación de sus titulares.

En la mayoría de los casos el largo de las claves debe proporcionar un balance entre las necesidades de seguridad y el rendimiento de la CA, en todo caso esto también dependerá del proveedor de servicios criptográficos y el algoritmo utilizado.

Para el caso de la CA se recomienda seleccionar las claves más largas factibles, claves de al menos 1024 bits son buena elección para las CA certificadoras aunque se recomienda usar 4096 bits -se debe tener en cuenta que generar claves grandes puede generar sobrecarga en un procesador y puede incrementar el tiempo necesario para una operación de firma-. Para un certificado de usuario lo recomendable es utilizar un tamaño de clave de 1024 bits.

En general el largo de las claves no tiene gran impacto sobre el tamaño del certificado, aunque puede ser significativo al momento de almacenarlas en una tarjeta inteligente. Tampoco impactan mayormente la interoperabilidad de distintas

PKI, aunque podría causar que dos PKI no puedan intercambiar claves simétricas o firmar y verificar datos.

6.6.3 Ciclo de Vida

Un número de factores impacta la duración de los certificados, entre los cuales están las necesidades de la organización, el tipo de certificado, e incluso regulaciones gubernamentales. En todo caso el uso de claves grandes avala ciclos de vida de certificados también mayores.

La duración de los certificados y por tanto de las claves impacta la seguridad y las operaciones de la PKI porque:

- Sobre un periodo de tiempo, las claves se vuelven más vulnerables. En general mientras mayor el tiempo que una clave esté en uso, mayor es el riesgo que pueda verse comprometida.
- Cuando el certificado de una CA expira todas las CA subordinadas que dependen de ésta y los certificados finales de usuario también expiran.
- Cuando un certificado CA es renovado todos los certificados que han sido emitidos por la CA deben también ser renovados, ya que todos los certificados emitidos por una CA expiran cuando su certificado es renovado.

Cuando se elige la duración de certificados se debe considerar cuan vulnerables son las claves y cuales son las potenciales consecuencias de su compromiso. Los siguientes factores se deben considerar para realizar esta elección:

- El largo de las claves privadas. Mientras más grandes las claves, es más factible utilizar certificados de mayor duración.

- La seguridad del almacenamiento. En general se puede extender la duración de un certificado si la forma de almacenamiento de la clave privada mejora mediante hardware criptográfico.
- Los usuarios de los certificados. Las organizaciones confían más en sus empleados que en los de otras organizaciones, entonces los certificados para usuarios externos requerirán duraciones inferiores.

En todo caso la fecha de expiración de un certificado se define cuando éste se emite y generalmente corresponde a un año.

Otro aspecto a considerar en el ciclo de vida de los certificados es la renovación. Las CA pueden renovar certificados mientras no alcancen la fecha final de su duración, esto para extender su periodo de validez siempre que no hayan sido revocados antes de esa fecha.

Para disminuir el riesgo de que la clave privada se vea comprometida, las claves pueden ser renovadas cada vez que el certificado es renovado, en lugar de ser renovadas cuando alcancen el final de su duración.

Los ciclos de vida de los certificados afectan también el número de futuras solicitudes de renovación de certificados, debido a esto los ciclos de vida podrían ser aumentados para reducir el número y frecuencia de estas solicitudes.

En general los certificados con claves de largo promedio y ciclos de vida cortos serán renovados con más frecuencia, sin embargo las renovaciones no deben extenderse más allá del ciclo de vida de la CA que está sobre ellos, ya que una CA no puede emitir certificados que posean un ciclo de vida mayor que su propio ciclo.

Para crear una estrategia de renovación de certificados se podría considerar:

- Cuáles certificados se permitirán renovar.
- Con qué frecuencia se podrá renovar un certificado.

Propósito del Certificado	Ciclo de Vida del Certificado	Estrategia de renovación clave privada
CA raíz (clave 4096-bits)	20 años	Renovar al menos cada 10 años para asegurarse que las CA certificadoras intermedias pueden ser emitidas con ciclos de vida de 10 años. Renovar usando una nueva clave al menos cada 20 años.
CA intermedia (clave 2048-bits)	10 años	Renovar al menos cada 5 años para asegurarse que las CA emisoras puede ser emitidas por 5 años. Renovar usando una nueva clave al menos cada 10 años.
CA emisora (clave 2048-bits)	5 años	Renovar usando una nueva clave al menos cada 5 años.
Correo seguro (clave 1024-bits)	1 años	Renovar usando una nueva clave al menos cada 2 años.
Servidor Web (clave 1024-bits)	2 años	Renovar usando una nueva clave al menos cada 2 años.
Socios (clave 1024-bits)	6 meses	Renovar usando una nueva clave al menos cada un año.

Tabla 13: Ejemplo ciclos de vida de certificados.

6.7 Operaciones

Todo sistema de seguridad es dependiente de sus componentes, de la forma en que éstos operan y de la forma en que interactúan. Un sistema de seguridad es tan débil como el más débil de sus componentes y muchas veces aunque éstos sean muy seguros de forma independiente no se garantiza que lo sean en conjunto.

En esta sección se deben definir los procedimientos operativos y controles necesarios para asegurar que los sistemas de seguridad de la PKI son efectivos.

Los CPS son una parte integral de esto. Estos proveen las bases de la confianza entre varias entidades ya que en ellos se plasman las medidas de seguridad de la PKI y además forman parte de las relaciones contractuales con los usuarios.



Figura 32: Principales pasos para definir las operaciones.

6.7.1 Seguridad

La confianza en los certificados y las claves dependerá de la seguridad del servidor CA. Las directivas de seguridad para administrar la CA deben ser claras y los administradores deben tener el entrenamiento adecuado para mantener un servidor seguro. Los accesos al servidor CA deben estar limitados al menor número de personas posibles y con los mayores niveles de seguridad permitidos.

Además, como los certificados y claves tienen una duración definida, puede ser necesario que los registros de transacciones o los documentos firmados estén archivados durante un periodo de tiempo largo, si se da esta necesidad se debe mantener también un archivo de certificados vencidos para poder verificar la firma de los documentos antiguos, por lo tanto estos archivos no deben ser manipulables por extraños que puedan reemplazar su contenido por otros falsos.

Las bases de datos del servidor de certificados deben contar con una copia de seguridad, que ha de necesitar procedimientos para que los datos no puedan ser alterados. Ya que si una base de datos se recupera desde un respaldo alterado, algunos certificados revocados podrían aparecer como válidos.

Por todo esto, se hace necesario determinar: ¿Cuánto tiempo se almacenarán estos archivos?, ¿Cómo se han de proteger? y ¿Dónde serán almacenados?, etc.

Por otra parte uno de los procedimientos operativos más complejos será la renovación de las claves de la CA raíz, ya que el trabajo asociado a esto podría ofrecer una oportunidad para la presentación de un riesgo de seguridad, por lo que en algún momento se deben definir los pasos para llevar a cabo esta acción.

6.7.2 Plan de Administración de Certificados

Una vez definido el contenido de los certificados y la duración de sus ciclos de vida, se necesita especificar un plan de administración para éstos, por lo que se necesita tomar algunas decisiones respecto a:

- Quién generará las claves, los usuarios o la CA, dónde serán almacenadas.
- Cómo se procesan las solicitudes de certificación, la revocación y la renovación de certificados y los datos requeridos para estos procedimientos.
- Cómo administrar y distribuir las CRL.
- Cómo permitir la recuperación de claves, etc.

6.7.2.1 Enrolamiento y Emisión

Para participar en una PKI los usuarios deben solicitar y recibir un certificado de una CA emisora o de una RA representante de ésta, este proceso de solicitud y recepción de un certificado generalmente se denomina enrolamiento.

Típicamente el enrolamiento es iniciado cuando un solicitante proporciona información acerca de su identidad y una clave pública¹⁴¹, hecho esto, el agente encargado del enrolamiento usa esta información para autenticar la identidad del solicitante antes de pasar al procedimiento de emisión del certificado.

¹⁴¹ En el caso que el par de claves sea generado por el usuario.

Para autenticar la información proporcionada por los usuarios se debe en la mayoría de los casos obligar a que éstos se presenten físicamente lo que puede tener ciertas complicaciones, sobre todo si la demanda es considerable o si los usuarios están dispersos por áreas geográficas muy distantes, por lo que para algunos solicitantes el proceso puede ser muy complejo.

Por otro lado si diferentes tipos de certificados requieren distintas revisiones de los antecedentes de los usuarios, éstos deben saber cuáles son las pruebas de identidad a mostrar.

Es importante también decidir si los usuarios podrán solicitar certificados a través de archivos de solicitudes generados por aplicaciones propias, mediante un sistema de enrolamiento Web o si sólo se hará esto de manera presencial.

Si los usuarios envían sus propias solicitudes bajo el formato estándar PKCS #10, implica que ellos han creado sus propias claves, de ser así se debe definir un procedimiento para comprobar la posesión de las claves por parte del solicitante, además se deberá definir si se le dará la opción a los usuarios de salvaguardar su clave privada en los almacenes de la PKI.

Adicionalmente se debe definir si la emisión del certificado será automática o la identidad del solicitante deberá pasar por algunas validaciones extras por parte del administrador de la PKI o de la CA.

Todos estos aspectos deben ser formalizados en un documento de administración del proceso de enrolamiento.

6.7.2.2 Revocación

Todos los certificados tienen un tiempo de vida, sin embargo habrá algunas situaciones en que se hará necesario revocar el certificado asociado a una clave privada antes de que éste alcance su fecha de expiración, por ejemplo cuando algún usuario es afectado por el hurto de un computador donde guarda su clave privada. Por lo tanto se necesitará de una directiva acerca de cómo se manejará este proceso.

Por lo tanto se debe dar respuesta a las siguientes interrogantes:

- ¿Quién revocará los certificados?
- ¿Cuál es el procedimiento y que información se solicitará?
- ¿Qué información quedará registrada después de una revocación?
- ¿Se implementará la capacidad de suspender certificados mientras dura la investigación acerca de la validez de éstos?
- ¿Se necesitan las CRL?
- ¿Cuál es la frecuencia de publicación de las CRL?
- ¿Dónde se publicarán?

No todas la PKI necesitan publicar CRL, si los certificados proveen un nivel de seguridad bajo y no es probable que sean mal utilizados, o si tiene ciclos de vida corto puede que no sea necesario tener que emitir una CRL. De otra manera se hace forzoso la emisión de estos archivos a menos que se tenga un método alternativo como OCSP para reemplazarlos.

Es recomendable también que se definan las circunstancias que justifican la revocación de certificados, entre las que se puede mencionar:

- Un sujeto sin autorización a obtenido acceso a la clave privada de un usuario.
- Un sujeto sin autorización a obtenido acceso a la clave privada de la CA (todos los certificados publicados por ésta deben ser revocados y reemitidos).
- El criterio de certificación ha cambiado.
- El certificado ha sido reemplazado (por otro con una clave mayor).
- La CA que emitió el certificado ya no está operativa, etc.

En cuanto a la localización de la CRL publicada, se debe resolver si éstas son necesarias tanto interna como externamente a la organización. Otro aspecto a tomar en cuenta es si se requieren múltiples localizaciones para publicar las CRL, ya sea por tolerancia a fallos o para soportar una gran cantidad de usuarios. Además se debe seleccionar servidores que provean una mayor cobertura y mejoren los tiempos de respuesta.

En cuanto al tipo de CRL a utilizar, lo más común es usar una lista completa con todo el historial de certificados que han sido revocados durante el tiempo de vida de la CA, lo que en organizaciones que emiten una gran cantidad de certificados hace que las CRL crezcan rápidamente de tamaño, lo que podría hacer aumentar los costos en términos de tiempo y recursos de red al proceder a consultarlas.

Una alternativa a este esquema es publicar CRL que contengan sólo la información que ha cambiando desde la última CRL publicada, como estas CRL son más pequeñas, requieren un ancho de banda menor y pueden ser publicadas con

mayor frecuencia, mejorando la seguridad de la PKI. Por esto combinar ambos tipos de CRL puede mejorar la eficacia de éstas.

En cuanto a las frecuencias de publicación, éstas pueden estar basadas en el número de revocaciones que se llevan a cabo en un periodo de tiempo y en que tan crítico son las necesidades de mantener actualizada la información de revocación de certificados para la organización. En todo caso los ciclos de vida de las CRL son más cortos que el de los certificados y cuando un certificado revocado expira éste es eliminado de la CRL para reducir su tamaño. Normalmente el ciclo de una CRL debería tener una frecuencia de una semana, a menos que los riesgos de usar un certificado revocado sean muy altos.

Una vez que se decida revocar un certificado, se debe generar un registro del solicitante de tal hecho, de quien hace la revocación en el sistema y la razón de ésta para mantener un control completo del proceso.

Todos los aspectos mencionados deben ser formalizados en un documento de administración del proceso de revocación.

6.7.2.3 Recuperación de claves

La pérdida de claves por una falla en el sistema de almacenamiento, por su extravío -frecuente si están almacenadas en una tarjeta inteligente- o sólo por el olvido de la contraseña que las protege, puede ocasionar un alto consumo de tiempo y recursos al intentar su recuperación, más aun si no existe una forma de hacer esto y las claves se deben reemplazar.

Por estas situaciones, datos importantes pueden quedar cifrados de manera permanente, o en el caso que las claves sean utilizadas para el control de acceso, su propietario ya no podría acceder a lugares o recursos importantes, otra razón por el

cual puede ser necesario recuperar una clave es para cambiarla de tipo de almacenamiento o cuando un usuario genera sus propias claves y por seguridad desea respaldarlas al interior de la PKI.

Por todo esto se debe evaluar las consecuencias potenciales de la pérdida de claves para crear una estrategia de recuperación eficiente y rápida, que garantice la seguridad del proceso y no permita la generación de desconfianzas.

Esta estrategia podría definir la utilización de un almacén o depósito de claves con altos requerimientos de seguridad y control de acceso, éste eventualmente y de acuerdo a las políticas de la organización, podría ser el mismo utilizado para la generación de las claves.

Estos aspectos deben también ser formalizados en un documento de administración de recuperación de claves.

6.7.2.4 Publicación

Es importante mantener los certificados al igual que las CRL al alcance de los usuarios para que éstos puedan verificar las identidades de los individuos con los cuales se comunican y para verificar los documentos firmados que pudieran utilizar.

Por esto es importante contar con un buen esquema de publicación, que sea seguro y de disponibilidad constante, que sea escalable en el tiempo dependiendo de la dinámica en la emisión de certificados, que cuente con buenas características de administración y que utilice los estándares más comunes.

Dentro de este ítem se debe definir la frecuencia de publicación de los certificados, por ejemplo si esto se hará cada cierto tiempo, dada una cantidad de certificados emitidos o inmediatamente después a la emisión de cada certificado.

De igual manera que las otras etapas del plan de administración, esto debe ser formalizado en un documento de administración de la publicación.

6.7.2.5 Renovación

La renovación de certificados debería seguir un proceso similar al de solicitud de certificado, pero con medidas menos restrictivas de aseguramiento de la identidad dado que se asume que el solicitante ya cumplió con un proceso de verificación confiable de ésta.

Aun así se deben considerar algunos puntos como son: si sólo se renovará el certificado o también las claves asociadas a éste, si las claves no han sido revocadas esto nos da un indicio para sólo renovar el certificado y seguir utilizando las mismas claves, aunque esto dependerá de las políticas definidas como por ejemplo que cada cierto número de renovaciones se deba obligar al usuario a presentar nuevamente todos los antecedentes que verifiquen su identidad y a renovar las claves.

Nuevamente todos estos aspectos deben quedar formalizados en un documento de administración de la renovación.

6.7.3 Planificación de CPS

El grado de confianza que puede tener un usuario en un certificado y en los datos contenidos en éste depende de varios factores, los que incluyen las prácticas seguidas por la CA durante la autenticación del titular del certificado, las políticas operativas de ésta, los procedimientos y controles de seguridad, las obligaciones y las responsabilidades legales del titular y de la CA. Todos estos puntos deben quedar establecidos en los Estamentos de Prácticas de Certificación de una CA.

Esta sección esboza algunos de los contenidos que debiera tener un CPS basado en el estándar X.509, el que establece ocho componentes principales:

- I Introducción.
- II Cláusulas generales.
- III Identificación y autenticación.
- IV Requerimientos operacionales.
- V Controles de seguridad personal, de procedimientos y físicos.
- VI Controles de seguridad técnica.
- VII Perfiles de certificados y CRL.
- VIII Especificaciones de administración.

Los tópicos aquí identificados son sólo candidatos a su inclusión en una CP¹⁴² o CPS¹⁴³, por lo que no es necesario la inclusión de un estamento para cada tópico.

- I **Introducción.** Este componente introduce al conjunto de cláusulas e indica los tipos de entidades y aplicaciones a los cuales la especificación está orientada. Este componente se puede dividir en:

- Visión general. Provee una introducción a la especificación.
- Comunidad y Aplicabilidad. Describe los tipos de entidades que emiten certificados o que son certificadas como CA, los tipos de entidades que realizan funciones de RA y las que son certificadas como personas o

¹⁴² Política de certificación.

¹⁴³ Estamento de Practicas de Certificación.

subscriptores. También contiene una lista de aplicaciones para las que los certificados son adaptables, restringidos y prohibidos.

- Detalles de contacto. Incluye el nombre y dirección de correo de la autoridad que es responsable de la política o CPS. Incluye también nombre, correo, teléfono y fax de una persona de contacto.

II **Cláusulas Generales.** Especifica algunas presunciones de tópicos legales y prácticas generales. Cada subcomponente puede necesitar cláusulas para cada tipo de entidad. Contiene:

- Obligaciones. Contiene para cada tipo de entidad cláusulas de sus obligaciones con otras entidades, incluye obligaciones de CA y RA; Obligaciones del subscriptor; Obligaciones de las partes confiables; Obligaciones del repositorio.
- Responsabilidades. Contiene para cada entidad cláusulas relacionadas con la responsabilidad: Limitaciones de las garantías; Tope de limitaciones por pérdidas de certificados o en transacciones; Otras excepciones por fuerza mayor.
- Responsabilidad Financiera. Contiene cláusulas relacionadas a las responsabilidades financieras de las entidades: Indemnizaciones de la CA y/o RA; Relaciones legales entre varias entidades.
- Interpretación y Ejecución. Cláusulas relacionadas con la interpretación y ejecución de las CP o CPS. Dirigiendo tópicos como: Ley gobernante; Procedimientos de resolución de disputas.

- Honorarios. Cláusulas relacionadas con los honorarios cargados por las CA, RA y repositorios; Honorarios de acceso a certificados; Honorarios de acceso a información de estado y revocación; Honorarios por otros servicios como información de políticas.
- Publicación y Repositorios. Contiene cláusulas relacionadas con: Obligaciones de la CA a publicar información relacionada con sus prácticas, certificados y estado actual de certificados; Frecuencia de publicaciones; Control de acceso a la información publicada; Requerimientos relativos al uso de repositorios.
- Conformidad de Auditorías. Dirige lo siguiente: Frecuencia de auditorías para cada entidad; Identidad y calificaciones del auditor; Lista de tópicos cubiertos bajo la auditoría; Acciones tomadas como resultado de una deficiencia encontrada mediante la auditoría; Publicación de resultados de la auditoría.
- Política de Confidencialidad. Dirige: Tipo de información que debe ser mantenida por la CA y RA; Tipo de información que no es considerada confidencial; Quién tiene derecho a ser informado de las razones de la revocación y suspensión de los certificados; Condiciones sobre las cuales una CA o RA puede revelar información; Cualquier circunstancia bajo la cual información confidencial puede ser revelada.
- Derechos de Propiedad Intelectual. Dirige los derechos de propiedad intelectual de los certificados, especificaciones de políticas y prácticas, nombres y claves.

III Identificación y Autenticación. Este componente describe los procedimientos utilizados para autenticar un candidato a certificar. También

describe como las partes solicitantes de una revocación y recertificación son autenticadas. Posee los siguientes subcomponentes:

- Registro inicial. Este subcomponente incluye elementos relacionados con los procedimientos de identificación y autenticación durante el registro o emisión del certificado; Reglas para la interpretación de varias formas de nombres; Si los nombres deben ser únicos; Si y cómo el sujeto debe probar la posesión de la clave privada concordante con la clave pública a ser registrada; Los requerimientos de autenticación para identidades de los sujetos y los requerimientos de autenticación para una persona actuando en representación de otra; Cómo una CA o RA valida estos elementos de identificación; Si el individuo debe presentarse personalmente ante la CA o RA.
- Rutina de Renovación. Describe los procedimientos de identificación y autenticación para la rutina de Renovación para cada tipo de sujeto.
- Recertificación después de la revocación. Describe los procedimientos de identificación y autenticación para la recertificación de cada tipo de sujeto después que el certificado del sujeto ha sido revocado.
- Solicitud de Revocación. Describe los procedimientos de identificación y autenticación para una solicitud de revocación para cada tipo de sujeto.

IV **Requerimientos Operacionales.** Este componente es usado para especificar requerimientos impuestos sobre la CA, RA o entidades finales con respecto a varias actividades operacionales. Consiste de los siguientes subcomponentes:

- Aplicación de Certificación. Es usado para declarar requerimientos relacionados con el enrolamiento del sujeto y la solicitud de emisión de certificado.
- Emisión de Certificado. Declara requerimientos relacionados con la emisión de un certificado y la notificación al candidato de tal emisión.
- Aceptación del Certificado. Declara requerimientos relacionados a la aceptación de un certificado emitido y por consiguiente a la publicación del certificado.
- Suspensión y Revocación. Dirige lo siguiente: Circunstancias bajo las cuales un certificado puede ser revocado; Quién puede solicitar la revocación de una entidad certificada; Periodo de gracia disponible para el sujeto; Procedimientos para solicitar la suspensión del certificado; Si se usa el mecanismo de la CRL; Requerimientos sobre las partes que confían de que revisen las CRL; Disponibilidad de la revisión del estado de revocación en línea.
- Procedimientos de Auditoria de Seguridad. Describe el registro de eventos y sistemas de auditoria implementado para el propósito de mantener un ambiente seguro, incluyen lo siguiente: Tipos de eventos registrados; Frecuencia con la cual los registros de auditoria son procesados y auditados; Protección de los registros de auditoria; Procedimientos de respaldo de registros de auditoria; Si el sistema de acumulación de registros de auditoria es interno o externo.
- Cambio de Claves. Describe los procedimientos para proporcionar una nueva clave a los usuarios de la CA.

- Recuperación ante Desastres y Compromisos. Describe requerimientos relacionados a los procedimientos de notificación y recuperación en el evento de un desastre o compromiso; Los procedimientos usados si la clave de la entidad está comprometida; Los procedimientos de la CA para asegurar sus instalaciones durante el periodo de tiempo que sigue a un desastre y los procedimientos antes de que se reestablezca el ambiente seguro en el sitio original o en uno remoto.
- Término de la CA. Describe los requerimientos relacionados con los procedimientos para el término y notificación de término de una CA o RA, incluyendo la identidad de quien conservará los registros de la CA y RA.

V **Controles de seguridad de personal, de procedimientos y físicos.** Estos componentes describen controles de seguridad no técnicos usados por la CA emisora para realizar de forma segura sus funciones. Consiste de los siguientes elementos:

- Controles de Seguridad Física. En este componente se describen los controles de seguridad física sobre las instalaciones que albergan los sistemas de la entidad. Localización de las instalaciones y construcción; Acceso físico; Energía y aire acondicionado; Exposición al agua; Prevención de incendios; Eliminación de basura.
- Controles de Seguridad del Personal. Dirige lo siguiente: Requisitos para el personal que cumple los roles de confianza; Requerimientos de entrenamiento para cada rol; Frecuencia y secuencia de la rotación de trabajo entre varios roles; Sanciones contra el personal por acciones sin autorización; Documentación a ser proporcionada al personal.

VI **Controles de Seguridad Técnica.** Es usado para definir medidas de seguridad tomadas por la CA emisora para proteger sus claves y datos de funcionamiento (Ej. PIN, contraseñas y claves compartidas). También describe otros controles de seguridad técnica usados por la CA emisora para realizar de forma segura sus funciones. Los controles técnicos incluyen la seguridad del ambiente de desarrollo de software y controles de seguridad operacional. Posee los siguientes subcomponentes:

- Instalación y generación del par de claves. Describe: Quién genera el par de claves de la entidad; Cómo la clave privada se proporciona de forma segura a la entidad; Cómo se provee la clave pública de la entidad a los usuarios; Si la generación de la clave desarrollada es en software o hardware; Para qué propósito puede ser usada la clave.
- Protección de la clave privada. En este subcomponente se describe: Los estándares requeridos para el módulo usado en generar las claves; Si está la clave privada bajo el control de múltiples personas; Si la clave privada está custodiada; Si está respaldada; Quién puede usar la clave privada; Cuáles son los periodos de uso.
- Controles de desarrollo de sistemas. Estos incluyen la seguridad del personal de desarrollo, prácticas de ingeniería de software, uso de técnicas de diseño e implementación tolerante a fallas y seguridad de las instalaciones de desarrollo.
- Controles de Seguridad de Red. Dirige controles relacionados con la seguridad de la red incluyendo el uso de cortafuegos.

VII **Descripción de Certificados y CRL.** Es utilizado para especificar el formato de los certificados y las CRL, asumiendo el uso del formato de certificados y CRL X.509, esto incluye información sobre perfiles, versiones y extensiones utilizadas. Tiene dos subcomponentes:

- Perfil de Certificados. Dirige asuntos como los siguientes: Número de versión soportada; Valor de las extensiones y que tan críticos son; Identificadores del objeto Algoritmos Criptográficos; Restricciones de nombres usados; Identificadores del objeto Política de Certificación, etc.
- Perfil de la CRL. Este dirige asuntos como: Número de versión soportado por la CRL; Valores de la CRL y de sus extensiones y la definición de si son críticas o no.

VIII **Especificaciones de Administración.** Es usado para especificar como serán mantenidos los CPS. Contiene los siguientes subcomponentes:

- Procedimientos de Cambio de Especificaciones. Ocasionalmente será necesario cambiar las CP y los CPS, algunos de estos cambios no reducirán la confianza que una CPS provee pero será juzgado por el administrador de políticas si la aceptabilidad de los certificados no cambia.
- Procedimientos de Notificación y Publicación. Contiene los siguientes elementos: Lista de componentes que existen pero que no son hechos públicos y finalmente, Descripciones de mecanismos usados para distribuir la CP o CPS incluyendo controles de acceso sobre la distribución.

6.8 Despliegue

La etapa final en la metodología implica la instalación y validación operacional de la PKI, verificando además la correcta integración entre los distintos elementos que la componen. Una revisión y pruebas de penetración pueden ser necesarias para asegurar que la implementación mantiene todos los requerimientos de seguridad.

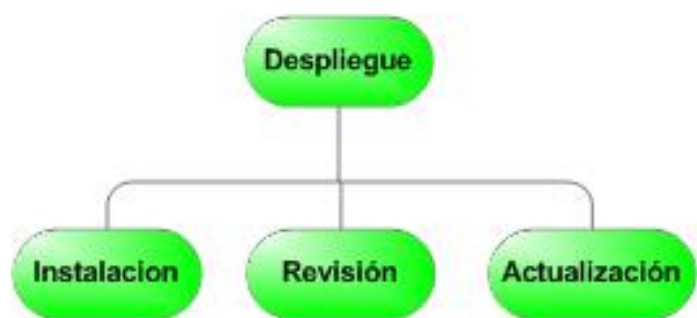


Figura 33: Principales pasos para el despliegue.

6.8.1 Instalación

Una vez completada la planificación de la PKI se debe comenzar su instalación, por lo que podría ser conveniente realizar este proceso por fases:

- **Selección**

Se evalúan distintas soluciones PKI por su capacidad para acomodarse al número de usuarios, tipos de certificados a emitir, la capacidad de los administradores para entender el software, y todos los otros aspectos definidos principalmente durante la toma de requerimientos y definición de arquitectura de la metodología.

▪ **Instalación**

Se configura el sitio seguro para la CA y RA (si se está usando una), éstas se instalan, configuran y ponen a prueba, así también los directorios y las bases de datos. Una parte fundamental de la instalación de la CA y RA será la generación y almacenamiento de sus propias claves para la firma de los certificados y solicitudes.

Adicionalmente se debe documentar cada uno de los pasos involucrados en la instalación de los servicios PKI, incluyendo los procedimientos para instalar, configurar, respaldar y restaurar la CA y RA.

6.8.2 Revisión

En el proceso de revisión se asegura que se han diseñado los sistemas de manera correcta para las necesidades de la organización.

Una fase piloto o de pruebas ayudaría a la organización a obtener experiencia en la operación de la PKI antes de una instalación completa. En esta fase, se deben emitir certificados a un grupo pequeño de usuarios, quienes deben instalar, configurar y usar una aplicación PKI.

La retroalimentación que estos usuarios proporcionen será de mucho valor para encontrar problemas potenciales. La respuesta que se observe de ellos será un indicador de la facilidad con que se podrá adoptar la PKI.

El grupo de administradores puede también probar reinstalar los servidores, mientras los usuarios pueden recibir una capacitación que les ayude a entender y usar las aplicaciones PKI.

En la etapa de pruebas se necesitará determinar por ejemplo:

- Si la PKI puede ser manejada eficiente y fácilmente.
- Si se puede restaurar por completo.
- Si ínteropera exitosamente con otras PKI.
- Si los usuarios pueden solicitar cada tipo de certificado definido.
- Si se verifica correctamente la validez de los certificados.
- Si los servidores Web y otras aplicaciones son capaces de utilizar PKI.
- Si se puede renovar un certificado de forma eficiente, etc.

De forma adicional para el proceso de revisión de los sistemas, las organizaciones pueden emplear un equipo especial de seguridad para realizar ataques simulados sobre sus redes, para descubrir y corregir debilidades antes que ataques reales tengan la oportunidad de explotar estas falencias.

La información que se obtenga de todas estas pruebas eventualmente puede requerir un cambio en la PKI como puede ser actualizar o agregar un sistema, aplicación o hardware para acomodarse a nuevas versiones o incrementar el rendimiento.

6.8.3 Actualización

Todos los sistemas son propensos a cambios y una PKI no es la excepción. Sin embargo, esto requiere una cuidadosa administración ya que una PKI en operación involucra varios sistemas críticos, distribuidos a través de múltiples sitios y que generalmente deben estar en constante operación, por esto se debe tener en mente un plan adecuado de posibles migraciones, lo que puede definir horarios de

actualizaciones, tiempo máximo de duración de éstas, esquemas de reemplazo de funciones, etc.

Para finalizar el proceso de despliegue, se debe considerar el soporte que un grupo de personas dentro de la organización debe asumir. Se debe definir el lugar donde se ubicará el grupo de soporte de manera que pueda ser accesible por usuarios que necesiten ayuda inmediata, también se debe definir el número de personas que se necesitarán para realizar estas funciones.

CAPITULO VII

DISEÑO PROTOTIPOS PKI

7.1 Preámbulo

El presente capítulo se centra en describir el análisis y diseño de los prototipos PKI a desarrollar, para esto define las funcionalidades y restricciones básicas de los sistemas con el objetivo de delimitar sus acciones.

El objetivo del capítulo es que con la información obtenida y la posterior implementación se pueda obtener conclusiones basados en la experimentación de la tecnología y no solamente en las definiciones teóricas encontradas a lo largo de la investigación, con lo que se podrá realizar una demostración empírica de la solución propuesta al problema de seguridad planteado en el comienzo de este trabajo de tesis.

7.2 Diseño Prototipo Autoridad Certificadora

Esta sección presenta decisiones acerca de cómo se va a implementar el prototipo de CA y se compone de una toma de requerimientos o definición de funcionalidades del sistema, la descripción de las características de los componentes involucrados en éste y la identificación de los datos utilizados junto con los cambios que éstos sufren durante la ejecución de las funcionalidades.

7.2.1 Ámbito

El ámbito específico de este prototipo corresponde al desarrollo de una autoridad de certificación para la implementación de una PKI. Esta Autoridad

Certificadora permitirá principalmente la emisión, validación y publicación de certificados y lista de revocación para apoyar los servicios que presten los prototipos de aplicaciones que se describen más adelante en este capítulo.

El ámbito del prototipo quedará restringido a sólo la CA, ya que se considera ésta como suficiente para probar la tecnología PKI. Además aumentar el número de CA para un prototipo no tiene mayor sentido, ya que la cantidad de usuarios será limitada, hacer esto también aumentaría los requerimientos de administración de confianzas, validación de caminos de certificación y necesidades de hardware, entre otros, lo que está demás para efectos demostrativos.

Por los mismos motivos se deja fuera del ámbito la construcción de un CPS ya que la definición de tal documento requiere un estudio acabado de las necesidades reales de una organización.

7.2.2 Requerimientos

A continuación se describen las principales funcionalidades que debería tener el prototipo de CA. Esto indica solamente lo que hay que implementar y no como se debe hacer.

- La CA debe ser manejada por una persona que cumpla las funciones de administrador y que apruebe todos los procesos realizados por la CA.
- La CA debe poder generar un par de claves para sí misma, con las cuales firmar los certificados para los usuarios. La clave privada de la CA deberá estar protegida con una contraseña y en un formato adecuado para su seguridad.
- El certificado de la CA deberá estar autofirmado.

- La CA debe poder generar un par de claves para los usuarios y debe poder mantener un registro de los usuarios certificados.
- La CA debe poder emitir certificados digitales tanto para usuarios personas como para servidores Web.
- Los certificados y las claves de usuarios deberán almacenarse en un formato transportable y protegido por una contraseña para hacerlos llegar a sus titulares.
- La CA debe poder revocar un certificado digital y su clave asociada.
- La CA debe poder publicar una CRL para que los usuarios establezcan la validez de los certificados digitales.
- La CA debe poder almacenar los certificados en un repositorio, ya sea subdirectorio o base de datos.
- La CA debe poder visualizar los certificados que emite, así como las CRL.
- La CA debe mantener un esquema de seguridad para no permitir que cualquier persona distinta al administrador pueda tomar control de ella.
- La CA debe mantener un archivo que registre todas las actividades realizadas por el administrador y que garantice la integridad de la información registrada.



Figura 34: Funcionalidades prototipo CA.

7.2.3 Restricciones

A continuación se establecen algunas restricciones para el prototipo:

- El modelo de confianza estará restringido a una única CA raíz que emita los certificados a los usuarios.
- Las claves para la CA serán de 2046 bits, privilegiándose la seguridad antes que el tiempo de procesamiento requerido para generar las claves, el algoritmo utilizado será el RSA ya que eventualmente necesitará comunicarse con otra entidad y se deberá cifrar tales comunicaciones.
- Las claves de los usuarios deben ser creadas con el algoritmo RSA y el tamaño de las claves será de 1024 bits.
- Los usuarios pueden ser de tipo Personal u Organizacional, y Servidores Web que necesiten realizar comunicaciones SSL, para éstos últimos se debe aceptar una solicitud de certificados bajo el estándar PKCS #10 ya que el par de claves no será generado por la CA.

- Los campos que contendrán los certificados personas serán: Nombre, rut, ciudad, región y país en el caso tipo Personal y en el caso tipo Organizacional serán los mismos acompañados con el nombre de la organización y el área de desempeño. En el caso de los servidores se acepta la información que viene en la solicitud bajo el formato PKCS #10.
- Los certificados deben ser generados bajo el formato X.509v3, para su interoperabilidad con las aplicaciones y otras PKI.
- Los campos opcionales de los certificados que se utilizarán son: uso de clave y uso de certificado.
- Las firmas de los certificados emitidos y de las solicitudes de servidor aceptadas deberán ser verificadas antes de la aceptación de éstos.
- Se debe generar un archivo PKCS #12 para que los usuarios puedan importar los certificados y sus claves a cualquier aplicación, navegador o cliente de correo.
- Las CRL deben contar con la causa de revocación de los certificados en ella mencionados.
- Los procedimientos de identificación y autenticación real de los usuarios así como la verificación de la información de una solicitud de revocación de certificados queda fuera del prototipo ya que esto requiere recursos adicionales. Por lo que en los procesos de simulación se considerará la información proporcionada como real.
- No habrá restricciones de espacio en disco ya que el prototipo sólo emitirá una cantidad limitada de certificados.

7.2.4 Modelo Estático

En esta sección se presenta un modelo sin flujo de información de los componentes del sistema para tener una definición clara de los actores involucrados.

Como muestra el esquema, el sistema estará compuesto por los usuarios o solicitantes de certificación, el prototipo de aplicación CA, una base de datos donde se almacenará información de los usuarios y sus certificados y un repositorio donde se publicarán los certificados y listas de revocación.



Figura 35: Modelo estático prototipo CA.

▪ **Los usuarios**

Son los propietarios de las claves y titulares de certificados. Proporcionan información para completar los campos correspondientes de los certificados digitales y la base de datos de la CA. Se aceptan tres tipos de usuarios Personal, Organizacional y servidor.

Función	Descripción – Formato
Solicitar Certificación Tipo Personal.	Inicia certificación de identidad digital, debe adjuntar información para certificación en persona. Nombre, rut, ciudad, región, país.
Solicitar Certificación Tipo Organizacional.	Inicia certificación de identidad digital, debe adjuntar información para certificación en persona. Nombre, rut, ciudad, región, país, unidad organizacional, organización.
Solicitar Certificación Tipo Servidor.	Inicia certificación de identidad digital, debe adjuntar archivo para certificación en persona. PKCS #10.
Solicitar Revocación.	Permite dar aviso de certificado no valido, debe adjuntar información mediante correo, teléfono o personalmente. Nombre, N° serie certificado, causa revocación.

Tabla 14: Descripción actor usuarios.

▪ La CA

Es manejada por el administrador y autentifica información de solicitudes de los usuarios, genera claves y las asocia a los solicitantes emitiendo el certificado digital correspondiente que almacena en su base de datos y que posteriormente publica a un subdirectorío donde publica también las CRL.

Función	Descripción – Formato
Generar Claves CA.	Crea par de claves propias de la CA que utiliza para firmar los certificados y CRL que emite. RSA 2048 bits.
Generar Claves Usuario.	Crea par de claves para usuarios. RSA 1024 bits.
Emitir Certificado.	Crea certificados digitales con información del solicitante y de sus claves, depende del tipo de solicitud. Formato X.509 V3.
Revocar Certificado	Cambia estado de certificado en la base de datos a no valido para agregarlo a una futura CRL.
Publicar CRL.	Crea archivo con lista de certificados no válidos y lo deposita en un subdirectorío. Formato X.509 V2, con información de causa de revocación.
Publicar Certificado.	Crea archivo de certificado y lo deposita en un subdirectorío Formato x.509 V3 en codificación binaria.
Exportar Claves.	Crea un archivo protegido por contraseña que contiene claves de usuario y certificado. Formato PKCS #12.

Tabla 15 : Descripción actor CA.

- **Las claves**

Números relacionados matemáticamente que permiten firmar y cifrar mensajes. Estas son solicitadas a la CA por los usuarios, la autoridad luego de la validación de identidad de los solicitantes las crea y entrega junto con un certificado en un archivo protegido por una contraseña. Para el caso de las solicitudes de servidor las claves no son generadas por la CA.

- **Los certificados**

Documentos que identifican al dueño de un par de claves dentro de un periodo establecido en el certificado. Son emitidos por la CA y pueden ser revocados. La información que contienen depende del tipo de solicitud que haya hecho el usuario. En el caso del certificado para servidores la información viene almacenada en el archivo de solicitud PKCS #10.

- **Las CRL**

Archivo que contiene una lista de certificados no válidos por causa establecidas en una solicitud de revocación. Es publicada por la CA cada cierto tiempo a criterio del administrador.

7.2.5 Modelo Funcional

Este modelo tiene el objetivo de visualizar la dinámica del proceso de certificación de los usuarios y organizar que es lo que hace cada parte en el sistema, muestra la interrelación a alto nivel de los componentes principales del prototipo y el flujo de información entre las funcionalidades.

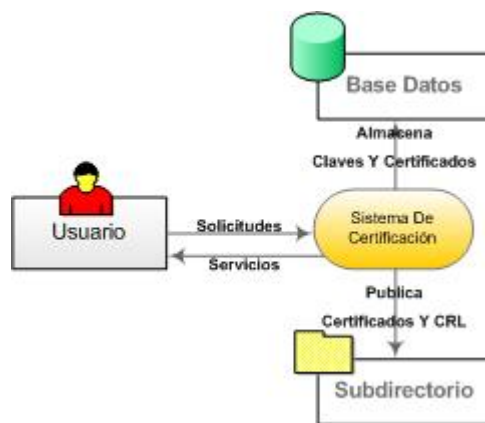


Figura 36: Modelo funcional prototipo CA.

En este modelo se puede ver el esquema funcional más básico del sistema. En él, los usuarios realizan solicitudes al sistema de certificación que luego de la aprobación del administrador serán completadas o denegadas.

A continuación este primer modelo se ira descomponiendo para reflejar en detalle el comportamiento del prototipo y proporcionar la suficiente información para su construcción.

Los procesos de “Verificar Solicitud Certificación” y “Verificar Solicitud Revocación” no se detallaran por las especificaciones planteadas en el ámbito del prototipo.

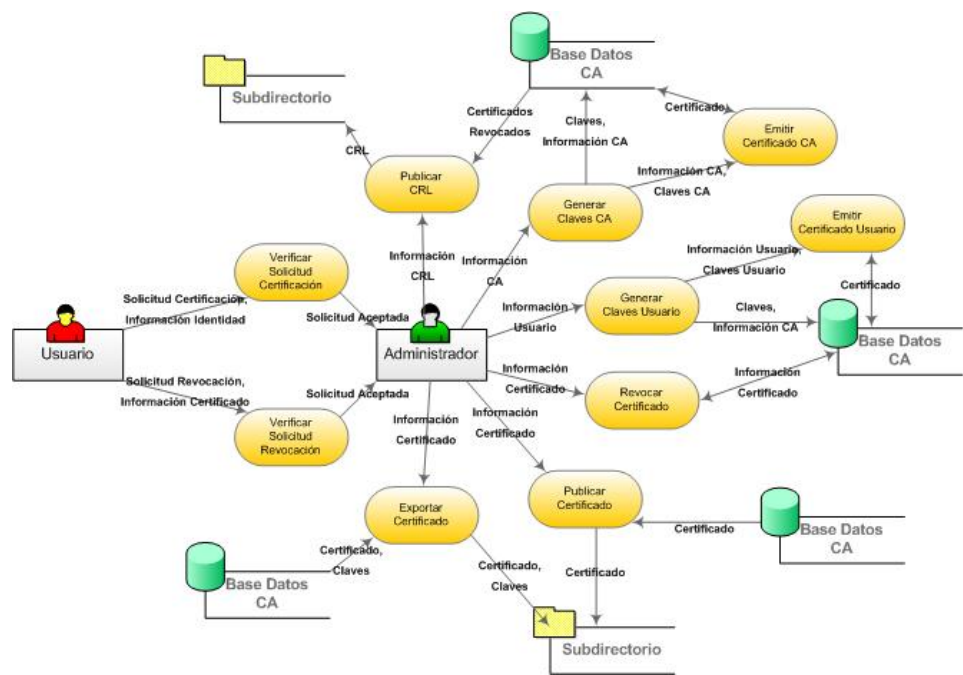


Figura 37: Descomposicion funcionalidades prototipo CA.

▪ Proceso Generar Claves CA

Este proceso permite generar el par de claves con que la CA firmará los certificados de los usuarios. La clave privada será protegida con una contraseña por seguridad y será almacenada en un archivo o en la base de datos de la CA, el proceso debe quedar registrado en un archivo de eventos para su posterior auditoria.

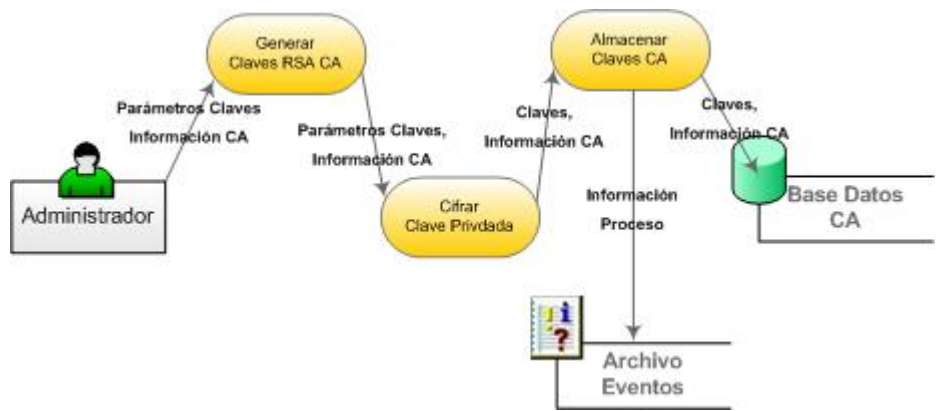


Figura 38: Proceso Generar Claves CA.

▪ **Proceso Emitir Certificado CA**

Este proceso almacena información de la CA y su clave pública en un archivo de certificado bajo el formato X.509 v3 y posteriormente autofirma el certificado. Para corroborar la validez del certificado realiza una verificación de su firma para luego almacenarlo en la base de datos y dejar un registro del proceso en un archivo de eventos.

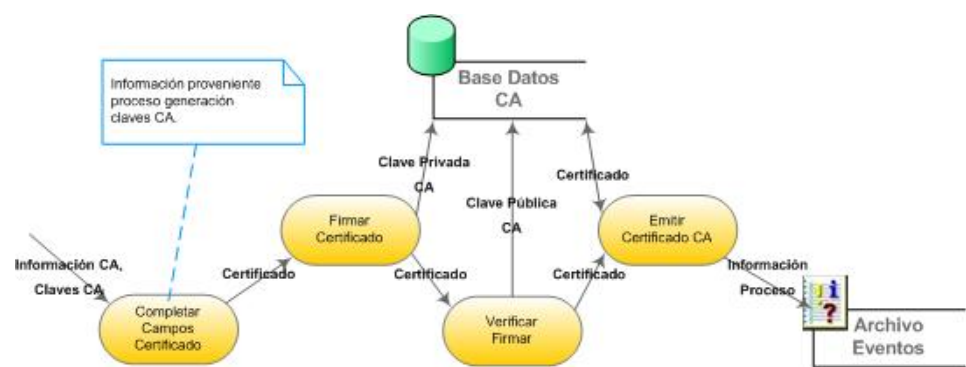


Figura 39. Proceso Emitir Certificado CA.

▪ **Proceso Generar Claves Usuario**

Este proceso se realiza al aceptar una petición de certificación de un usuario y permite la generación de las claves RSA de éste, estas claves son almacenadas en la base de datos de la CA, y para finalizar el proceso se registra en un archivo de eventos.



Figura 40: Proceso Generar Claves Usuario.

▪ **Proceso Emitir Certificado Usuario**

Este proceso se expande del proceso Generar Claves Usuario y almacena información de la identidad del usuario y su clave pública en un archivo de certificado bajo el formato X.509 v3, luego busca la clave privada de la CA y firma el certificado. Para garantizar la firma del certificado se realiza una verificación con la clave pública de la CA para luego almacenarlo en la base de datos y dejar un registro del proceso en el archivo de eventos.

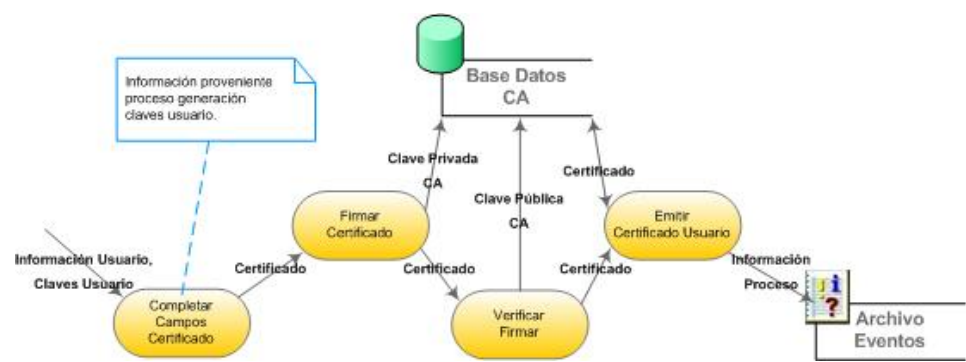


Figura 41: Proceso Emitir Certificado Usuario.

▪ **Proceso Publicar Certificado**

Este proceso permite almacenar el certificado ya sea de la CA o de los usuarios en un archivo físico para que pueda ser enviado a un repositorio público donde ser consultado.

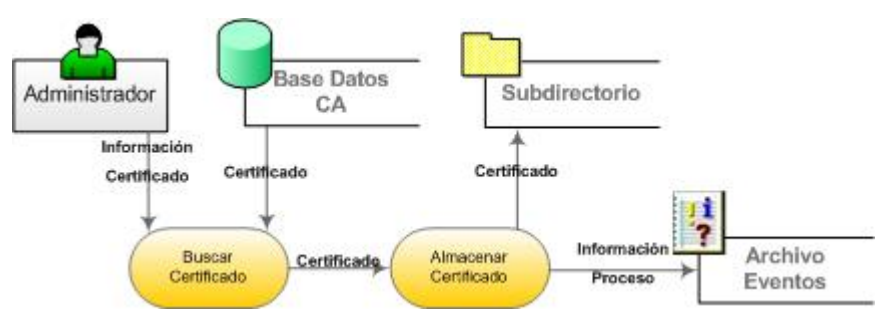


Figura 42: Proceso Publicar Certificado.

▪ **Proceso Exportar Certificado**

Este proceso crea un archivo de transporte bajo el estándar PKCS #12 en el que se almacenan las claves del usuario y su certificado, protegidos por una contraseña. Este archivo es almacenado en un directorio de la CA para ser luego enviado al titular del certificado, finalmente el proceso se registra en el archivo de eventos.



Figura 43: Proceso Exportar Certificado.

▪ **Proceso Revocar Certificado**

Este proceso se realiza al aceptar una solicitud de revocación de un usuario y cambia el estado de un certificado, de valido a revocado en la base de datos de la CA. El proceso se registra en el archivo de eventos.



Figura 44: Proceso Revocar Certificado.

▪ **Proceso Publicar CRL**

Este proceso se genera cada cierto tiempo configurado en la CA o bien por disposición del administrador, y permite generar un archivo con la lista de todos los

certificados con el valor del campo “Estado” igual a “Revocado” dentro de la base de datos de la CA. El proceso se registra en el archivo de eventos.

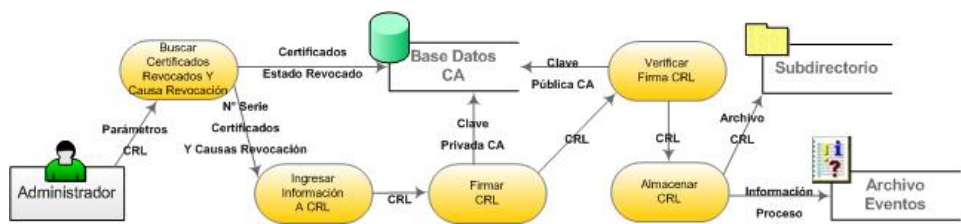


Figura 45: Proceso Publicar CRL.

7.3 **Diseño Prototipo Autenticador de Documentos Electrónicos**

Esta sección representa decisiones acerca de cómo se va a implementar el prototipo autenticador de documentos electrónicos. Se compone de una toma de requerimientos o definición de funcionalidades, la descripción de las características de los componentes involucrados y una representación de los cambios que sufren los datos al ser manipulados por las funcionalidades.

7.3.1 **Ámbito**

El ámbito de este prototipo corresponde al desarrollo de una aplicación que permita a los usuarios de la PKI utilizar los certificados digitales emitidos por la Autoridad Certificadora prototipo, y poder de esta manera intercambiar documentos electrónicos de forma segura mediante la firma y cifrado de éstos. La forma en que los usuarios intercambian los archivos queda fuera del ámbito de esta aplicación.

7.3.2 **Requerimientos**

El prototipo debe permitir a los usuarios básicamente dos cosas: la firma de documentos para garantizar su autenticidad y el cifrado de éstos para mantener la confidencialidad. Estas actividades deben hacer uso de los certificados digitales emitidos por la CA prototipo.

Las funcionalidades son entonces:

- Generación de firmas digitales sobre documentos electrónicos.
- Verificación de las firmas digitales.
- Cifrado de los documentos electrónicos.
- Descifrado de documentos electrónicos.



Figura 46: Funcionalidades prototipo Autenticador documentos electrónicos.

7.3.3 Restricciones

- La aplicación debe firmar documentos de texto y archivos de aplicación ejecutables.
- Debe permitir al usuario buscar de forma sencilla los archivos a firmar y cifrar.
- Debe poder visualizar los documentos de texto antes de firmarlos.
- Debe poder utilizar las claves y certificados emitidos por la CA prototipo.
- Debe poder visualizar un certificado antes de utilizarlo.
- Debe verificar que el archivo no esté ya firmado.

7.3.4 Modelo Estático

En esta sección se describirán cada uno de los actores involucrados en la aplicación de autenticación de documentos electrónicos.

- **El Usuario**

Es el ente que utilizará la aplicación y proporcionará las rutas a los archivos sobre los que se realizarán las acciones implementadas en la aplicación.

- **El Autentificador**

Es el prototipo de aplicación encargado de la firma, cifrado, verificación de firma y descifrado de los archivos digitales.

- **El Almacén de Certificados**

Este almacén corresponde al que utiliza el sistema operativo Windows para resguardar certificados y claves, y al que antes de utilizar el Autentificador se deben importar el certificado y claves del Usuario, los que han sido exportados por la CA en un archivo bajo el formato PKCS #12 después de la certificación de éste.

- **El subdirectorio**

Corresponde al directorio en el computador del usuario donde se almacenan los documentos generados por los procesos de firma y cifrado.

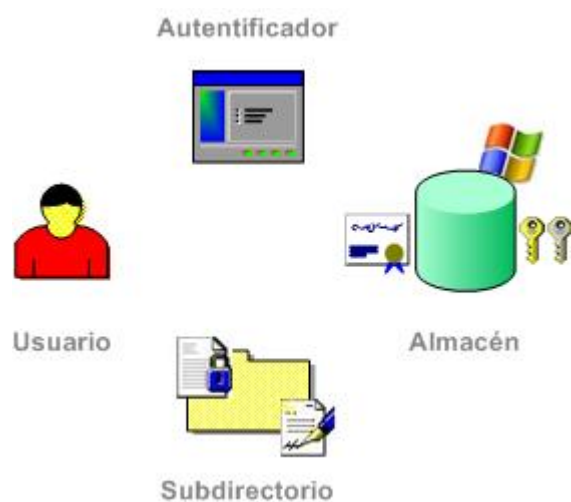


Figura 47: Modelo estático prototipo Autenticador documentos electrónicos.

7.3.5 Modelo Funcional

Esta sección describe mediante distintos diagramas el funcionamiento del prototipo para la autenticación y cifrado de documentos electrónicos.

Para comenzar se muestra un primer esquema con la descripción más básica del sistema, en él un usuario interactúa con la aplicación activando sus respectivas funcionalidades.

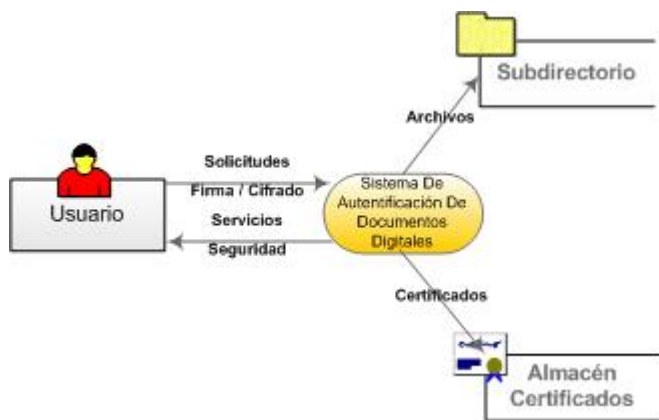


Figura 48: Modelo funcional prototipo Autenticador documentos electrónicos.

Al descomponer este primer modelo se observa que:

El usuario solicita a la aplicación la firma o cifrado de mensajes de texto o archivos de código, ante lo cual la aplicación busca en el almacén de certificados una clave privada o pública respectivamente con la cual realizar el proceso solicitado.

Si encuentra una clave apropiada para el caso, realiza el proceso generando un nuevo archivo firmado o cifrado que es almacenado en un subdirectorio de la maquina del usuario para su posterior intercambio.

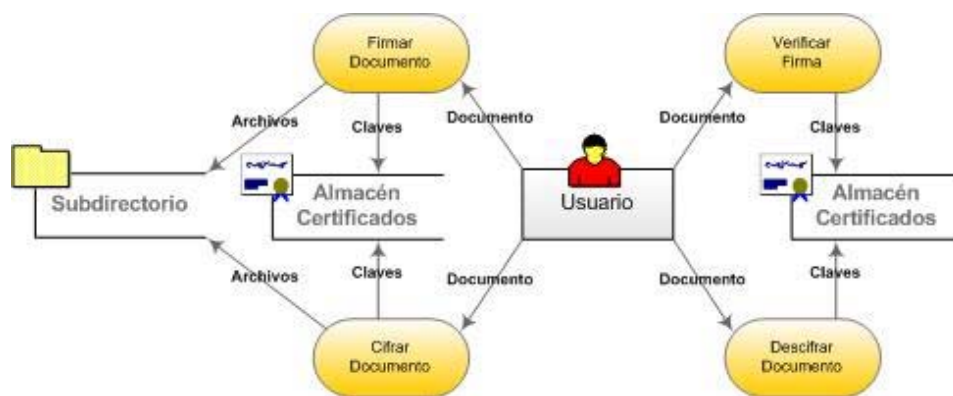


Figura 49: Descomposición funcionalidades prototipo Autenticador.

Adicionalmente el usuario puede solicitar la verificación de una firma o el descifrado de un documento, para lo cual el prototipo busca una clave pública o una privada, según sea el caso, en el almacén de certificados para realizar el proceso requerido.

A continuación se descomponen cada una de las funcionalidades del prototipo desglosadas del primer modelo:

- **Proceso de firma**

Este proceso permite al usuario firmar archivos electrónicos, para lo cual requiere que el usuario proporcione un archivo a firmar, el que se visualiza para

conocimiento del usuario. Antes de la firma, se verifica que el archivo no esté ya firmado, ante lo cual se podría generar un mensaje de error. De no ser así la aplicación busca en el almacén una clave válida para el proceso de firma, si no la encuentra generará un mensaje de error. Si no se han generado errores la aplicación procede a la firma del documento con la clave.

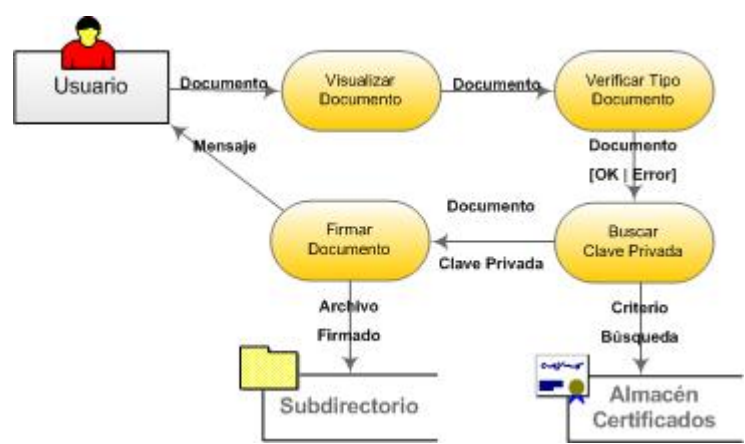


Figura 50: Descomposición firma documento.

▪ Proceso verificación de firma

El proceso de verificación de firma requiere que el usuario proporcione un archivo firmado en un formato correcto, si éste concuerda con el formato el prototipo busca una clave pública en el almacén con que verificar la firma. El formato para los archivos de texto debe ser: Mensaje + CR/LF + “----INICIO FIRMA---”.

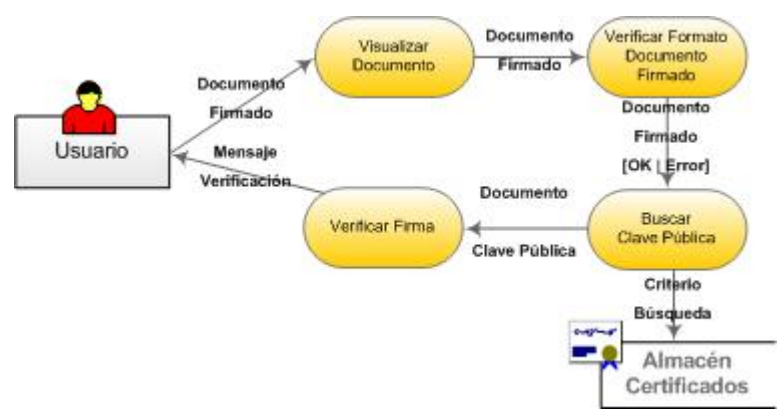


Figura 51: Descomposición verificación firma documento.

▪ **Proceso de cifrado**

Este proceso requiere un archivo que opcionalmente puede estar firmado, una vez seleccionado el archivo la aplicación permitirá escoger los destinatarios del archivo cifrado o sea quienes tendrán las claves privadas que podrán descifrarlos. Realizado esto la aplicación utiliza un algoritmo y clave predeterminados para cifrar el documento, esta clave es cifrada con la clave pública de los destinatarios con lo que se generará un nuevo archivo que se almacenará en un subdirectorio de la maquina del usuario.

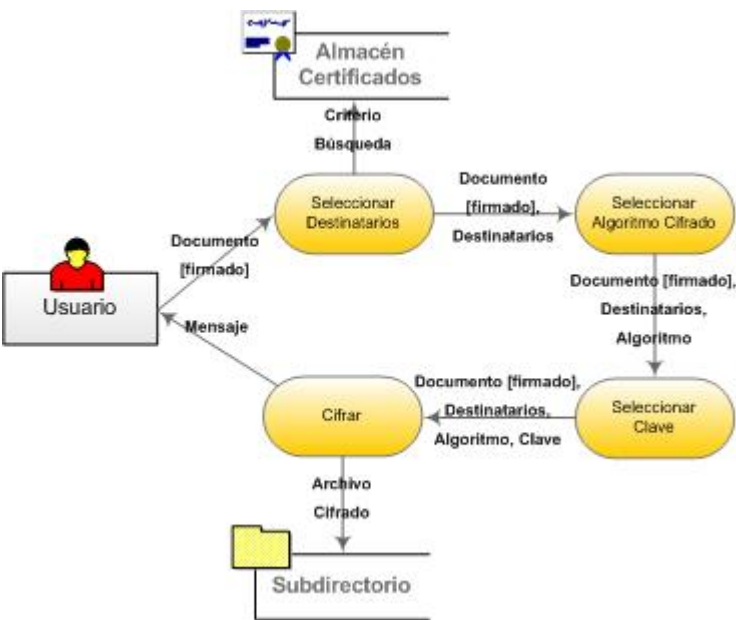


Figura 52: Descomposicion cifrado de documento.

▪ **Proceso de descifrado**

El proceso de descifrado utiliza un documento cifrado y una clave privada que se busca en el almacén de certificados, con esta clave privada se descifra la clave con que fue cifrado el documento completo, posteriormente se procede a determinar el algoritmo con que se cifró el documento. Con todos estos elementos, el documento cifrado, la clave y el algoritmo se procede a descifrar el documento que es almacenado en un nuevo archivo dentro de un subdirectorio.

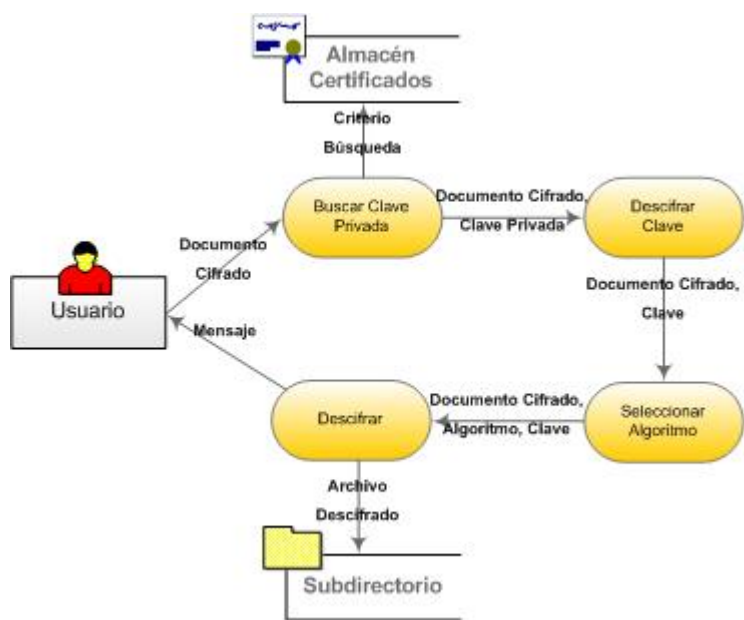


Figura 53: Descomposición descifrado de documento.

7.4 Diseño Prototipo Portal Web Bancario

Esta sección define como implementar un prototipo de portal Web bancario que utilice certificados digitales para firmar transacciones en línea, que permita garantizar la autenticidad de los usuarios y el no repudio de las transacciones electrónicas realizadas. Se compone de la especificación del ámbito del prototipo, una definición de funcionalidades, la descripción de las características de los componentes involucrados y una representación de los cambios que sufren los datos al ser procesados.

7.4.1 Ámbito

El ámbito de la aplicación corresponde al desarrollo de un sitio Web o portal bancario donde se realicen transacciones electrónicas típicas de estas entidades, las que deberán ser firmadas digitalmente por los usuarios o clientes.

De los servicios dentro del portal será suficiente con la implementación de sólo uno, ya el objetivo del prototipo es poder utilizar la firma digital en cualquier

transacción de los clientes, no siendo relevante que servicio la utiliza, ya que para cada uno de estos servicios sólo cambiarán los datos con los cuales se generará la firma.

La forma como se procesan o llevan a cabo las transacciones después de su firma queda fuera del ámbito del prototipo ya que su función no es mostrar todas las actividades involucradas dentro de los servicios bancarios.

7.4.2 Requerimientos

El portal debe permitir una comunicación segura con el cliente, debe poder identificarlo y permitirle realizar transacciones de las que debe quedar un registro firmado digitalmente, además de almacenar los datos con que se procedió a la firma.

Las funcionalidades principales son:

- El sitio Web debe autenticar al usuario mediante certificados digitales.
- El portal debe verificar la validez del certificado digital.
- La aplicación Web debe poder determinar si el usuario identificado tiene permiso para realizar transacciones.
- Realizada la transacción el sitio Web debe firmar digitalmente ésta.
- El portal debe almacenar la firma y los datos de la transacción para garantizar el no repudio por parte del usuario.

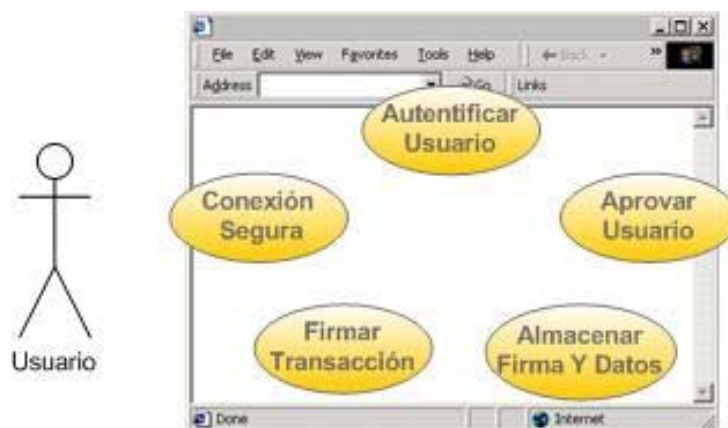


Figura 54: Funcionalidades prototipo Portal Web Bancario.

7.4.3 Restricciones

A continuación se mencionan algunas restricciones para el sistema:

- El usuario debe conectarse vía SSL con el sitio Web de servicios bancarios.
- El usuario debe utilizar un certificado digital de una autoridad de confianza para el sitio Web.
- El portal debe validar el certificado digital contra la ultima CRL de la CA emisora del certificado.

7.4.4 Modelo Estático

En esta sección se describen los actores que participan en el prototipo Web de servicios bancarios.

- **El usuario**

Es el cliente del banco que accede al portal Web y debe autenticarse con un certificado digital para poder realizar movimientos de fondos al interior de éste. Una vez que las realiza debe firmarlas para que se lleve a cabo el proceso completo y garantizar el no repudio.

- **La aplicación Web**

Es el portal bancario conformado por las distintas páginas Web almacenadas en el servidor que se encargan de presentar los servicios u opciones de transacciones al usuario del prototipo.

- **El servidor Web**

Es quien almacena las páginas Web que visualiza el usuario, éste debe tener instalado un certificado digital que permita comunicaciones SSL.

- **El almacén**

Es una base de datos donde está almacenada la información del usuario y donde se almacenan los datos de las transacciones y las firmas digitales de las mismas.



Figura 55: Modelo estático prototipo Portal Web Bancario.

7.4.5 Modelo de Datos

Esta sección muestra los repositorios de información que permiten la permanencia en el tiempo de los datos involucrados en las transacciones del prototipo Web.

La aplicación deberá utilizar una base de datos con al menos tres tablas principales, una en la que se almacene la información de los clientes, otra donde se almacene los datos de las transacciones y la principal para el carácter demostrativo del prototipo que corresponde a la encargada de almacenar los datos generados durante la firma de las transacciones.

▪ **Tabla Clientes**

Almacena información correspondiente a los clientes del banco, es utilizada para validar los datos contenidos en el certificado presentado por el usuario durante su autenticación en el acceso a los servicios del portal Web, más específicamente se valida el rut de éste.

Clientes		
Rut	Texto	
Numero_cuenta	Numérico	
Nombre	Texto	
Direccion	Texto	
Correo	Texto	
Telefono	Texto	
Saldo	Numérico	

Tabla 16: Descripción tabla Clientes.

▪ **Tabla Transacciones**

Es utilizada para almacenar los datos generados durante las transacciones o transferencias de fondos de los clientes o usuarios del prototipo.

Transacciones		
Numero_transaccion	Numérico	
Fecha	Fecha/Hora	
Monto	Numérico	
Cuenta_origen	Numérico	
Cuenta_destino	Numérico	
Banco	Texto	

Tabla 17: Descripción tabla Transacciones.

Asociado a cada una de las transacciones bancarias de los clientes deberá existir un registro almacenando información correspondiente a la firma digital de esta.

▪ **Tabla Firmas**

Es la más importante de las tablas del prototipo, ya que almacena la información generada en el proceso de firma de cada una de las transacciones de los clientes, almacena también los datos que fueron firmados y el certificado utilizado en el proceso.

Firmas		
Numero_transaccion	Numérico	
Datos	Memo	Texto HTML de formularios
Firma	Memo	
certificado	Memo	

Tabla 18: Descripción tabla Firmas.

7.4.6 Modelo Funcional

En esta sección se describe mediante distintos diagramas el funcionamiento y capacidades del prototipo de Portal con servicios bancarios y firma digital.



Figura 56: Modelo funcional prototipo Portal Web Bancario.

Como muestra el modelo, un usuario podrá a través de un portal Web realizar distintos tipos de transacciones relacionadas con sus fondos, las que deberán ser firmadas por éste y almacenadas junto con toda la información de las transacciones en la base de datos del prototipo.

Al descomponer el modelo básico se pueden detectar los principales procesos involucrados dentro del sistema.

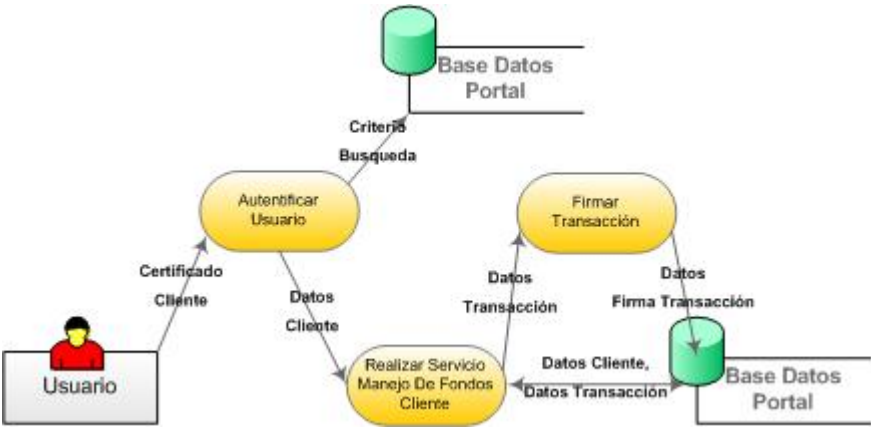


Figura 57: Descomposición funcionalidades Portal Web Bancario.

▪ **Proceso autenticar usuario**

Este proceso es realizado principalmente por el servidor Web, el que se encarga de solicitar un certificado digital al usuario, el certificado debe ser proveniente de una autoridad de confianza y debe contar con la información necesaria, específicamente el rut del usuario, para que el sistema lo lea y pueda validarlo en su base de datos, permitiéndole o no el acceso a los servicios.

Una vez que el usuario proporcione un certificado digital al servidor para su autenticación, este último debe validar el certificado contra la CRL más reciente emitida por la CA garante del certificado digital.

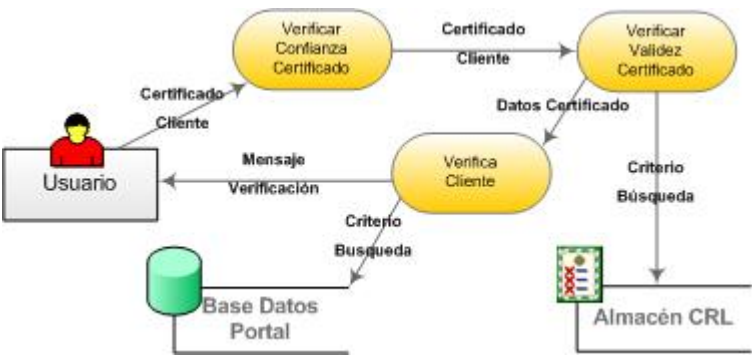


Figura 58: Descomposición autenticar usuario.

Si el proceso se completa satisfactoriamente se le permitirá al usuario el ingreso a los servicios del portal.

▪ **Proceso realizar servicios**

El proceso se ejecuta una vez que el usuario ha sido autenticado, éste se encarga de solicitarle la información necesaria para que pueda utilizar los distintos servicios del sistema, y de guiar la navegación del usuario a través del portal. Adicionalmente verifica los datos proporcionados por el usuario antes de concretar los movimientos de sus fondos.

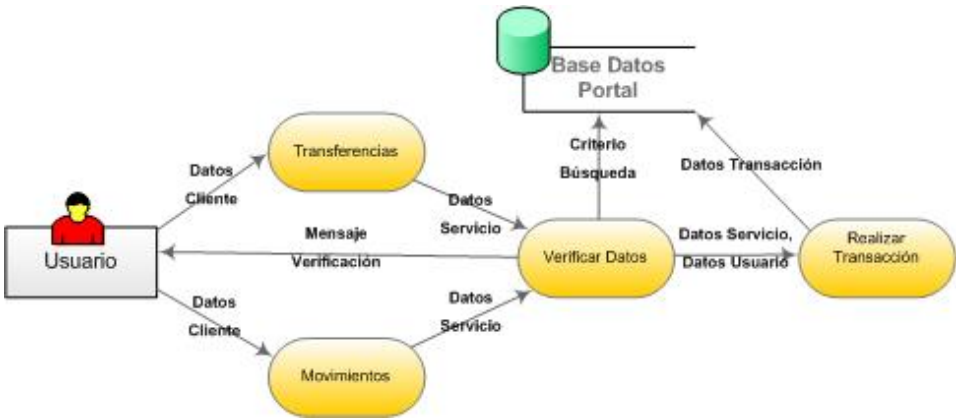


Figura 59: Descomposición realizar servicio.

La figura muestra solo un par de servicios ya que el objetivo del prototipo es demostrar la utilización de la firma digital y no los servicios bancarios.

Finalmente este proceso se encarga de llamar al proceso firmar para garantizar el no repudio de las acciones realizadas en el portal por parte del usuario.

▪ **Proceso firmar**

Este proceso se encarga de solicitar al usuario o cliente un certificado digital válido asociado a una clave privada para poder llevar a cabo el procedimiento de firma.

Para esto se debe solicitar el mismo certificado que utilizó el cliente para autenticarse cuando ingreso al portal Web.



Figura 60: Descomposición firmar transacción.

Una vez que se verifica el certificado se utiliza la clave privada que tenga asociada para firmar los datos proporcionados al servicio por el usuario.

Finalmente se almacenan los datos de las transacciones y las firmas en la base de datos del portal.

CAPITULO VIII

PRESENTACION PROTOTIPOS

8.1 Preámbulo

Este capítulo tiene como función presentar los prototipos diseñados en la sección anterior, para esto se mostrarán las pantallas de sus principales funcionalidades y la descripción de cada una.

8.2 Desarrollo

Para el desarrollo de estos prototipos se decidió buscar en el mercado la existencia de librerías criptográficas que proporcionaran el soporte para las funcionalidades descritas en el capítulo de diseño, ya que el desarrollo de unas propias involucraba un mayor tiempo que el destinado para el proyecto de tesis.

Después de analizar varias librerías tomando en cuenta la disponibilidad de licencias de carácter libre, facilidad de uso, plataforma para la que estaban diseñadas, existencia de documentación apropiada, etc. Se tomo la decisión de utilizar la librería Cryptlib Security Toolkit Versión 3.0 desarrollada por Peter Gutmann, que cuenta con todas las funcionalidades para desarrollar una CA y que es de carácter libre para aplicaciones no comerciales, esta librería se encuentra descrita en el Apéndice E.

Para los prototipos Autenticador de Documentos Electrónicos y Portal Web Bancario, se decidió utilizar la librería Microsoft CAPICOM descrita en el Apéndice F, ya que ésta posee funcionalidades para firmar y cifrar mensajes, además viene

incluida en el sistema operativo Windows y puede también ser utilizada en aplicaciones Web para el navegador IExplorer.

8.3 Recursos utilizados

- **Software**

- Windows 2000 Server, Windows 2000 Professional, Service Pack 2.
- Bases de datos Microsoft Access 2000.
- Microsoft Visual Basic de Visual Studio 6.0 Service Pack 5.0.
- IIS 5.0, Microsoft IExplorer, HTML, CSS, ASP, VBScript, JScript.
- Dreamweaver MX, Fireworks MX.

- **Hardware**

- Pentium III, 700 Mhz, 256 RAM, HD 7,8 GB.
- AMD K6 II 500 Mhz, 256 RAM, HD 2,1 GB.

8.4 Presentación Prototipo CA

La aplicación CA comienza con una pantalla de presentación de la aplicación.



Figura 61: Cuadro presentación prototipo CA.

Siguiendo el esquema de seguridad, la CA no puede ser operada por personas no autorizadas por lo que seguido a la pantalla inicial se muestra un cuadro de dialogo donde el administrador de la CA debe ingresar un nombre de usuario y una contraseña, esta contraseña está almacenada en forma de un resumen o Hash de la contraseña verdadera en la base de datos de la aplicación, por lo que de ser accesada por personas extrañas no podrán descubrir la contraseña real.

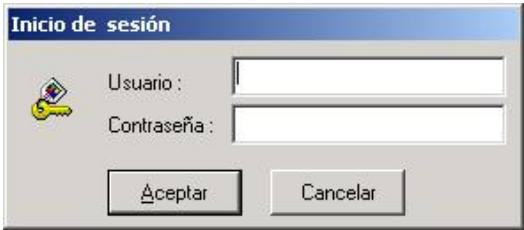


Figura 62: Cuadro inicio de sesión prototipo CA.

De no ser posible la autenticación del administrador se visualizará un mensaje de error y se dará la opción de autenticarse nuevamente.

Una vez autenticado el administrador mediante su contraseña, se visualiza la pantalla principal donde se encuentran todas las funcionalidades de la CA, representadas por una barra de herramientas.

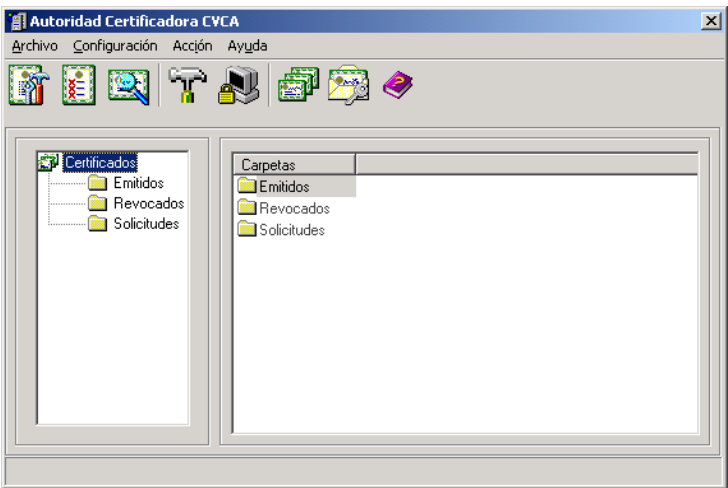


Figura 63: Cuadro administración prototipo CA.

Las funciones se describirán de acuerdo al orden que presentan en la barra de herramientas de la pantalla principal.

La primera que se describirá es la de emisión de certificados. Esta función cuenta con las opciones de emitir certificados a personas comunes y organizacionales, la diferencia está en que el usuario organizacional cuenta con campos adicionales en la cadena que lo identifica y que lo asocia a una organización.

Figura 64: Pantalla emisión certificados persona.

La otra opción es emitir certificados de servidor al aceptar solicitudes bajo el formato PKCS # 10, la información que se solicita es para llevar un registro de quien solicitó el certificado servidor, pues la información del certificado en sí viene en la solicitud de certificación ya mencionada.

The screenshot shows a window titled "Emisión de Certificados" with two tabs: "Personal" and "Servidor". The "Servidor" tab is selected. Under the heading "Información de Identificación", there are several input fields: "Nombre:", "Dirección:", "RUT:", "Ciudad:", "Correo:", "Región:" (with a dropdown menu showing "Primera"), and "Teléfono:". There is also an "Organización:" field. Below these fields is a "Solicitud:" label followed by a large empty text area. At the bottom of the window are two buttons: "Aceptar" and "Cancelar".

Figura 65: Pantalla emisión certificados servidor.

La siguiente función de la CA es la publicación de las CRL, para esto la aplicación busca todos los certificados en su base de datos que aparezcan como “revocados”, con los que completa una lista de certificados revocados. Antes de emitir la CRL la aplicación muestra un mensaje de confirmación de la publicación.

The screenshot shows a dialog box titled "Confirme publicación CRL". It contains a question mark icon and the text: "¿Esta seguro que desea emitir la CRL?" and "La CRL contendra todos los certificados actualmente revocados." At the bottom are two buttons: "Yes" and "No".

Figura 66: Cuadro confirmación publicación CRL.

Otras de las funciones de la CA es buscar certificados en su base de datos de acuerdo a distintos parámetros, esto para facilitar la administración de los certificados, importante cuando el número de certificados es significativo.

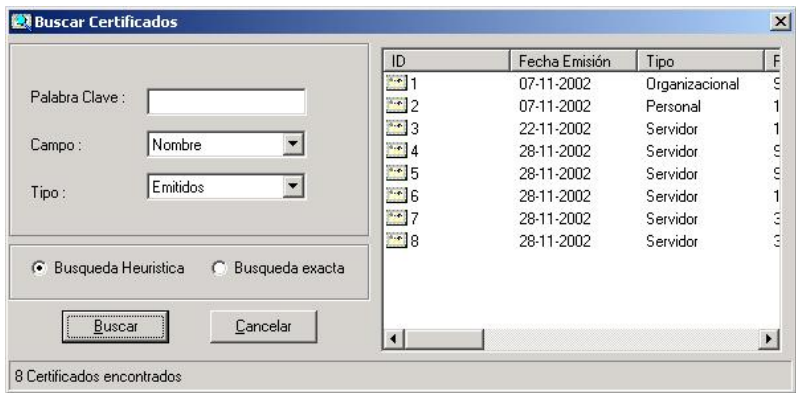


Figura 67: Pantalla búsqueda de certificados.

La CA también cuenta con una opción de bloqueo para mayor seguridad, esto por si el administrador quiere mantener operativa la aplicación mientras está ausente.

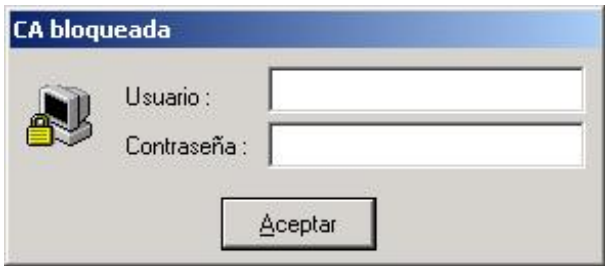


Figura 68: Cuadro bloqueo de aplicación.

La siguiente función corresponde a la publicación en un subdirectorio preestablecido de los certificados emitidos por la CA, éstos se encuentran almacenados en la base de datos de la misma, por lo que mediante esta operación quedan a disposición de los usuarios para su consulta.

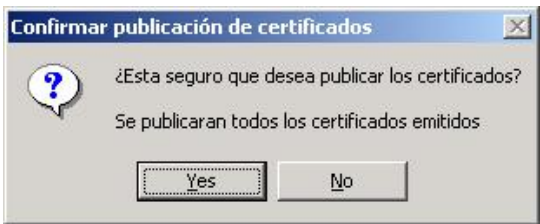


Figura 69: Cuadro confirmación publicación certificados.

Para poder hacer llegar las claves y los certificados a sus respectivos usuarios la aplicación utiliza el procedimiento exportar certificados, para esto almacena claves y certificados en un archivo bajo el estándar de transporte PKCS #12 protegido por una contraseña, lo que permite que sean importados fácilmente a las aplicaciones de los usuarios.

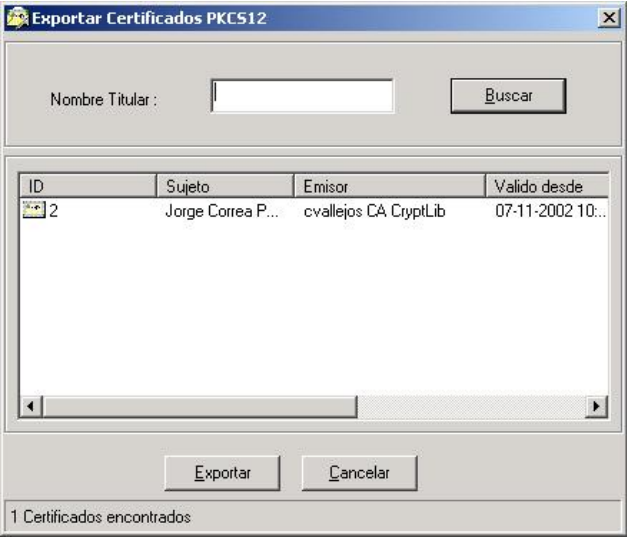


Figura 70: Pantalla exportar certificado y claves a formato PKCS #12.

El prototipo cuenta también con funciones adicionales a las que se presentan en la barra de herramientas representados por menús emergentes definidos según el estado del certificado sobre el cual se están realizando operaciones.

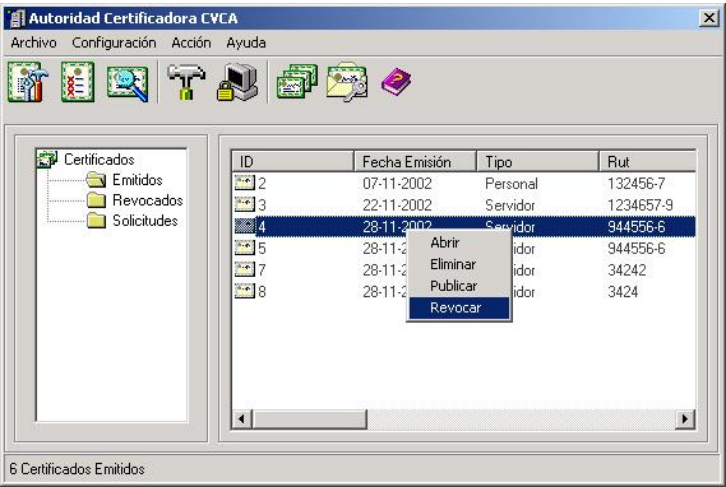


Figura 71: Menú emergente para certificados válidos.

Si los certificados son válidos, éstos se pueden visualizar a través de la opción Abrir del menú emergente.



Figura 72: Resultado Menú Abrir Certificado.

Si se desea eliminar de la base de datos el certificado, se utiliza la opción Eliminar.

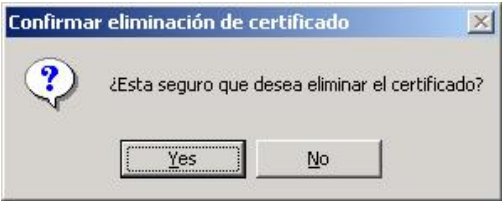


Figura 73: Cuadro confirmación eliminar certificado.

La opción Publicar del menú permite enviar el certificado al subdirectorio predeterminado.

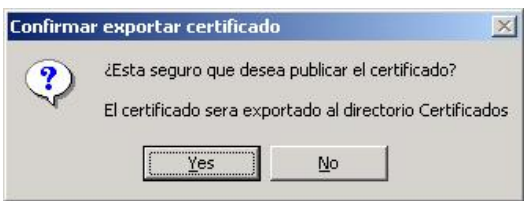


Figura 74: Cuadro confirmación publicar certificado.

Por último, la opción revocar del menú emergente permite cambiar el estado de un certificado dentro de la base de datos de la CA para su posterior inclusión en la CRL. Permite también la especificación de la causa de revocación.

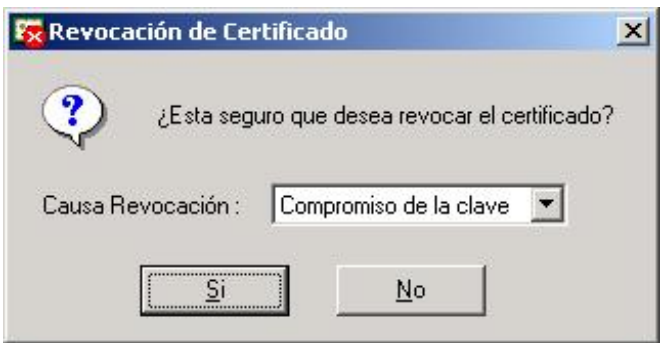


Figura 75: Cuadro revocar certificado y opciones de revocación.

Por otro lado, los certificados revocados también cuentan con algunas opciones en un menú emergente personalizado para ellos. Estos corresponden a Abrir para visualizar el certificado y Eliminar para borrarlo de la base de datos de la CA.

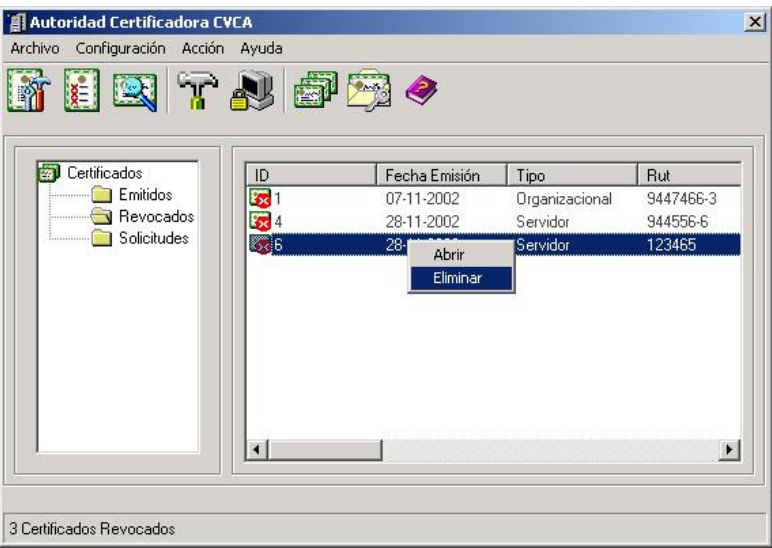


Figura 76: Menú emergente para certificados revocados.

Dentro de los menús de la pantalla principal de la aplicación se encuentran Archivo donde están las opciones de Cerrar y Bloquear la aplicación.

También se encuentra el menú Configuración, donde están las posibilidades de cambio de contraseña de administración de la CA, volver a crear las claves y certificado de la CA y otras opciones de configuración.

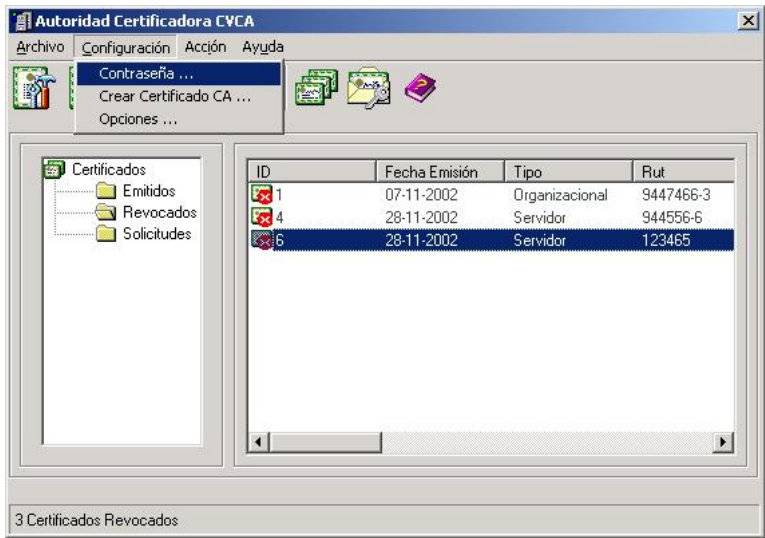


Figura 77: Menú Configuración de la aplicación.

En el menú Acción por su parte se encuentran las mismas funcionalidades ya descritas de la barra de herramientas, además de la opción de ver el archivo de registro de actividades.

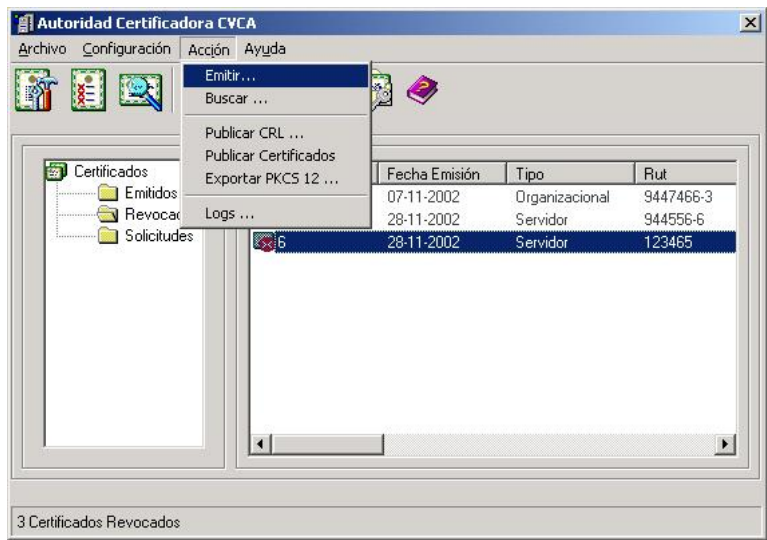


Figura 78: Menú Acción de la aplicación.

Este archivo de eventos mantiene información referente a las actividades realizadas por el administrador de la CA y muestra la hora y la acción que fue realizada.

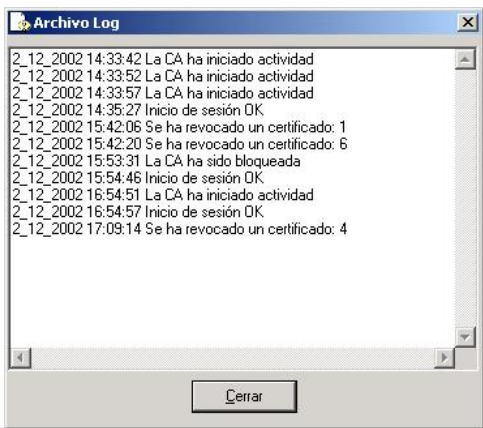


Figura 79: Visualizar archivo de eventos de la CA.

Una vez que la CA termina de operar o sea se selecciona la opción Cerrar del menú Archivo, se despliega un cuadro en el que se solicita una confirmación de si se desea firmar el archivo de las actividades realizadas por el administrador de la CA.



Figura 80: Cuadro confirmación firmar archivo eventos CA.

8.5 Presentación Prototipo Autenticador de Documentos
Electrónicos

Esta sección describe el prototipo desarrollado para probar las funciones de firma, verificación y cifrado de documentos electrónicos por parte de los usuarios de la PKI. Aquí se mostrarán las funcionalidades especificadas en el capítulo de diseño, describiendo cada una de las opciones que el prototipo entrega a los usuarios.

La aplicación comienza con una pantalla de presentación de la aplicación.



Figura 81: Pantalla presentación prototipo autenticador.

Posterior a la presentación el usuario se encuentra con la pantalla principal del prototipo, donde se encuentran las funcionalidades representadas por una barra de herramientas.

La primera opción de la aplicación es poder firmar mensajes de texto, para lo cual el usuario debe seleccionar un documento con tales características.

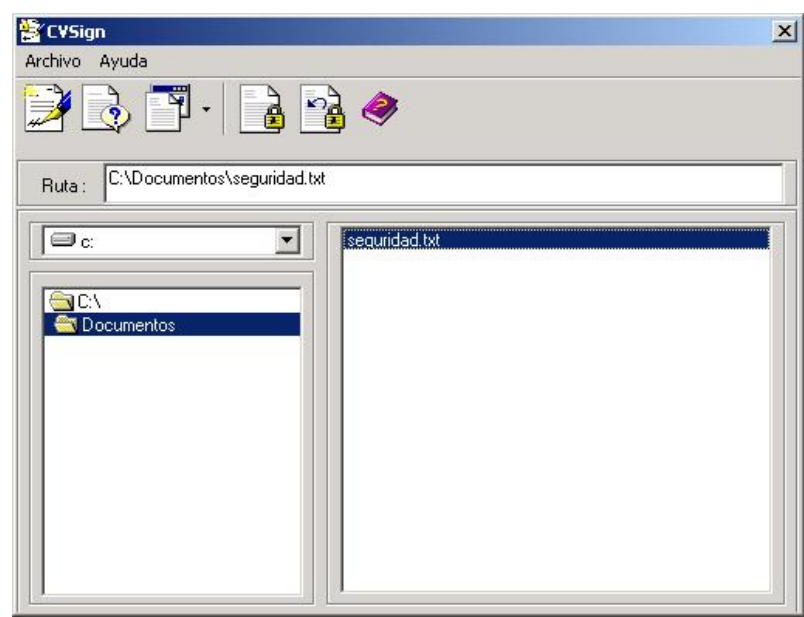


Figura 82: Pantalla principal prototipo autenticador.

Una vez seleccionado el documento la aplicación mostrará al usuario el contenido de éste y la opción de seleccionar si desea firmar el documento o cancelar la acción.

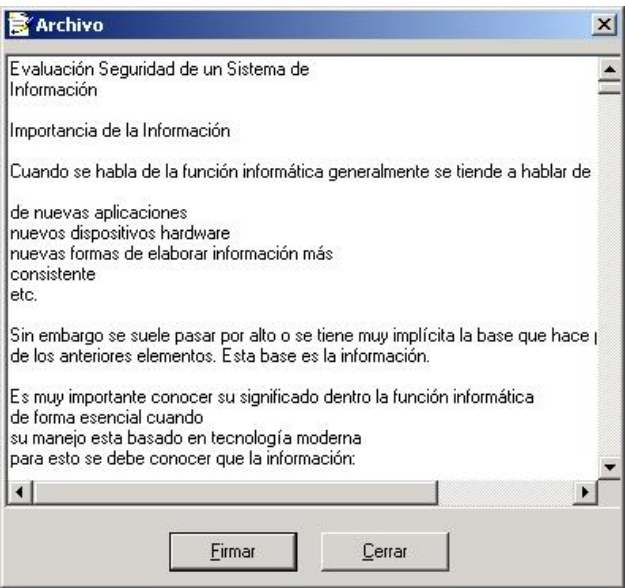


Figura 83: Pantalla presentación de archivo a firmar.

De aceptar firmar el documento, se le solicitará al usuario la elección de un certificado digital con una clave privada asociada para llevar a cabo el proceso.

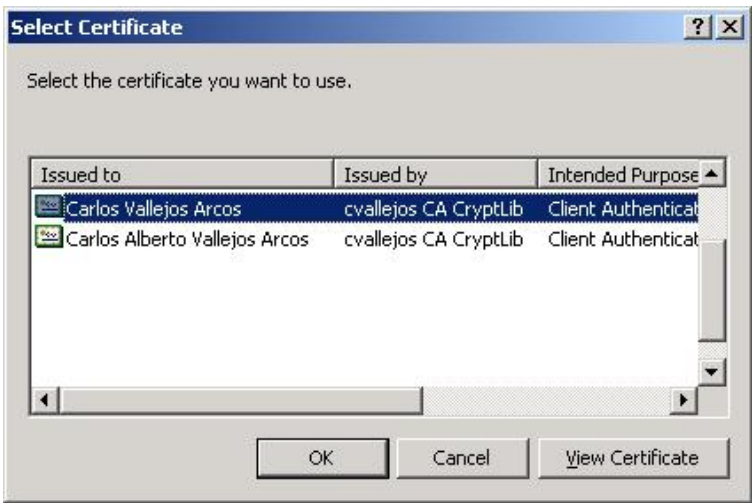


Figura 84: Pantalla de selección de certificado para firma.

De forma adicional, el usuario tiene la opción de ver el certificado antes firmar con la clave privada asociada a éste.



Figura 85: Certificado utilizado para firmar documento.

Si el usuario entonces elige un certificado, el sistema operativo le dará aviso que una aplicación está intentando acceder a su clave privada instalada en el sistema de almacenamiento de certificados de Windows y si da la autorización para que esta acción se lleve a cabo.

Si al importar el certificado con las claves al sistema el usuario las protegió con una contraseña, entonces el cuadro de verificación de acceso a la clave privada solicitará que se ingrese ésta para poder proceder a la firma del documento.



Figura 86: Cuadro confirmación de acceso a clave privada.

Si el proceso se ha realizado con éxito la aplicación despliega un mensaje de proceso finalizado.



Figura 87: Cuadro proceso de firma terminado.

Después de todo este proceso, al documento original se le anexa una firma codificada en formato ASCII.

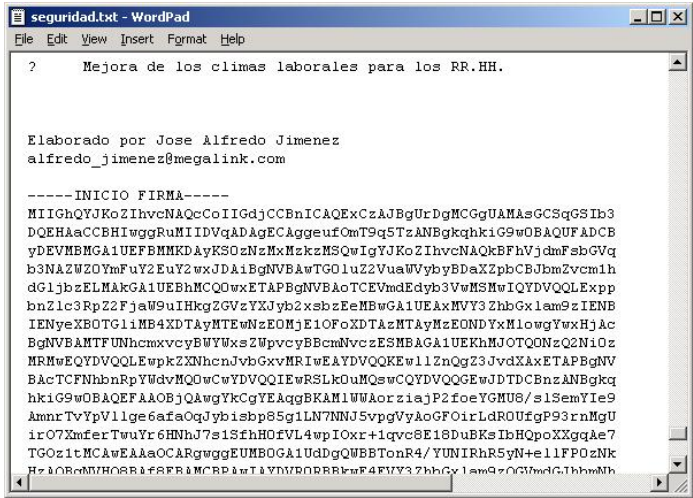


Figura 88: Visualización archivo de texto firmado.

La siguiente funcionalidad del prototipo es también firmar, pero esta vez un archivo de aplicación ya sea “.exe” o “.dll”, para esto se debe cambiar el tipo de archivo que la aplicación es capaz de visualizar.

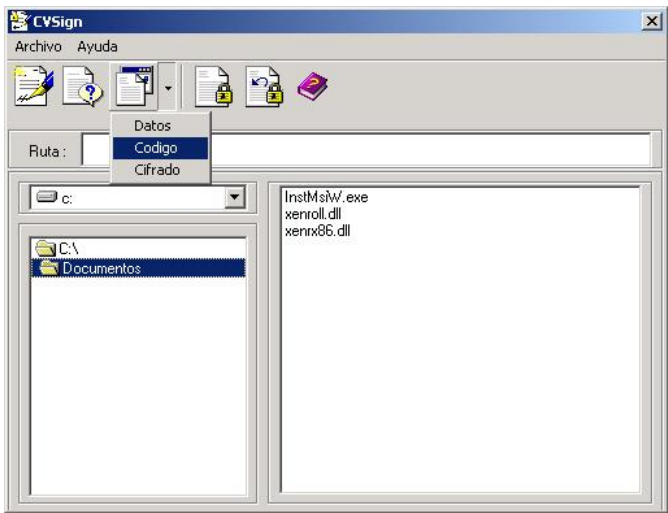


Figura 89: Menú cambio tipo de archivo a firmar.

El usuario entonces puede presionar el botón firmar de la barra de herramientas, se desplegará entonces un cuadro de dialogo en donde el usuario podrá ingresar una descripción del archivo y una dirección donde encontrar información de tal aplicación.

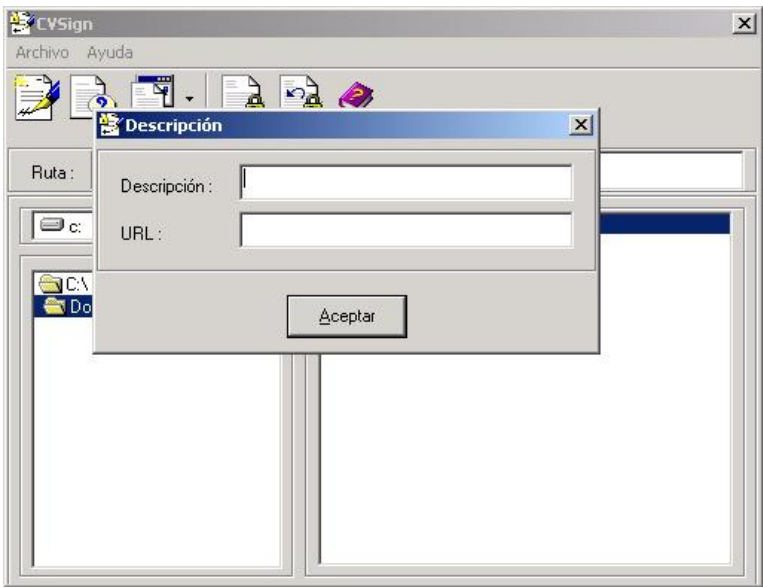


Figura 90: Cuadro descripción de código a firmar.

Una vez hecho esto se le solicitará al usuario un certificado digital asociado a una clave privada para realizar el proceso.

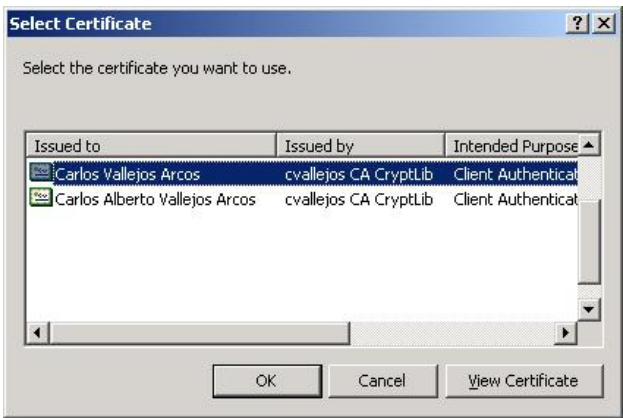


Figura 91: Cuadro solicitud certificado para firma de código.

Seguido a esto se mostrará al usuario las mismas opciones que para firmar mensajes de texto, ver certificado, cuadro de confirmación de acceso a la clave y si la firma se realiza con éxito el mensaje de proceso de firma finalizado correctamente.

La siguiente funcionalidad del prototipo tiene que ver con el proceso inverso o sea la verificación de la firma. Para esto el usuario debe nuevamente cambiar la opción de tipo de archivo para visualizar los de texto y escoger el mensaje firmado. La aplicación entonces muestra el archivo firmado y le da al usuario nuevamente dos opciones, las que son verificar la firma del documento o cerrar para cancelar el proceso.

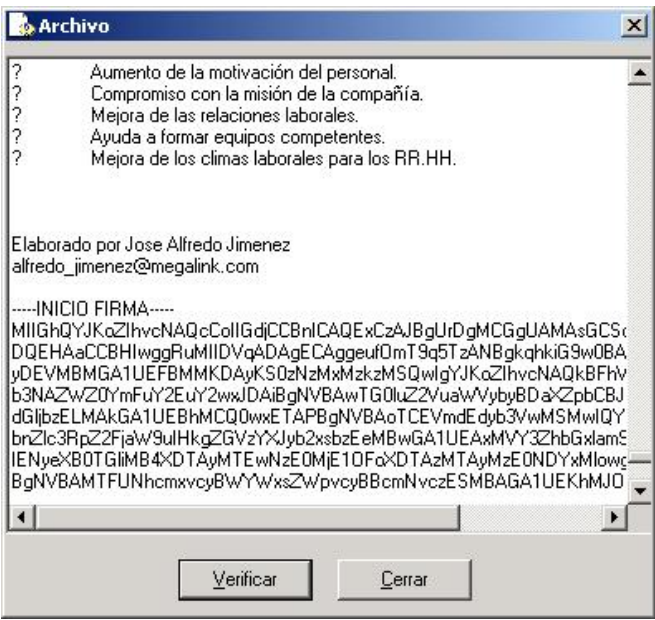


Figura 92: Pantalla visualización archivo para verificar firma.

Si el archivo no tiene la estructura mensaje-firma la aplicación muestra un mensaje expresando tal condición. Si el proceso de verificación se realizó correctamente la aplicación muestra un mensaje expresando que la verificación fue correcta.

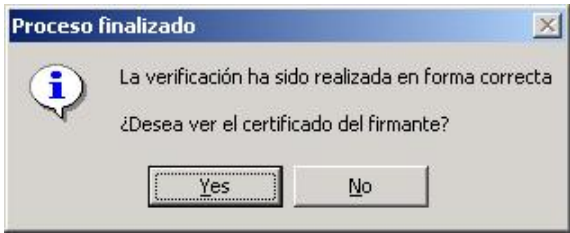


Figura 93: Cuadro de confirmación verificación de firma.

También da la opción al usuario de visualizar el certificado del firmante, con lo que termina el proceso de verificación.



Figura 94: Certificado asociado a firma de documento.

Para la verificación de la firma de código el proceso es similar. Se cambia el tipo de archivo que la aplicación maneja y se presiona verificar firma en la barra de herramientas.

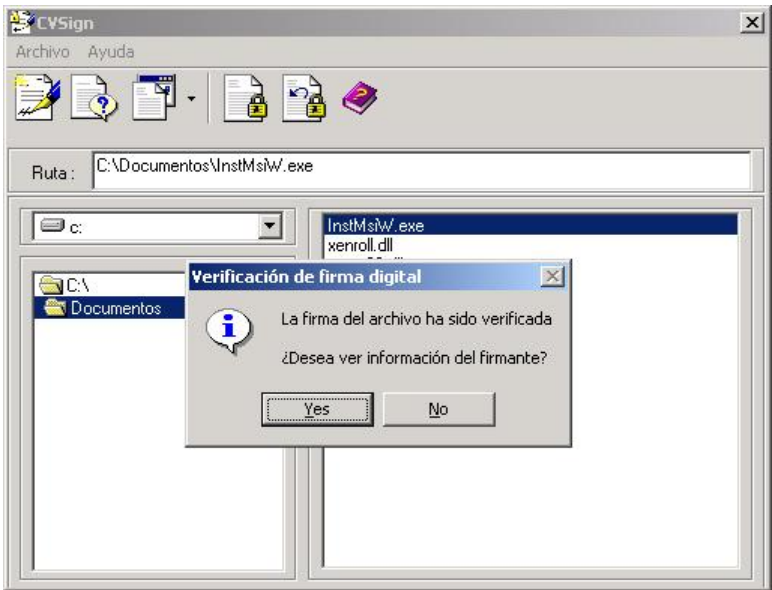


Figura 95: Cuadro confirmación verificación firma archivo código.

Si la verificación se realizó con éxito se muestra un cuadro con el mensaje de verificación correcta y la opción de ver información del firmante del código.

Si el usuario acepta ver la información del firmante se despliega un cuadro de información acerca del código y el certificado del firmante.

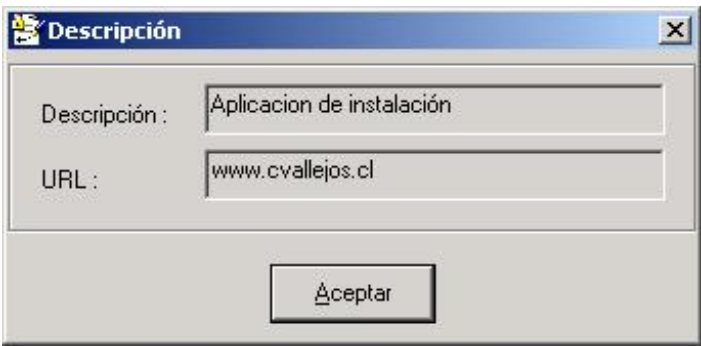


Figura 96: Cuadro información firmante archivo de código.



Figura 97: Certificado asociado a firma archivo de código.

El prototipo también cuenta con la opción de envolver un mensaje de texto o en otras palabras cifrarlo, para esto por defecto se utiliza el algoritmo TDES con la opción de máximo tamaño de clave permitido para la versión de CAPICOM instalada en el sistema.

Para cifrar entonces el usuario debe seleccionar el archivo a cifrar y presionar el botón cifrar en la barra de herramientas. Con esto la aplicación presenta un cuadro donde seleccionar la ruta para almacenar el nuevo archivo envuelto.

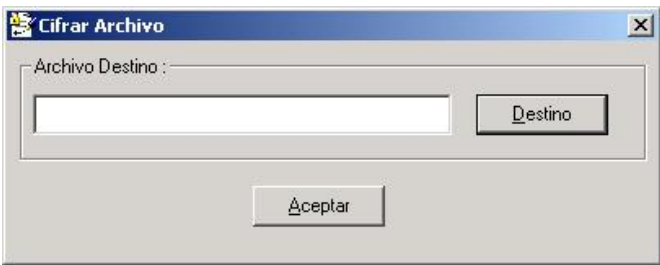


Figura 98: Cuadro destino archivo a envolver.

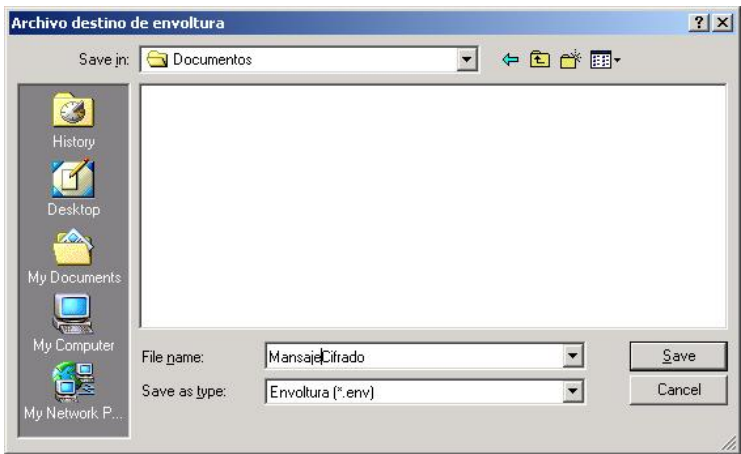


Figura 99: Cuadro selección ruta archivo a envolver.

Una vez establecida la ruta del nuevo archivo envuelto, la aplicación solicita al usuario la selección de los certificados y por tanto de las claves públicas de los destinatarios que podrán descifrar el mensaje.

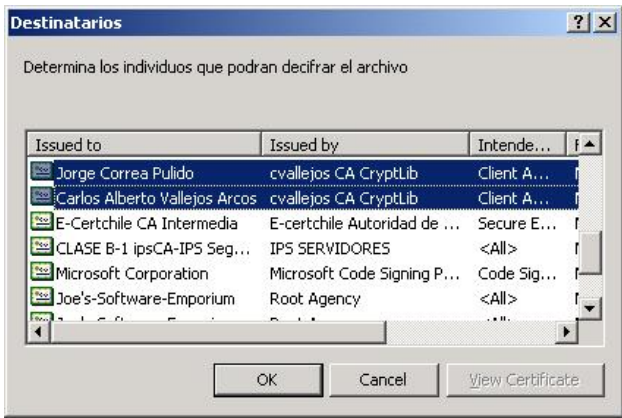


Figura 100: Cuadro selección de destinatarios del mensaje.

Realizada esta selección la aplicación muestra un mensaje de fin de proceso.

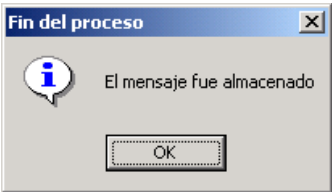


Figura 101: Cuadro mensaje fin proceso de envoltura.

Como resultado se genera un archivo cifrado con la extensión “.env”.

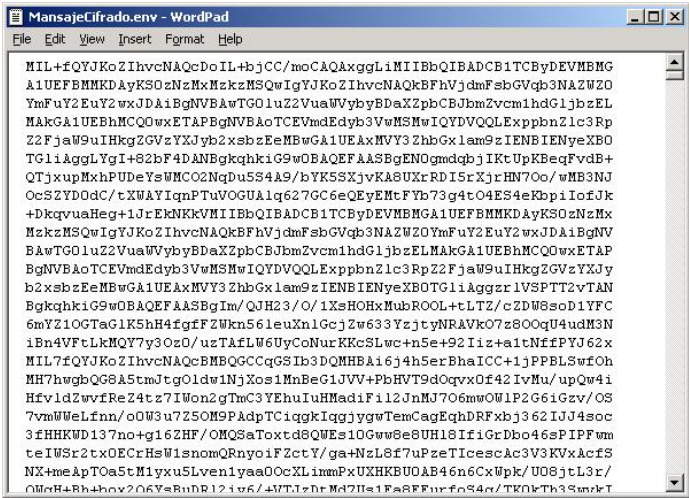


Figura 102: Visualizacion archivo de texto cifrado.

Para realizar ahora el proceso de desenvoltura del archivo, el usuario debe cambiar la opción del tipo de archivo a manejar por la aplicación, para que ahora utilice archivos con la extensión “.env”. Luego debe presionar el botón descifrar en la barra de herramientas.

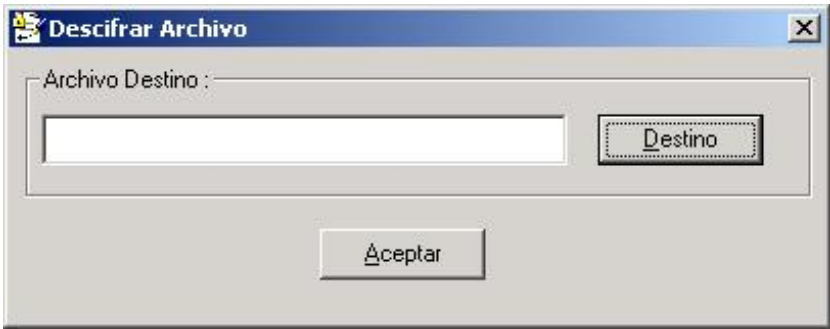


Figura 103: Cuadro selección ruta destino archivo descifrado.

El prototipo entonces muestra un cuadro para la selección de la ruta de destino para el archivo que contendrá los datos a desenvolver. Después de seleccionar la ruta, la aplicación busca en el almacén de certificados del sistema operativo del usuario una clave privada asociada a uno de los certificados incluidos como destinatario, si lo encuentra descifra el mensaje y muestra un cuadro que informa el fin del proceso.

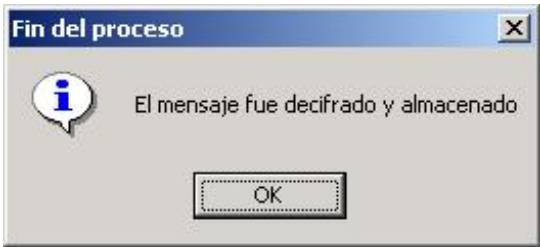


Figura 104: Cuadro mensaje fin proceso descifrado.

Si la aplicación no encuentra una clave privada apropiada para descifrar el archivo genera un mensaje de error en el proceso de descifrado, especificando que no se encontró una clave privada que pudiera desenvolver el mensaje.

8.6 Presentación Prototipo Portal Web Bancario

Esta sección describe el prototipo Web bancario desarrollado de acuerdo a las especificaciones de diseño definidas en el capítulo anterior. Este prototipo permite probar y demostrar la autenticidad de los usuarios en el acceso al sistema mediante la utilización de certificados digitales y PKI.

La aplicación Web bancaria comienza con una pantalla de presentación.



Figura 105: Página principal prototipo Web.

Esta página se encuentra almacenada en un directorio normal del servidor Web, o sea en un directorio que no realiza solicitud de certificados al usuario ni establece un canal seguro mediante el protocolo SSL.

Un enlace central en la página, invita al usuario a utilizar un certificado digital como forma de autenticación, mediante éste se puede acceder a un portal bancario típico en el que los clientes pueden encontrar una serie de servicios para el manejo de sus fondos.

Al intentar acceder a través de este enlace, el servidor Web previamente configurado, solicita al usuario un certificado digital emitido por una autoridad que esté establecida dentro de una lista de confianza especificada en el mismo servidor.

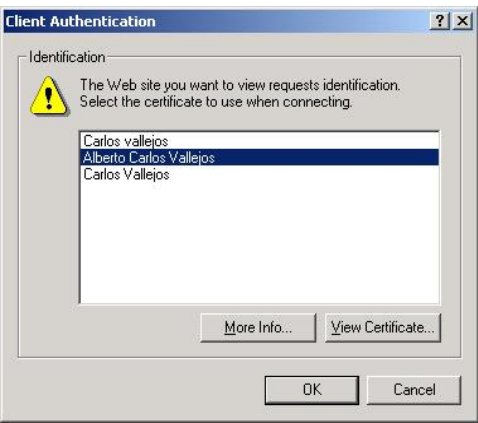


Figura 106: Cuadro solicitud de autenticación del cliente.

El usuario entonces debe seleccionar un certificado que cumpla estas condiciones, para esto el IIS presenta la pantalla que se muestra arriba en la figura con los certificados aptos para el proceso.

Si el usuario ha establecido un grado de seguridad alto para la utilización de su certificado, se le solicitará la contraseña de acceso a éste para poder proseguir con el procedimiento.



Figura 107: Cuadro solicitud contraseña del certificado.

Si el usuario no se equivoca al introducir la contraseña la aplicación podrá acceder al almacén de certificados y utilizar el certificado especificado por el usuario. Durante este proceso el servidor Web valida la ruta de confianza del certificado, accediendo a la CRL a través de una dirección que se especifica en uno de sus

campos, de estar revocado el certificado el IIS lo rechazará y no permitirá el acceso al sitio Web.

Si el certificado es verificado como válido, el usuario podrá ingresar a las páginas con los servicios bancarios. Estas han sido almacenadas en un directorio del servidor Web configurado para establecer comunicaciones seguras mediante el protocolo SSL, con el fin de poder cifrar los datos intercambiados en la comunicación cliente servidor.

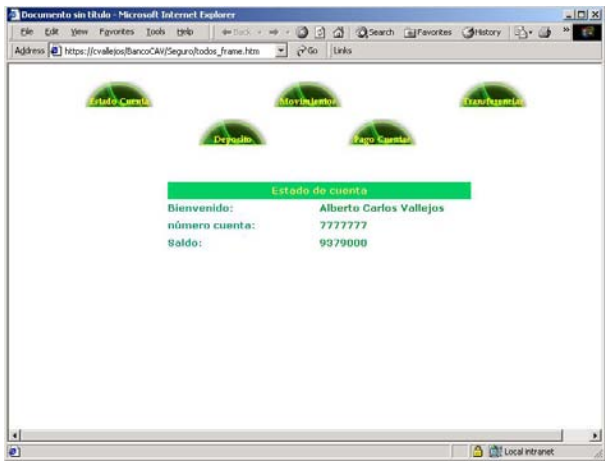


Figura 108: Pagina de servicios del prototipo bancario.

Dentro de los servicios de ejemplo implementados en el prototipo se encuentra el de transferencias de fondos del cliente, en éste el usuario puede realizar una traspaso normal de capitales pero adicionalmente debe firmar la transacción para garantizar el no repudio de ésta.

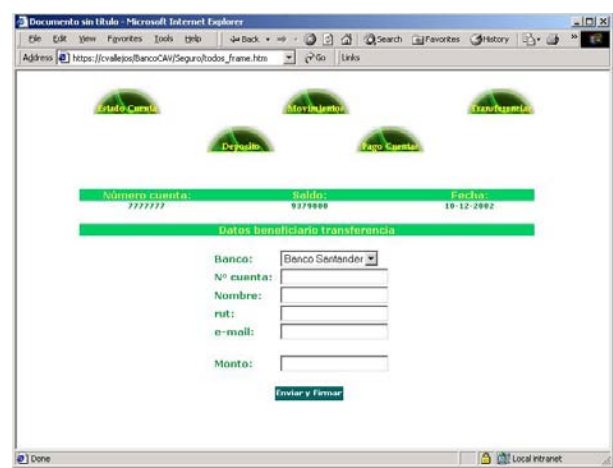


Figura 109: Pagina servicio de transferencia de fondos.

Una vez que el usuario a completado la información correspondiente y da curso a la transferencia, se le solicita nuevamente acceso a su almacén de certificados para utilizar una clave privada con la cual firmar los datos del formulario.

Durante este proceso el computador del usuario le informa a éste que el sitio Web visitado está intentando acceder al almacén de certificados y del peligro que esta acción implica, permitiéndole elegir si desea que el proceso continúe.

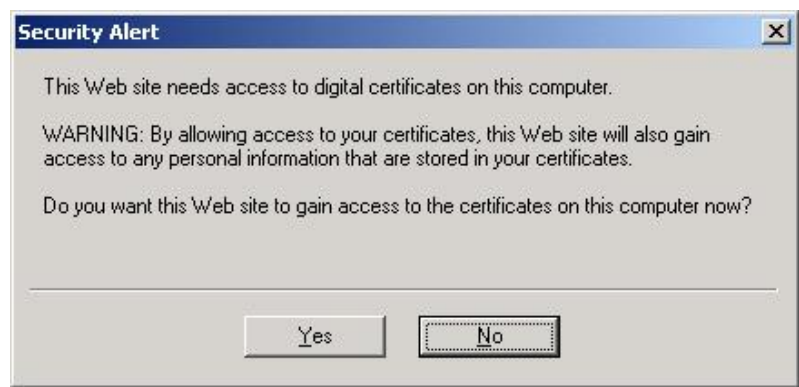


Figura 110: Cuadro alerta de acceso a certificado digital.

Si el usuario decide continuar con el procedimiento, la aplicación le informa que debe seleccionar el mismo certificado con que se autenticó al inicio de la aplicación, esto para que no utilice un certificado invalido o emitido por una autoridad no confiable para la aplicación.



Figura 111: Cuadro información selección certificado para firma.

A continuación se muestra al usuario un cuadro de selección de certificados, éstos han sido filtrados para seleccionar aquellos que están dentro de su periodo de validez y que tienen una clave privada asociada para poder firmar.

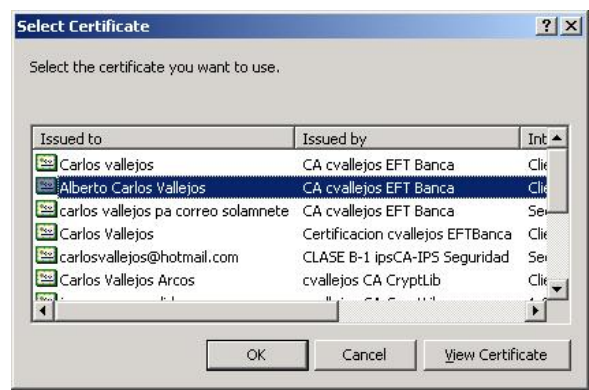


Figura 112: Cuadro selección de certificados para firma.

El usuario entonces selecciona un certificado y continua el procedimiento, el sistema le informa ahora que el sitio Web necesita crear una firma digital para lo cual utilizará la clave privada asociada al certificado elegido, también le advierte del riesgo de seguridad que esto implica y le da la opción de elegir continuar o cancelar el acceso a la clave.



Figura 113: Cuadro alerta de acceso a clave privada.

Si el usuario permite continuar, se le solicitará mediante un cuadro de dialogo, la contraseña de acceso a la clave privada seleccionada.



Figura 114: Cuadro solicitud contraseña para acceso a clave privada.

Si el usuario ingresa la contraseña correcta se realiza la transacción y se almacenan los datos de ésta y la firma en las respectivas bases de datos de la aplicación.

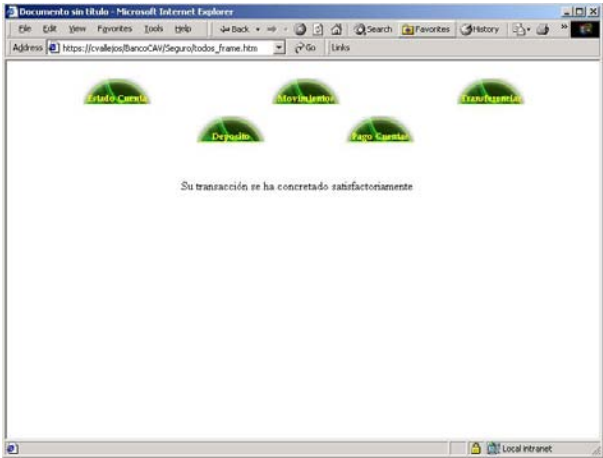


Figura 115: Pagina de información termino de transacción.

La información de la firma es almacenada en la tabla Firmas de la aplicación de forma que pueda ser verificada mediante el prototipo desarrollado para verificación de firmas digitales sobre archivos de texto descrito con anterioridad.

num	datos	firma	hash certificado
1	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
2	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
3	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
5	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
6	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
7	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
8	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
9	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
10	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
11	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3
12	<TABLE align=center bo	-----INICIO FIRMA-----	BE62CE9868518F02C78D3C900205B6907DA3

Figura 116: Imagen tabla Firmas.



Figura 117: Zoom campo firma de tabla Firmas.

9.1 Preámbulo

Para finalizar este trabajo de tesis, no queda más que plasmar las conclusiones obtenidas en el estudio de cada uno de los temas en ella abordados. Además de esto, se proponen también algunas mejoras en la implementación de los prototipos desarrollados y ampliaciones a las funcionalidades de éstos.

De igual forma se describen algunas líneas futuras de investigación que no alcanzaron lamentablemente a ser abordadas en el presente trabajo.

9.2 Conclusiones

- Los beneficios de la utilización de documentos electrónicos son muy variados como por ejemplo en costos, distribución, almacenamiento, reproducción, etc. y sus peligros también son varios relacionados con la autenticación, integridad y el no repudio principalmente de éstos.
- Estos peligros son la principal barrera para la utilización y progreso de los medios electrónicos. Por lo que se identificó claramente las necesidades de seguridad de personas y organizaciones que realizan actividades en Internet.
- El uso de la criptografía es una solución para los problemas de empleo legal de los documentos electrónicos, y más directamente el uso de las firmas digitales y las PKI, avaladas ahora por instrumentos jurídicos.

- Las legislaciones de las diversas naciones están aun en proceso de desarrollo y mejoramiento, sobre todo la de los países menos desarrollados, por lo que todavía falta avanzar en algunos temas.
- La legislación ayudará mucho a la utilización y aceptación de la tecnología de firma digital en las transacciones electrónicas realizadas por el común de las personas.
- El sistema judicial deberá adaptarse, capacitarse y evolucionar ya que si no, malamente podrá administrar justicia en el ámbito tecnológico de la firma digital.
- Todos los temas teóricos y prácticos analizados permitieron aumentar los conocimientos en cuanto a seguridad y criptografía, lo que permitió el desarrollo de una metodología de implantación de PKI y de los prototipos.
- Los prototipos ayudaron a descubrir problemas técnicos respecto a la tecnología y lograron proporcionar los servicios de confidencialidad, integridad, autenticidad y no repudio buscados. Por lo que se logró demostrar las características de seguridad que satisface una PKI y su utilidad. Con esto también se logra satisfacer las necesidades de conocimiento de la empresa, ya que el trabajo permitió disipar dudas acerca de esta tecnología.
- La metodología propuesta permite a personas u organizaciones interesadas en implementar una PKI entender y minimizar los riesgos asociados a este proceso.
- PKI NO es una fábrica productora de certificados, sino múltiples servicios que ayudan a los usuarios a identificarse de manera inequívoca en una red abierta y a intercambiarse información de forma segura.

- Faltan aplicaciones que utilicen la firma digital, ya que los usuarios de PKI generalmente se preguntan: ¿Después de instalar la PKI que se hace?, ¿Qué se firma?, ¿Cómo?.
- La tecnología PKI confunde a la mayoría de las personas, los cuales tienden a ignorarla, por lo que es necesario aumentar la sencillez de sus procedimientos y el soporte a los usuarios.
- PKI puede garantizar los servicios de seguridad dentro de su esquema o estructura, pero no puede garantizar la seguridad que subyace a los usuarios y su entorno.
- Se necesitan medios de validación de certificados más rápidos y eficientes.
- No se debe reinventar la rueda, ya existen librerías para el desarrollo de aplicaciones PKI por lo que es conveniente utilizarlas.
- El trabajo insta a futuras investigaciones y desarrollo de aplicaciones que utilicen PKI.

Después de analizar este trabajo y sus conclusiones puede que se planteen aun más preguntas que respuestas, pero ésto es normal, la tecnología PKI está en sus comienzos y como toda cosa nueva tiene que mejorar y madurar.

9.3 Mejoras

Mejoras o nuevas funcionalidades a implementar en los prototipos PKI pueden ser:

- Integrar la CA con una RA y servidores de directorio para mejorar su interoperabilidad y alcance de usuarios. Usar en esta integración un protocolo de comunicación seguro.
- Utilizar un servicio de sello de tiempo confiable para garantizar el momento en que se realizan las firmas de certificados.
- Flexibilizar la configuración de la CA, permitiéndole personalizar durante su funcionamiento la utilización de algoritmos y formatos de almacenamiento de las claves.
- Utilizar un sistema de almacenamiento de claves más seguro como por ejemplo tarjetas inteligentes.
- Cifrar los contenidos de las bases de datos de la CA para mayor seguridad.
- Generar de forma aleatoria las contraseñas que protegen los archivos de transporte de las claves de los usuarios.
- Implementar la suspensión de certificados.
- Mejorar el esquema de seguridad del archivo de eventos de la CA.

En cuanto a la aplicación de autenticación de documentos electrónicos se puede mejorar respecto a:

- Poder procesar archivos de mayores dimensiones ya que actualmente éstos se encuentran limitados al largo del tipo de dato String de Visual Basic.
- Mejorar la flexibilidad pudiendo configurar el tipo de algoritmo y el tamaño de la clave a utilizar al momento de cifrar los archivos.
- Poder verificar las CRL de forma directa desde la aplicación.
- Utilizar tarjetas inteligentes para almacenar las claves.

En el prototipo Portal Web se puede mejorar respecto a:

- Mejorar la seguridad de la base de datos, ya que por errores físicos o de programación la información de ésta podría estar mucho más expuesta.
- Demostrar que los datos de los formularios de transacciones no son alterados antes de llevarse a cabo la firma.
- Probar que al tener acceso al almacén de certificados del usuario no se puede sustraer su clave privada.
- Utilizar un servicio de fechado de tiempo confiable para las firmas de transacciones.

9.4 Investigaciones futuras

Esta sección está orientada a delinear futuras investigaciones relacionadas con el tema de PKI y la firma digital y que no alcanzaron a ser desarrollados en este trabajo de tesis. Entre ellas se puede mencionar:

La implementación y uso del protocolo OCSP para la verificación del estado de los certificados, lo que se mencionó como solución a los problemas relacionados con las CRL, consideradas como poco eficientes y engorrosas para este proceso.

Otro tema que no pudo ser plasmado en este documento es el estudio y desarrollo de una autoridad de estampado de tiempo como garante del momento en que se realizan actos relacionados con la firma digital, ya que hasta el momento se puede garantizar la autenticidad de un documento a través de la firma digital, pero no se puede tener confianza en el momento en que fue realizada la firma. Dentro del mismo tema se debe estudiar los protocolos relacionados con el tiempo en las redes informáticas como el NTP, ya que los sistemas computacionales actuales generalmente no tienen un registro y mantenimiento confiable del tiempo que miden sus relojes internos.

Otro tema que podrá ser abordado a futuro es el de los notarios digitales, personas o entidades que puedan garantizar la suscripción de contratos a través de Internet sin tener que estar presentes las personas interesadas en realizar estos actos.

Los documentos electrónicos firmados digitalmente llevan consigo generalmente la inclusión del formato de presentación de estos, cosa poco relevante cuando lo que se quiere autenticar es solo la información contenida en ellos, esto permite que la firma de documentos que contienen la misma información pero formatos distintos sean incompatibles. Con relación a esto se están definiendo algunos estándares en orden a especificar reglas de creación y representación de firmas digitales en documentos del tipo XML, por lo que este tema también debe ser considerado para una futura investigación.

Otro tema que no quedo muy claro es la base teórica sobre la cual se define la duración o ciclo de vida de los certificados digitales y cual sería el tiempo necesario entre la emisión de cada CRL, durante este trabajo de tesis no se encontraron mayores pruebas al respecto por lo que el tema amerita un análisis más profundo.

Para finalizar esta sección se propone el estudio de los estándares de comunicación entre entidades PKI ya que de éstos depende gran parte de su seguridad, lo que además entrega la posibilidad de desarrollar un sistema mayor al prototipo que se planteó en este trabajo.

Esta sección contiene una extensa lista de los libros, documentos electrónicos y principalmente trabajos de investigación encontrados en la red y consultados durante la elaboración del presente trabajo de tesis, también contiene una lista de direcciones en Internet donde se puede encontrar información adicional respecto de los distintos temas tratados.

10.1 Libros y Publicaciones

[1] ABRAMOVICH, M., S. LOWRASCH, S. LEVI, J. LEIVA (2001) DOCUMENTO ELECTRÓNICO.

[2] ALAMILLO, I. (2001) TIPOLOGÍA LEGAL DE LA FIRMA ELECTRÓNICA EN LA UNIÓN EUROPEA.

[3] BADÍA, J. M., O. COLTELL (1998) SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN.

[4] BELENGUER, P. (2002) SEGURIDAD EN EL COMERCIO MÓVIL.

[5] BELINGUERES, G. (2000) INTRODUCCIÓN A LOS CRIPTOSISTEMAS DE CURVA ELÍPTICA.

[6] BORGHELLO, C. (2001) SEGURIDAD INFORMÁTICA IMPLICANCIAS E IMPLEMENTACIÓN.

[7] CAMPS, P. (2000) ANÁLISIS Y DESARROLLO DE UN ENTORNO DE SEGURIDAD SOBRE PLATAFORMAS DE LIBRE DISTRIBUCIÓN.

- [8] CASTRO, J.C., J. FORNÉ (2001) ACCESO SEGURO A INTERNET MÓVIL.
- [9] CUERVO, J. LA FIRMA DIGITAL Y ENTIDADES DE CERTIFICACIÓN.
- [10] CUESTA, J., M. PUÑALES (2002) PKI INFRAESTRUCTURA DE CLAVE PÚBLICA.
- [11] DÁVILA, J., J. MORANT, J. SANCHO (1998) AUTORIDADES DE CERTIFICACIÓN Y CONFIANZA DIGITAL.
- [12] DEVOTO, M. (2001) COMERCIO ELECTRÓNICO Y FIRMA DIGITAL.
- [13] ELLISON, C., B. SCHNEIER (2000) TEN RISKS OF PKI: WHAT YOU'RE NOT BEING TOLD ABOUT PUBLIC KEY INFRASTRUCTURE.
- [14] FAJARDO, L. LA FIRMA ELECTRÓNICA EN EL DERECHO PRIVADO.
- [15] GONZÁLEZ, M., R. DANTOWITZ, D. RUGNA (1998) TRABAJO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA.
- [16] GRAHAM, J. (2001) LA FIRMA VIRTUAL Y LA DIRECTIVA EUROPEA SOBRE LA FIRMA ELECTRÓNICA.
- [17] GUTMANN, P. (2001) MANUAL CRYPTLIB SECURITY TOOLKIT VERSIÓN 3.0.
- [18] LANDAVERDE, M., J. GALILEO, J. TORRES (2000) DELITOS INFORMÁTICOS.
- [19] LUCENA, M. (2002) CRIPTOGRAFÍA Y SEGURIDAD EN COMPUTADORES.
- [20] MAÑAS, J. (2001) SERVICIOS DE SEGURIDAD SSL.

- [21] MARTINEZ, F. (2000) THE ABC OF CRYPTOGRAPHY AND ITS ALGORITHMS.
- [22] MARTINEZ, F. (2001) CRIPTOGRAFÍA DE CLAVE SECRETA.
- [23] MENDÍVIL, I. (1999) EL ABC DE LOS DOCUMENTOS ELECTRÓNICOS SEGUROS.
- [24] MENEZES, A., P. VAN OORSCHOT, S. VANSTONE (1996) HANDBOOK OF APPLIED CRYPTOGRAPHY.
- [25] NASH, A., D. WILLIAM, C. JOSEPH, D. BRINK (2002) INFRAESTRUCTURAS DE CLAVES PÚBLICAS, MCGRAW-HILL COLOMBIA.
- [26] PONS, M. (2000) SEGURIDAD EN EL COMERCIO ELECTRÓNICO.
- [27] PONS, M. (2001) CRIPTOLOGÍA.
- [28] POWER, R. (2002) COMPUTER SECURITY ISSUES & TRENDS, FBI.
- [29] RAMIÓ, J. (1999) APLICACIONES CRIPTOGRÁFICAS.
- [30] RFC2314 PKCS #10: CERTIFICATION REQUEST SYNTAX VERSION 1.5.
- [31] RFC2459 INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE AND CRL PROFILE.
- [32] RFC2527 INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE INTERNET POLICY AND CERTIFICATION PRACTICES FRAMEWORK.
- [33] RODRÍGUEZ, S., T. SMEDINGHOFF, R. HILL LA LEGISLACIÓN COMO INSTRUMENTO PARA EL DESARROLLO DEL COMERCIO ELECTRÓNICO.

- [34] SÁNCHEZ, J. (1999) DESCRIPCIÓN DEL ALGORITMO DES.
- [35] SCHNEIER, B. DESCRIPTION OF A NEW VARIABLE-LENGTH KEY, 64-BIT BLOCK CIPHER (BLOWFISH).
- [36] SEPÚLVEDA, D. PROTOCOLOS SEGUROS PARA EL WEB.
- [37] SHANNON, C. (1948) A MATHEMATICAL THEORY OF COMMUNICATION.
- [38] SUAZO, A. (2001) SEMINARIO DE TITULO, SEGURIDAD EN LAS TRANSACCIONES DE COMERCIO ELECTRÓNICO.
- [39] TENA, J. (2001) HISTORIA DE LA CRIPTOGRAFÍA.
- [40] XENITELLIS, S. (2000) THE OPEN-SOURCE PKI BOOK.
- [41] (1994) PUBLIC KEY INFRASTRUCTURE STUDY, NIST.
- [42] (1999) DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 13 DE DICIEMBRE DE 1999 POR LA QUE SE ESTABLECE UN MARCO COMUNITARIO PARA LA FIRMA ELECTRÓNICA.
- [43] (1999) REAL DECRETO-LEY, DE 17 DE SEPTIEMBRE, SOBRE FIRMA ELECTRÓNICA.
- [44] (2000) ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT.
- [45] (2001) INFORME SOBRE COMERCIO ELECTRÓNICO Y DESARROLLO, UNCTAD.
- [46] (2001) LA ECONOMÍA DIGITAL EN CHILE ASPECTOS LEGALES DE LA ECONOMÍA DIGITAL, CCS.

[47] (2001) LA ECONOMÍA DIGITAL EN CHILE PROYECCIONES DEL COMERCIO ELECTRÓNICO EN CHILE, CCS.

[48] (2001) LEY ARGENTINA SOBRE FIRMA DIGITAL..

[49] (2001) LEY MODELO DE LA CNUDMI SOBRE LAS FIRMAS ELECTRÓNICAS.

[50] (2002) LEY CHILENA 19799 SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA.

10.2 Direcciones Internet

- **Autoridades Certificadoras chilenas:**

<http://www.acepta.com>

<http://www.cnc-once.cl>

<https://www.e-certchile.cl>

- **Autoridades Certificadoras extranjeras**

<http://www.ace.es>

<http://www.baltimore.com>

<http://www.camerfirma.com>

<http://www.certisur.com>

<http://www.entrust.com>

<http://www.ipsca.com>

<http://www.pki.gva.es>

<http://www.verisign.com>

- **Seguridad y Criptografía**

<http://csrc.nist.gov>

<http://garaje.ya.com/alvy/cripto>
<http://seguridad.diatel.upm.es/tutorial.htm>
<http://www.ausejo.net/seguridad/seguridad.htm>
<http://www.ba.ucsa.edu.ar/cs/sec.htm>
<http://www.cacr.math.uwaterloo.ca/hac>
<http://www.cryptography.com>
<http://www.cryptosoft.com/html/secpub.htm>
<http://www.gocsi.com>
<http://www.hispasec.com>
<http://www.htmlweb.net/seguridad/seguridad.html>
<http://www.iec.csic.es/criptonomicon>
<http://www.infosecuritymag.com>
<http://www.iti.upv.es/seguridad>
<http://www.kriptopolis.com>
<http://www.microsoft.com>
<http://www.seguridata.com>

- **PKI**

<http://csrc.nist.gov/pki/>
<http://tirnanog.ls.fi.upm.es/>
http://www.cio-dpi.gc.ca/pki-icp/index_e.asp
<http://www.pki.gov.ar>
<http://www.pkiforum.com>
<http://www.pkiforum.org>
<http://www.pkilaw.com>
<http://www.pki-page.org>
<http://www.rsasecurity.com>

<http://www.terena.nl/tech/projects/pki/pki-info.html>

<http://www.valicert.com>

APENDICE A

GLOSARIO

A

Algoritmo: Secuencia de pasos usados para realizar una operación matemática.

Algoritmo de cifrado: Formula matemática que se usa para cifrar u ocultar información.

Algoritmo de curva elíptica: Formula matemática alternativa al algoritmo RSA y DSA para generar firmas digitales.

ANSI: Organismo público de los EE.UU. que tiene como función definir y aprobar los estándares de los Estados Unidos en muchas áreas, incluyendo computación e informática.

Autenticación: Servicio de seguridad que verifica información como la identidad de un participante en una transacción electrónica.

Autorización: Otorgamiento de privilegios de acceso a usuarios.

B

Biometría: Autenticación de usuarios basada en una característica física única como la retina o huella dactilar.

C

CA: Autoridad de certificación, organización o compañía de confianza que emite certificados digitales.

Certificado: Conocido también como certificado digital, es un documento electrónico que se usa en sistemas de clave pública y que contiene información acerca de la identidad y clave pública de un usuario.

Cifrado: Técnica por la cual a través de un algoritmo se modifica o altera la representación de un texto legible, convirtiéndolo en un criptograma de forma que su interceptación por extraños no entregue información alguna del mensaje original.

Cifrado asimétrico: Método criptográfico que usa una clave para cifrar un mensaje y usa otra diferente pero relacionada a la anterior para descifrarlo.

Cifrado simétrico: Método que usa el mismo algoritmo y clave para cifrar y descifrar un mensaje.

Cifrador: Sistema que cuenta con un algoritmo que permite cifrar un texto en claro. Es sinónimo de criptógrafo.

Cifrador de bloques: Sistema que divide previamente el mensaje en bloques de igual tamaño y que luego cifra cada bloque con la misma clave.

Cifrador de flujo: Sistema que cifra el mensaje carácter a carácter. Se compara con el cifrado en bloques.

Clave: Secreto utilizado para cifrar o descifrar un texto cifrado.

Clave privada: Clave secreta utilizada para cifrar un mensaje y cuyo secreto mantiene la inmunidad del sistema. En los sistemas asimétricos es la clave confidencial pareja de la clave pública.

Clave pública: Clave utilizada en criptosistemas asimétricos conjuntamente con una clave privada de forma que se cifra con una de ellas y se descifra con la otra.

Cliente: Entre dos equipos conectados, es el que solicita un servicio determinado del otro que actúa como servidor.

Codificación: Técnica para cifrar por códigos usando una relación directa entre palabra y código. No es propiamente un cifrado.

Confidencialidad: Servicio de seguridad que limita una comunicación al ámbito privado de dos partes conocidas y autorizadas.

Contraseña: Secuencia de caracteres mantenidos en secreto por un usuario y que le permiten autenticarse en un sistema.

Cortafuegos: Equipo dedicado que es utilizado para comunicar una red privada con la red pública. Este equipo es un ordenador especializado que controla y administra el flujo de información entre la red privada interna y el mundo exterior.

CP: Política de Certificación, reglas que gobiernan el uso de certificados de clave pública en un ambiente particular.

CPS: Estamentos Prácticas de Certificación, descripción de las prácticas que una CA realiza para emitir, revocar y renovar sus certificados, amplían generalmente las CP de una CA.

Criptoanalista: Persona cuya función básica es la de romper códigos y textos cifrados para recuperar de forma ilegítima la información allí contenida, utiliza el criptoanálisis.

Criptografía: Etimología de ocultar y escritura. Es el arte, técnica o ciencia que permite proteger información por medio de la aplicación del cifrado a un mensaje.

Criptograma: Documento no legible obtenido al cifrar un texto en claro. La representación o alfabeto del criptograma puede ser distinto a la del texto en claro.

Criptología: Ciencia que estudia e investiga todo lo concerniente a la criptografía y criptoanálisis.

Criptólogo: Persona cuya función básica es la de crear algoritmos de cifrado y descifrado.

CRL: Lista de Revocación de Certificados, lista de certificados no válidos de una CA.

CSP: Proveedor de Servicios Criptográficos, herramienta de software o hardware que contiene implementaciones de algoritmos y estándares criptográficos.

D

Decodificación: Recuperación de la información codificada aplicando la relación inversa entre palabra y código.

DES: Estándar de Cifrado de Datos, método más común de cifrado de simétrico.

Descifrado: Técnica por la cual a través de un algoritmo, un receptor puede recuperar la información contenida en un criptograma, inverso del cifrado.

Directorio: Servicio o repositorio para almacenar información, típicamente se utiliza para almacenar certificados y CRL emitidos por una CA.

DN: Nombre Distinguido, nombre único dentro de un dominio de directorio, cadena única integrada por múltiples atributos que como un todo identifica una entidad.

DSA: Algoritmo de Firma Digital, algoritmo que se usa en firma digital según lo define el NIST en su estándar de firma digital.

DSS: Estándar de Firma Digital definido por el NIST.

E

E-tailing: Comercio electrónico detallista por Internet.

F

Firma digital: Técnica para comprobar que no se ha adulterado un mensaje usando criptografía de clave pública.

Fuerza Bruta: Técnica de ataque informático que usa la repetición constante para superar las condiciones de seguridad de un sistema.

Función Hash: Algoritmo matemático que transforma un bloque de texto en un bloque único de texto cifrado de longitud fija y que no puede ser descifrado.

H

HTML: Lenguaje de Etiquetas de Hipertexto, lenguaje basado en texto ASCII utilizado para crear documentos Web.

HTTP: Protocolo de Transferencia de Hipertexto, protocolo Web utilizado para transmitir información y para su representación

HTTPS: Versión segura del protocolo HTTP, bajo este la conexión entre un cliente y un servidor se cifra usando SSL.

I

Integridad: Servicio de seguridad referido a que la versión transmitida de un documento mantiene la fidelidad en todas sus formas con el original.

IPSec: Conjunto de protocolos desarrollados por IETF para construir características de seguridad a nivel del protocolo IP.

ISO: Organización Internacional de Normalización, entidad que establece las normas o estándares que definen el modelo de referencia de interconexión de sistemas abiertos para redes Internet.

ISP: Sigla con la que se denomina un proveedor de conexión a Internet.

K

Kerberos: Sistema de autenticación y autorización cliente servidor desarrollado por el MIT, usa cifrado simétrico.

L

LDAP: Protocolo de Acceso Liviano a Directorios, permite a los usuarios acceder y buscar en directorios de Internet.

M

MD: Función Hash o de resumen desarrollada por laboratorios RSA.

MIME: Extensiones Multipropósito para Correo en Internet, son estándares para anexar archivos adicionales en los correos electrónicos.

N

NIST: Organismo fundado por el congreso de los Estados Unidos con el objeto de desarrollar tecnologías, incrementar la calidad y modernizar los procesos de manufactura entre otros.

No repudio: Servicio de seguridad que asegura que un emisor no puede negar el envío de un mensaje.

P

Pareja de claves: Las dos claves generadas en la criptografía asimétrica y matemáticamente relacionadas. Clave pública y clave privada.

PIN: Secuencia de dígitos usados para verificar la identidad del propietario de un Token, es un tipo de contraseña.

PKCS: Estándares Criptográficos de Clave Pública, una serie de estándares definidos por los laboratorios RSA que definen elementos y estructuras criptográficos.

PKI: Infraestructura de Clave Pública. Sistema que usa cifrado asimétrico para ofrecer pruebas de identidad, confidencialidad, integridad y no repudio.

PKIX: Grupo de trabajo del IETF que define estándares de criptografía de clave pública para usar en Internet.

R

RA: Autoridad de Registro, persona o entidad encargada de la identificación y autenticación de un solicitante de certificado digital.

Resumen o Hash: Texto cifrado creado por un algoritmo o función Hash, es una representación única de un mensaje.

RSA: Criptosistema de clave pública con base en el problema de factorización.

S

S/MIME: Especificación del IETF que define un marco de referencia para el cifrado y/o firma digital de un mensaje de correo electrónico.

SSL: Capa de Socket Seguro, estándar abierto propuesto por Netscape para ofrecer servicios seguros en el Web, utiliza el sistema de cifrado asimétrico de RSA.

Sustitución: Técnica criptográfica que consiste en sustituir un carácter del texto en claro por otro en el texto cifrado.

Sustitución monoalfabética: Cifrado que sustituye cada carácter del texto en claro por otro carácter en el criptograma, usando un único alfabeto.

Sustitución polialfabética: Cifrado que mediante una clave, sustituye los caracteres del texto en claro por otros caracteres en el texto cifrado, utilizando para ello más de un alfabeto.



Tarjeta Inteligente: Pequeño dispositivo del tamaño de una tarjeta de crédito que contiene circuitos electrónicos. Se utilizan generalmente para almacenar datos de carácter personal.

TCP/IP: Conjunto de protocolos de comunicación que soporta la comunicación entre redes locales y redes de área extendida, como Internet.

Texto cifrado: Información que ha sido convertida en un código aparentemente sin sentido.

Texto en claro: Documento original o mensaje no cifrado que se desea enviar a uno o más destinatarios o bien almacenar en forma cifrada. También se le denomina texto base.

Token: Objeto físico algunas veces de electrónica sofisticada por lo que se les llama también tarjeta inteligente.

Transacción: Transferencia electrónica de información.

Transposición: Técnica de cifrado que consiste en reordenar un texto en claro. También se conoce como permutación.

Triple DES: Técnica usada para hacer más fuerte el sistema de cifrado DES, para esto aplica tres veces el algoritmo con diferentes claves.



X.500: Estándares ANSI que definen a un servicio de directorios.

X.509: Estándar que define la estructura de datos de los certificados digitales.

"Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

TITULO I

DISPOSICIONES GENERALES

Artículo 1º.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.

Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel.

Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados.

Artículo 2º.- Para los efectos de esta ley se entenderá por:

- a) Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;
- b) Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica;
- c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas;
- d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior;
- e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción;
- f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;

g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, y

h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica.

Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

Lo dispuesto en el inciso anterior no será aplicable a los actos o contratos otorgados o celebrados en los casos siguientes:

a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;

b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes; y,

c) Aquellos relativos al derecho de familia.

La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en el artículo siguiente.

Artículo 4º.- Los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

Artículo 5º.- Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:

1.- Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales; y

2.- Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el numeral anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.

TITULO II

USO DE FIRMAS ELECTRÓNICAS POR LOS ÓRGANOS DEL ESTADO

Artículo 6º.- Los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica.

Se exceptúan aquellas actuaciones para las cuales la Constitución Política o la ley exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas.

Lo dispuesto en este título no se aplicará a las empresas públicas creadas por ley, las que se registrarán por las normas previstas para la emisión de documentos y firmas electrónicas por particulares.

Artículo 7º.- Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel.

Con todo, para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse mediante firma electrónica avanzada.

Artículo 8º.- Las personas podrán relacionarse con los órganos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos.

Los órganos del Estado deberán evitar, al hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias.

Artículo 9º.- La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos del Estado se realizará por los respectivos ministros de fe. Si éste no se encontrare establecido en la ley, el reglamento a que se refiere el artículo 10 indicará la forma en que se designará un funcionario para estos efectos.

Dicha certificación deberá contener, además de las menciones que corresponda, la fecha y hora de la emisión del documento.

Los efectos probatorios de la certificación practicada por el ministro de fe competente serán equivalentes a los de la certificación realizada por un prestador acreditado de servicios de certificación.

Sin perjuicio de lo dispuesto en el inciso primero, los órganos del Estado podrán contratar los servicios de certificación de firmas electrónicas con entidades certificadoras acreditadas, si ello resultare más conveniente, técnica o económicamente, en las condiciones que señale el respectivo reglamento.

Artículo 10.- Los reglamentos aplicables a los correspondientes órganos del Estado regularán la forma cómo se garantizará la publicidad, fiabilidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas de este título.

TITULO III

DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 11.- Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Asimismo, son prestadores acreditados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad al Título V de esta ley, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Artículo 12.- Son obligaciones del prestador de servicios de certificación de firma electrónica:

a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano;

b) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N° 19.628, sobre Protección de la Vida Privada;

c) En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad;

d) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

e) En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;

f) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;

i) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos, y

j) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes N° 19.496, sobre Protección de los Derechos de los Consumidores y N° 19.628, sobre Protección de la Vida Privada.

Artículo 13.- El cumplimiento, por parte de los prestadores no acreditados de servicios de certificación de firma electrónica, de las obligaciones señaladas en las letras a), b), c) y j) del artículo anterior, será considerado por el juez como un antecedente para determinar si existió la debida diligencia, para los efectos previstos en el inciso primero del artículo siguiente.

Artículo 14.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica.

Para los efectos de este artículo, los prestadores acreditados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquéllos homologados en virtud de lo dispuesto en el inciso final del artículo 15.

El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado.

En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado.

TITULO IV

DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Artículo 15.- Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:

- a) Un código de identificación único del certificado;
- b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;
- c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y
- d) Su plazo de vigencia.

Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente.

Artículo 16.- Los certificados de firma electrónica quedarán sin efecto, en los siguientes casos:

- 1) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;
- 2) Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias:
 - a) A solicitud del titular del certificado;
 - b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;
 - c) Por resolución judicial ejecutoriada, o
 - d) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 24;
- 3) Por cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados que señala el artículo 18, en razón de lo dispuesto en el artículo 19 o del cese de la actividad del prestador, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad con lo dispuesto en las letras c) y h) del artículo 12; y,

4) Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad a la letra c) del artículo 12.

La revocación de un certificado en las circunstancias de la letra d) del número 2) de este artículo, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el prestador al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación o la suspensión. En cualquier caso, ni la revocación ni la suspensión privarán de valor a los certificados antes del momento exacto en que sean verificadas por el prestador.

El término de vigencia de un certificado de firma electrónica por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro de acceso público.

TITULO V

DE LA ACREDITACIÓN E INSPECCIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 17.- La acreditación es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en esta ley y en el reglamento, permitiendo su inscripción en el registro que se señala en el artículo 18.

Para ser acreditado, el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones:

- a) Demostrar la fiabilidad necesaria de sus servicios;
- b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;
- c) Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados;
- d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;
- e) Haber contratado un seguro apropiado en los términos que señala el artículo 14; y,
- f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.

Artículo 18.- El procedimiento de acreditación se iniciará mediante solicitud ante la Entidad Acreditadora, a la que se deberá acompañar los antecedentes relativos a los requisitos del artículo 17 que señale el reglamento y el comprobante de pago de los costos de la acreditación. La Entidad Acreditadora deberá resolver fundadamente sobre la solicitud en el plazo de veinte días contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de

resolverse. Si el interesado denunciare el incumplimiento de ese plazo ante la propia autoridad y ésta no se pronunciare dentro del mes siguiente, la solicitud se entenderá aceptada.

La Entidad Acreditadora podrá contratar expertos con el fin de verificar el cumplimiento de los requisitos señalados en el artículo 17.

Otorgada la acreditación, el prestador será inscrito en un registro público que a tal efecto llevará la Entidad Acreditadora. Durante la vigencia de su inscripción en el registro, el prestador acreditado deberá informar a la Entidad Acreditadora cualquier modificación de las condiciones que permitieron su acreditación.

Artículo 19.- Mediante resolución fundada de la Entidad Acreditadora se podrá dejar sin efecto la acreditación y cancelar la inscripción en el registro señalado en el artículo 18, por alguna de las siguientes causas:

a) Solicitud del prestador acreditado;

b) Pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o peritos que la Entidad Acreditadora ocupe en la inspección a que se refiere el artículo 20; y,

c) Incumplimiento grave o reiterado de las obligaciones que establece esta ley y su reglamento.

En los casos de las letras b) y c), la resolución será adoptada previa audiencia del afectado y se podrá reclamar de ella ante el Ministro de Economía, Fomento y Reconstrucción, dentro del plazo de cinco días contados desde su notificación. El Ministro tendrá un plazo de treinta días para resolver. Dentro de los diez días siguientes a la fecha en que se notifique la resolución que éste dicte o, en su caso, desde que se certifique que la reclamación administrativa no fue resuelta dentro de plazo, el interesado podrá interponer reclamación jurisdiccional, para ante la Corte de Apelaciones de su domicilio. La reclamación deberá ser fundada y para su agregación a la tabla, vista y fallo, se regirá por las normas aplicables al recurso de protección. La resolución de la Corte de Apelaciones no será susceptible de recurso alguno.

Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de firmas electrónicas certificadas por ellos. Sin perjuicio de ello, la Entidad Acreditadora publicará un aviso dando cuenta de la cancelación, a costa del certificador. A partir de la fecha de esta publicación, quedarán sin efecto los certificados, a menos que los datos de los titulares sean transferidos a otro certificador acreditado, en conformidad con lo dispuesto en la letra h) del artículo 12. Los perjuicios que pueda causar la cancelación de la inscripción del certificador para los titulares de los certificados que se encontraban vigentes hasta la cancelación, serán de responsabilidad del prestador.

Artículo 20.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Entidad Acreditadora ejercerá la facultad inspectora sobre los mismos y podrá, a tal

efecto, requerir información y ordenar visitas a sus instalaciones mediante funcionarios o peritos especialmente contratados, de conformidad al reglamento.

Artículo 21.- La Entidad Acreditadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los certificadores acreditados.

Artículo 22.- Los recursos que perciba la Entidad Acreditadora por parte de los prestadores acreditados de servicios de certificación constituirán ingresos propios de dicha entidad y se incorporarán a su presupuesto.

TITULO VI

DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE FIRMAS ELECTRÓNICAS

Artículo 23.- Los usuarios o titulares de firmas electrónicas tendrán los siguientes derechos:

1º. A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar;

2º. A la confidencialidad en la información proporcionada a los prestadores de servicios de certificación. Para ello, éstos deberán emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos;

3º. A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso, y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o que se convinieren;

4º. A que el prestador de servicios o quien homologue sus certificados le proporcionen la información sobre sus domicilios en Chile y sobre todos los medios a los que el usuario pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

5º. A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 4) del artículo 16 de la presente ley, o bien, para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador.

6º. A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus

certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 3) del artículo 16 de la presente ley, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;

7º. A traspasar sus datos a otro prestador de servicios de certificación;

8º. A que el prestador no proporcione más servicios y de otra calidad que los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario;

9º. A acceder, por medios electrónicos, al registro de prestadores acreditados que mantendrá la Entidad Acreditadora, y

10º. A ser indemnizado y hacer valer los seguros comprometidos, en conformidad con el artículo 14 de la presente ley.

Los usuarios gozarán de estos derechos, sin perjuicio de aquellos que deriven de la Ley N° 19.628, sobre Protección de la Vida Privada y de la Ley N° 19.496, sobre Protección a los Derechos de los Consumidores y podrán, con la salvedad de lo señalado en el número 10º de este artículo, ejercerlos conforme al procedimiento establecido en esa última normativa.

Artículo 24.- Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando.

TITULO VII

REGLAMENTOS

Artículo 25.- El Presidente de la República reglamentará esta ley en el plazo de noventa días contados desde su publicación, mediante uno o más decretos supremos del Ministerio de Economía, Fomento y Reconstrucción, suscritos también por los Ministros de Transportes y Telecomunicaciones y Secretario General de la Presidencia.

Lo anterior es sin perjuicio de los demás reglamentos que corresponda aprobar, para dar cumplimiento a lo previsto en el artículo 10.

Artículo transitorio.- El mayor gasto que irroque a la Subsecretaría de Economía, Fomento y Reconstrucción las funciones que le asigna esta ley, durante el año 2002, se financiará con los recursos consultados en su presupuesto.

APENDICE C

CERTIFICACION DE PERSONA

Para realizar el proceso de certificación de un individuo, éste debe presentarse ante la CA y realizar los procesos correspondientes que permitan verificar y garantizar su identidad, realizado esto la autoridad le entregará un archivo que contendrá su par de claves y su certificado digital. Para instalar éstos en su computador debe seguir los siguientes pasos:

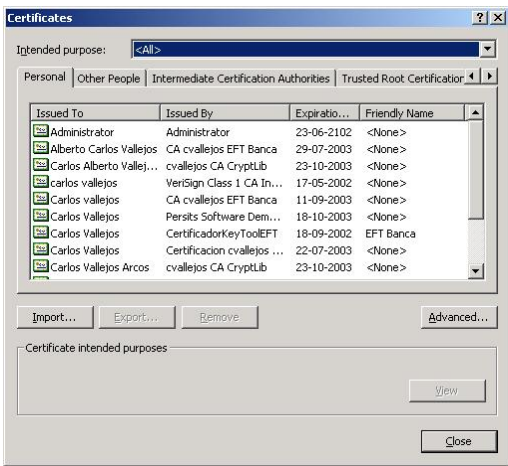
1. Seleccionar Opciones de Internet desde el menú Herramientas.



2. Seleccionar la solapa Contenido.



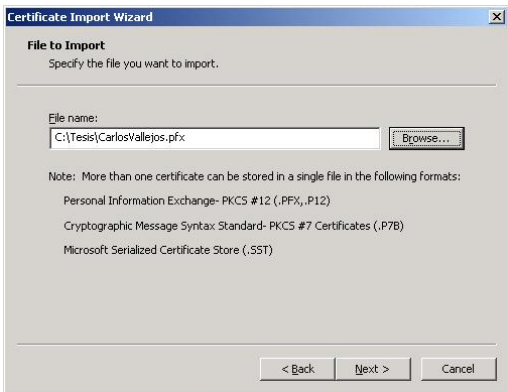
3. Presionar sobre el botón Certificados. Aparecerá una vista del almacén de certificados personales de Windows.



4. Presionar sobre el botón importar. Aparecerá el ayudante de importación de certificados.



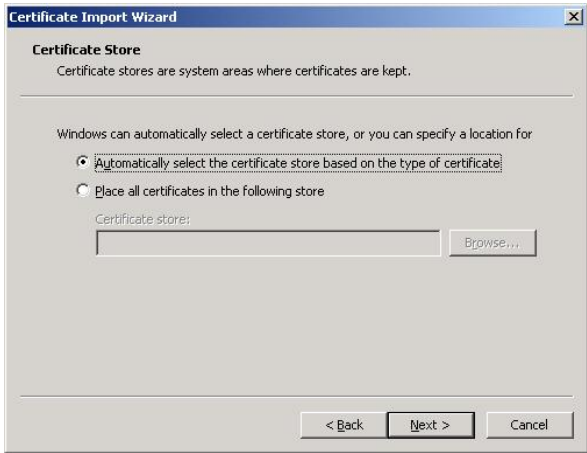
5. Se debe especificar la ruta y el tipo de archivo a importar. En este caso será un archivo con la extensión “pfx”.



6. Se debe ingresar la contraseña que protege el archivo y que debió ser informada por la CA al usuario. Si en esta etapa se selecciona Activar protección de clave Privada, posteriormente el ayudante solicitará una contraseña para tal acción.



7. Seleccionar la opción Automáticamente Seleccionar el Almacén de certificado.



8. El ayudante muestra un resumen del proceso.



9. El ayudante finalmente informa que el proceso se ha completado con éxito.



Si en el paso 6 se seleccionó Activar Protección de Clave Privada, al finalizar el proceso de importación el ayudante informará el nivel actual de protección de la clave privada.



Y dará la opción de cambiar este nivel de seguridad.



Si se define un nivel de seguridad alto el ayudante solicitará especificar una contraseña que será exigida cada vez que se quiera utilizar la clave privada.



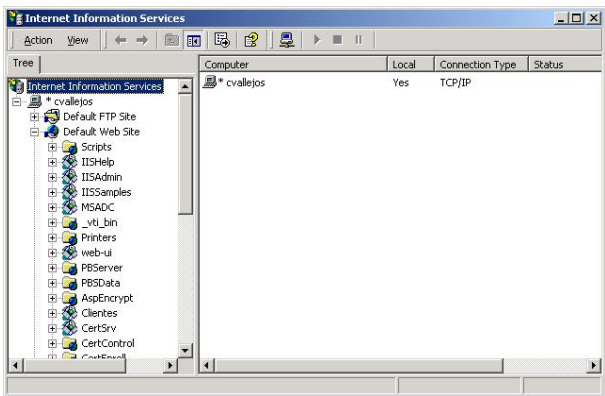
APENDICE D

CERTIFICACION SERVIDOR

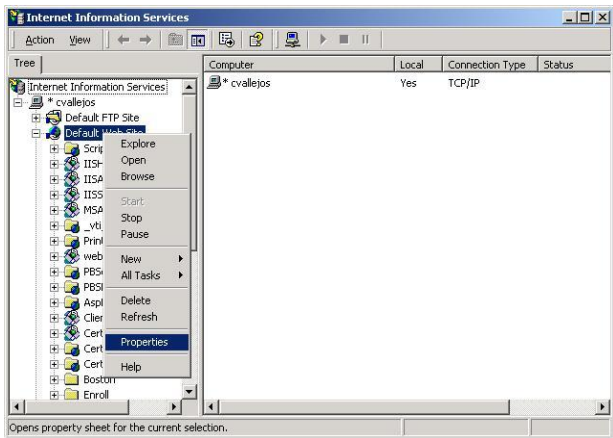
▪ **Solicitud de Certificado Servidor**

Para comenzar el proceso de solicitud de certificación de un servidor Web, se debe generar en éste una solicitud en el formato PKCS #10. para esto se debe seguir la siguiente secuencia de pasos:

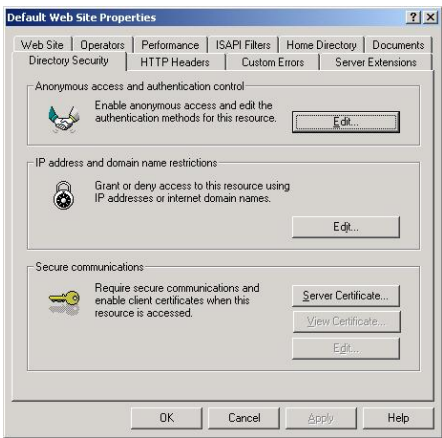
- 1. Abrir el administrador de servicios de Internet desde Herramientas Administrativas.



- 2. Seleccionar la ventana propiedades sobre el sitio Web que utilizará el certificado digital para autenticarse.



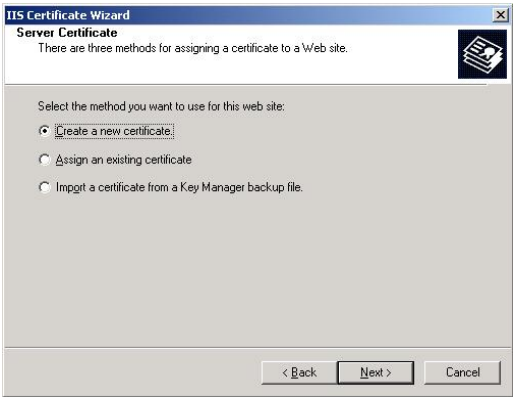
- 3. Seleccionar Seguridad de Directorio y presionar sobre el botón Certificado Servidor en la sección Comunicaciones Seguras.



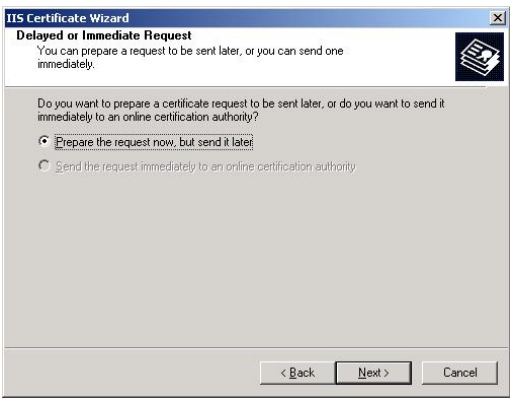
4. Aparecerá un ayudante para el proceso de solicitud de certificado Servidor.



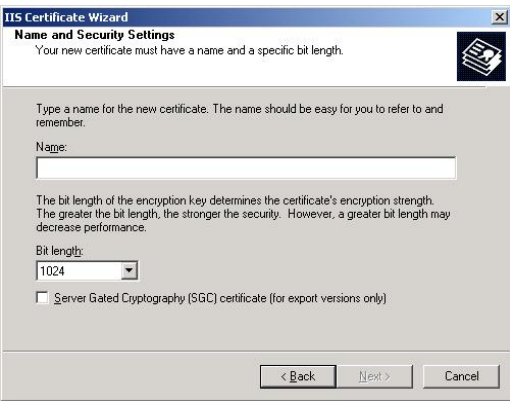
5. Elegir crear nuevo certificado.



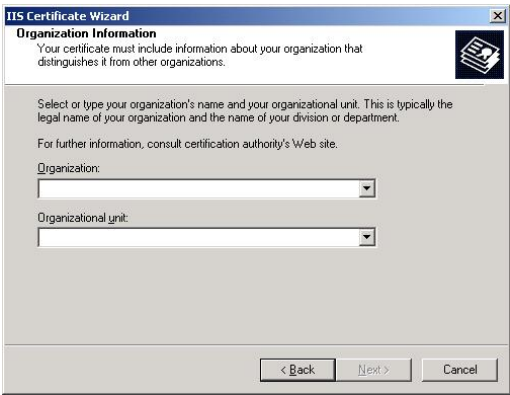
6. Elegir preparar solicitud ahora y enviar después.



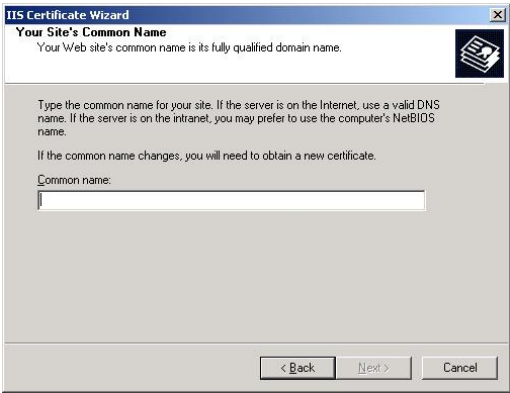
7. En esta etapa se debe ingresar el nombre que tendrá el certificado y el tamaño de las claves que se generarán para el servidor. Se recomienda 1024 bits por compatibilidad y seguridad. El par de claves se genera y almacena en el registro del servidor Web, y la clave pública será incluida en la solicitud.



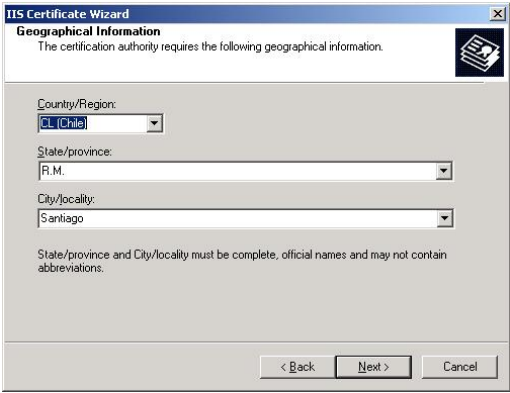
8. Ahora se procederá a crear la solicitud de certificado. Ingrese la información de la organización.



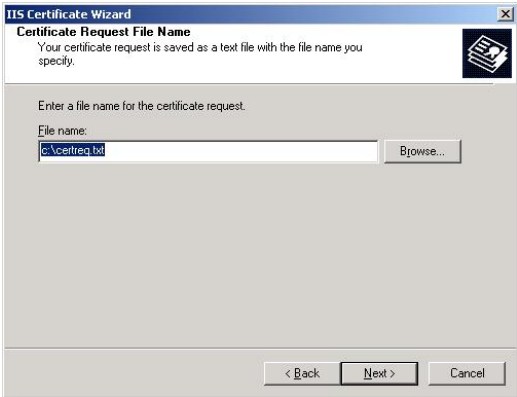
9. Ingrese el Nombre Común del servidor, este corresponde al nombre de dominio del servidor Web, por ejemplo "www.cvallejos.cl".



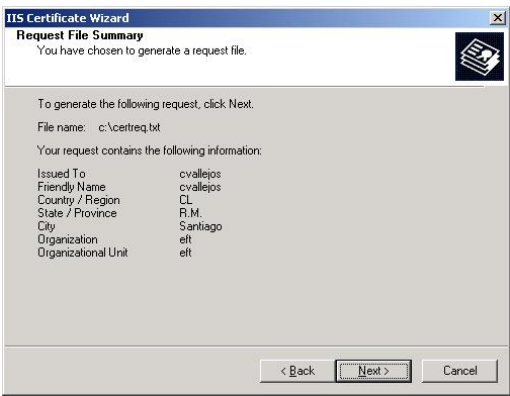
10. Ingrese los detalles geográficos.



11. Ingrese ruta y nombre de archivo donde se almacenará la solicitud.



12. El ayudante mostrará un resumen del contenido de la solicitud para su confirmación.



13. Se da aviso que se ha completado el proceso. Una buena medida de seguridad sería respaldar las claves generadas para el servidor.

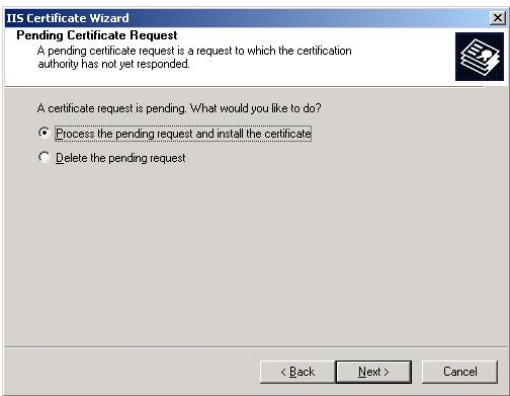


▪ **Instalación Certificado Servidor**

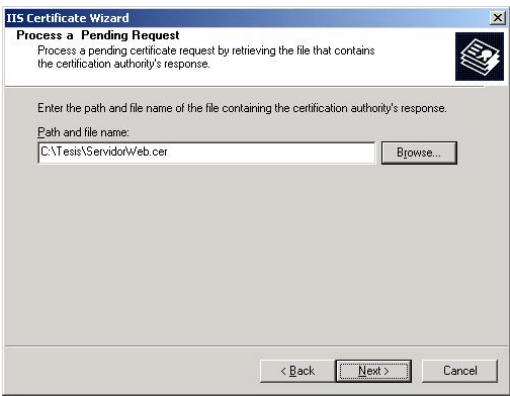
Finalizado el proceso de generar el archivo de solicitud de certificación, se debe hacer llegar este a la autoridad certificadora para que esta cree y firme el certificado del servidor.

Recibido el certificado emitido por la CA, se deben realizar los siguientes pasos en el servidor:

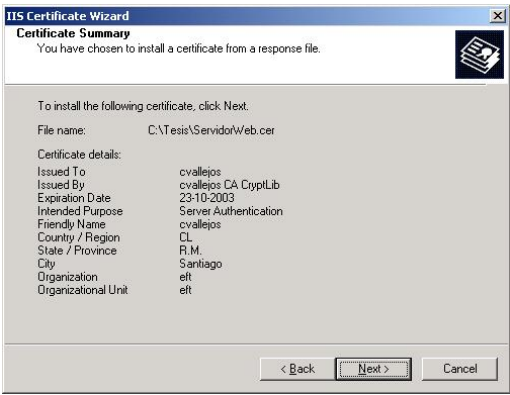
1. Abrir el administrador de servicios de Internet desde Herramientas Administrativas y Seleccionar propiedades sobre el sitio Web donde se generó la solicitud. Aparecerá nuevamente el ayudante, debe seleccionar procesar solicitud pendiente e instalar certificado.



2. Ingrese la ruta al archivo del certificado emitido por la CA.



3. El ayudante presentará un resumen del certificado digital.



4. Por último se dará aviso de proceso completado.

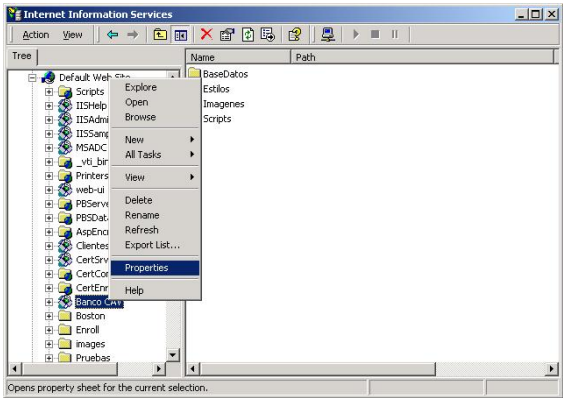


▪ **Configuración directorio Web con SSL**

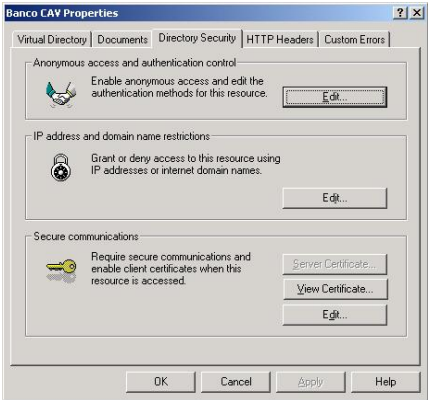
Una vez instalado el certificado en el sitio Web del servidor, se puede habilitar la utilización de SSL. Esto se puede realizar para cualquier carpeta virtual disponible dentro del sitio Web.

Para completar este proceso se deben realizar los siguientes pasos:

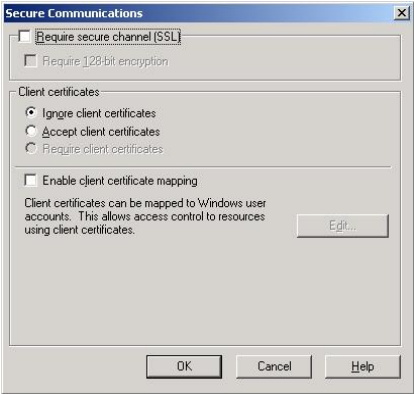
1. En el Administrador de servicios de Internet, seleccionar Propiedades sobre el directorio virtual que utilizará SSL dentro del sitio Web certificado.



2. Seleccione la solapa Seguridad de directorio.



3. Presionar en le botón editar en la sección comunicaciones seguras.



4. Por último seleccione la opción Requiere canal seguro (SSL), adicionalmente puede obligar a los usuarios a autenticarse presentando un certificado digital ante el servidor Web, y a continuación haga clic en Aceptar para completar el proceso.

APENDICE E

CRYPTLIB

Cryptlib es un API para desarrollo aplicaciones de seguridad que permite a programadores inexpertos en criptografía agregar fácilmente servicios de cifrado y autenticación a sus aplicaciones.

Su interfaz de alto nivel permite a cualquier persona agregar encriptación fuerte y capacidades de autenticación a una aplicación en poco tiempo sin necesitar conocer los detalles a bajo nivel que hacen este trabajo. Por esto Cryptlib puede reducir el costo involucrado en agregar seguridad a aplicaciones nuevas y a otras ya existentes.

Cryptlib provee una interfaz transparente a un extenso número de servicios y algoritmos criptográficos usados comúnmente en el mundo de la seguridad, los cuales son accesados a través de interfaces estandarizadas y sencillas, con parámetros seleccionados por el usuario como el algoritmo y el tamaño de la clave.

Incluye como componentes centrales los más populares algoritmos de cifrado convencional como Blowfish, CAST, DES, triple DES, IDEA, RC2, RC4, RC5; algoritmos de resumen como MD2, MD4, MD5, RIPEMD-160, SHA-1 y algoritmos de clave pública como Diffie-Hellman, DSA, ElGamal y RSA.

Algoritmo	Tamaño de clave	Tamaño de bloque
Blowfish	448	64
CAST-128	128	64
DES	56	64
Triple DES	112/168	64
IDEA	128	64
RC2	1024	64
RC4	2048	8
RC5	832	64
Skipjack	80	64
MD2	—	128
MD4	—	128
MD5	—	128
RIPEMD-160	—	160
SHA	—	160
HMAC-MD5	128	128
HMAC-SHA	160	160
HMAC-RIPEMD-160	160	160
Diffie-Hellman	4096	—
DSA	4096	—
ElGamal	4096	—
RSA	4096	—

Tabla 19: Resumen algoritmos y parámetros utilizados por Cryptlib.

A diferencia de productos similares originados en US, Cryptlib no contiene cifrado deliberadamente débil o puertas traseras y permite a todo el mundo el uso de claves de hasta 4096 bits.

Sobre los servicios básicos de cifrado, Cryptlib provee un extenso rango de capacidades de alto nivel, incluyendo manejo completo de certificados X.509 con soporte para todos los aspectos de los certificados PKIX y X.509v3 así como soporte para certificados SET, Microsoft AuthenticCode, S/MIME y SSL de cliente o servidor.

Provee también manejo de CRL y solicitudes de certificación, incluyendo la revisión de certificados contra CRL y servicios que utilicen OCSP. Permite la creación y procesamiento de cadenas de certificados PKCS #7 y un completo rango de funciones de CA

Además del manejo de certificados, Cryptlib provee una interfaz a bases de datos lo cual permite el uso de un extenso y variado rango de bases de datos para almacenar claves, estas van desde Tokens de software PKCS #15 a sistemas de bases de datos relacionales comerciales y directorios LDAP.

Para complementar esto, Cryptlib provee una implementación S/MIME permitiendo a archivos de correo electrónico ser autenticados con firmas digitales, y cifrados en un formato estándar.

Además Cryptlib hace uso de capacidades criptográficas de una extensa variedad de dispositivos criptográficos externos tales como aceleradores criptográficos en hardware, dispositivos PKCS #11 y tarjetas inteligentes.

APENDICE F

MICROSOFT CRYPTOAPI

El API de criptografía de Microsoft o CryptoAPI, provee servicios que permiten a desarrolladores de aplicaciones Win32 agregar funcionalidades de criptografía y manejo de certificados.

Las aplicaciones pueden usar las funciones de la CryptoAPI sin conocer nada acerca de la implementación que existe bajo esta. Así como una aplicación puede usar una librería de gráficos sin saber nada acerca de la configuración del hardware gráfico subyacente.

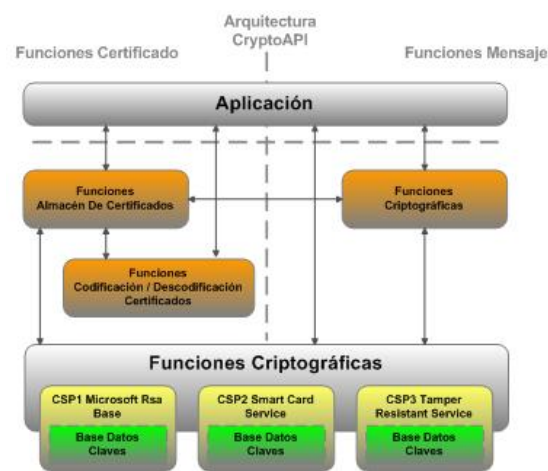


Figura 118: Arquitectura Microsoft CryptoAPI.

La CryptoAPI de Microsoft provee un conjunto de funciones que permite a las aplicaciones encriptar o firmar digitalmente datos en forma flexible, mientras los datos de la clave privada permanecen protegidos. Todas las operaciones criptográficas son realizadas por módulos independientes conocidos como Proveedores de Servicios Criptográficos o CSP¹⁴⁴. Un número de CSP, incluyendo los proveedores Microsoft RSA y DSA/DH son ofrecidos libremente por el sistema operativo.

La CryptoAPI soporta muchos tipos diferentes de CSP. Algunos proveen diferentes juegos de algoritmos criptográficos, mientras otros contienen componentes para interfaces de hardware tales como tarjetas inteligentes.

Cada CSP tiene una base de datos de claves en la cual almacena de forma permanente sus claves criptográficas. Cada base datos de claves contiene uno o más contenedores, cada uno de los cuales contiene todas las claves pertenecientes a un usuario específico. Cada contenedor tiene un nombre único el cual las aplicaciones utilizan para manejar el contenedor de claves.

Las interfaces CryptoAPI pueden también ser accesadas a través de un objeto llamado CAPICOM el cual es construido sobre la CryptoAPI, éste es un COM¹⁴⁵ que realiza funciones criptográficas como firmar datos, verificar firmas, cifrar y descifrar información. CAPICOM puede ser utilizada en aplicaciones que realicen operaciones criptográficas creadas en varios lenguajes de programación tales como Visual Basic o Visual C++.

¹⁴⁴ Cryptographic Service Provider.

¹⁴⁵ Component Object Model.

APENDICE G

CODIGOS FUENTE

En este apéndice se muestra el código fuente de los principales módulos programados para los distintos prototipos desarrollados en la etapa experimental de este trabajo de tesis.

El módulo de interfaz para Visual Basic de la librería Cryptlib utilizada para programar la CA no se incluye en este apéndice.

PROTOTIPO CA

El prototipo de autoridad de certificación esta compuesto principalmente de los siguientes segmentos de código:

- **frmLogin.frm**

En este formulario se encuentra programado el acceso al prototipo mediante la validación de una contraseña proporcionada por el usuario.

Option Explicit

```
Dim LoginOK As Boolean
Dim identificaOK As Boolean
Public BLOQUEAR_CA As Boolean
```

```
Private Sub Form_Load()
Dim describeLog As String
'centrar el formulario
Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
RUTA_BASEDATOS_PASS = App.Path & "\BaseDatos\Pwd.mdb"
RUTA_LOG_APP = creaArchLog
describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " La CA ha iniciado actividad"
If BLOQUEAR_CA Then
frmLogin.Caption = "CA bloqueada"
frmLogin.cmdCancelar.Visible = False
frmLogin.cmdAceptar.Move (1452)
frmLogin.imgLogin.Picture = LoadPicture(App.Path & "\Tarrobloqueado2.ico")
frmLogin.txtLogin.Text = NOMBRE_SESION
frmLogin.txtPassword.TabIndex = 1
describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " La CA ha sido bloqueada"
End If
Call guardaLog(describeLog)
End Sub
```

```
Private Sub cmdCancelar_Click()
Unload Me
End Sub
```

```
Private Sub cmdAceptar_Click()
'comprobar si la contraseña es correcta
Dim consultaSql As String
Dim hashPassword
Dim passwordTabla As String
Dim mensaje
Dim describeLog As String
```

```

identificaOK = False
LoginOK = False
On Error GoTo manejaError
If (Len(txtPassword.Text) = 0) Or (Len(txtLogin.Text) = 0) Then
    mensaje = MsgBox("Debe ingresar un valor en los campos nombre de usuario y
    contraseña." & vbCrLf & _
    "Vuelva a intentarlo", vbExclamation + vbOKOnly, "Error en inicio de sesión")
    describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " Error en inicio de sesión,
    Usuario y Contraseña nulos"
    Call guardaLog(describeLog)
    txtLogin.SetFocus
    SendKeys "{Home}+{End}"
Else
    passwordTabla = obtieneRegistroPass(txtLogin.Text, "Password")
    If passwordTabla = "" Then
        mensaje = MsgBox("El nombre de usuario no existe. vuelva a intentarlo",
        vbCritical, "Usuario no reconocido") 'o el registro se borro y se debe reinstalar
        describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " Error en inicio de sesión,
        Usuario desconocido"
        Call guardaLog(describeLog)
        txtLogin.SetFocus
        SendKeys "{Home}+{End}"
    Else
        LoginOK = True
        hashPassword = HexString(Hash_MD5(txtPassword.Text))
        If hashPassword = passwordTabla Then
            identificaOK = True
            describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " Inicio de sesión OK"
            NOMBRE_SESSION = txtLogin.Text
            Call guardaLog(describeLog)
        Else
            mensaje = MsgBox("La contraseña no es válida. Vuelva a intentarlo",
            vbExclamation + vbOKOnly, "Inicio de sesión")
            describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " Error en inicio de sesión,
            Contraseña incorrecta"
            Call guardaLog(describeLog)
            txtPassword.SetFocus
            SendKeys "{Home}+{End}"
        End If
    End If
End If
If identificaOK Then
    Unload Me
    frmPrincipal.Show
End If
manejaError:
If Err.Number <> 0 Then
    Dim describeError As String
    describeError = "Se ha producido el error, " & CStr(Err.Number) & ", " &
    Err.Description & _
    ", " & Err.Source & ", en el modulo frmlogin"
    Call guardaError(describeError)
End If
End Sub

```

▪ **Frm_CA.frm**

Corresponde al formulario principal de la aplicación y es el que contiene todas las opciones de administración de los certificados.

Option Explicit

```

Private Sub Form_Load()
Dim itmx As ListItem
'Inicializa variables
RUTA_BASEDATOS_PASS = App.Path & "\BaseDatos\Pwd.mdb"
RUTA_BASEDATOS_CA = App.Path & "\BaseDatos\CA.mdb"
RUTA_CERTIFICADOS = App.Path & "\Certificados\"
RUTA_EXPORTADOS = App.Path & "\Exportados\"
RUTA_ALMACEN_CA = App.Path & "\Claves\ca.p15"
RUTA_CRL = App.Path & "\Crl\"
'centrar el formulario
Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
'establece los nodos del treeview
TrVieArbol.Nodes.Add.Root.Text = "Certificados"

```

```

TrVieArbol.Nodes(1).Image = 1
TrVieArbol.Nodes(1).Expanded = True
TrVieArbol.Nodes.Add 1, tvwChild, "CEmitidos", "Emitidos", 2, 3
TrVieArbol.Nodes.Add 1, tvwChild, "CRevocados", "Revocados", 2, 3
TrVieArbol.Nodes.Add 1, tvwChild, "CSolicitudes", "Solicitudes", 2, 3
'inicializa los iconos para listview
LstVieCertificados.SmallIcons = ImgLstListaCerti
'inicia la listview
LstVieCertificados.View = lvwReport
LstVieCertificados.ColumnHeaders.Clear
LstVieCertificados.ColumnHeaders.Add , , "Carpetas"
LstVieCertificados.ListItems.Clear
Set itmX = LstVieCertificados.ListItems.Add(, , "Emitidos", , 3)
Set itmX = LstVieCertificados.ListItems.Add(, , "Revocados", , 3)
Set itmX = LstVieCertificados.ListItems.Add(, , "Solicitudes", , 3)
End Sub

```

```

Private Sub Form_Unload(Cancel As Integer)
Dim respuesta
Dim describeLog As String
    respuesta = MsgBox("¿Desea firmar el archivo de eventos?", vbQuestion + vbYesNo, "Firma
    archivo de eventos")
    If respuesta = vbYes Then
        Call firmaArchivoLog
    End If
    describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " La CA ha detenido su actividad"
    Call guardaLog(describeLog)
End Sub

```

```

Private Sub LstVieCertificados_DblClick()
'verifica si esta sobre un certificado y no sobre una carpeta
Dim cert As New certificate
Select Case TrVieArbol.SelectedItem.Key
    Case Is = "CEmitidos"
        If Not LstVieCertificados.SelectedItem Is Nothing Then
            cert.Import (LstVieCertificados.SelectedItem.SubItems(13))
            cert.Display
        End If
    Case Is = "CRevocados"
        If Not LstVieCertificados.SelectedItem Is Nothing Then
            cert.Import (LstVieCertificados.SelectedItem.SubItems(13))
            cert.Display
        End If
End Select
End Sub

```

```

Private Sub LstVieCertificados_MouseUp(Button As Integer, Shift As Integer, x As Single, y As
Single)
'menu contextual sobre la lista de certificados

    If Button = vbRightButton And Not LstVieCertificados.SelectedItem Is Nothing Then
        Select Case TrVieArbol.SelectedItem.Key
            Case Is = "CEmitidos"
                Me.PopupMenu mnuEmitidos, vbPopupMenuRightButton
            Case Is = "CRevocados"
                Me.PopupMenu mnuRevocados, vbPopupMenuRightButton
        End Select
    End If
End Sub

```

```

Private Sub mnuAbrirEmitido_Click()
Dim cert As New certificate
    If Not LstVieCertificados.SelectedItem Is Nothing Then
        cert.Import (LstVieCertificados.SelectedItem.SubItems(13))
        cert.Display
    End If
End Sub

```

```

Private Sub mnuAbrirRevocado_Click()
Dim cert As New certificate
    If Not LstVieCertificados.SelectedItem Is Nothing Then
        cert.Import (LstVieCertificados.SelectedItem.SubItems(13))
        cert.Display
    End If
End Sub

```

```
End If
End Sub
```

```
Private Sub mnuEliminaEmi_Click()
Dim respuesta
    respuesta = MsgBox("¿Esta seguro que desea eliminar el certificado?", vbQuestion + vbYesNo,
        "Confirmar eliminación de certificado")
    If respuesta = vbYes And Not LstVieCertificados.SelectedItem Is Nothing Then
        Call eliminaCertificado(LstVieCertificados.SelectedItem)
        Call llenaLista("E")
    End If
End Sub
```

```
Private Sub mnuEliminaRev_Click()
Dim respuesta
    respuesta = MsgBox("¿Esta seguro que desea eliminar el certificado?", vbQuestion + vbYesNo,
        "Confirmar eliminación de certificado")
    If respuesta = vbYes And Not LstVieCertificados.SelectedItem Is Nothing Then
        Call eliminaCertificado(LstVieCertificados.SelectedItem)
        Call llenaLista("R")
    End If
End Sub
```

```
Private Sub mnuPublicar_Click()
Dim cert As New certificate
Dim respuesta
Dim nombreCert As String
    respuesta = MsgBox("¿Esta seguro que desea publicar el certificado?" & vbCrLf & vbCrLf _
        & "El certificado sera exportado al directorio Certificados", vbQuestion + vbYesNo,
        "Confirmar exportar certificado")

    If respuesta = vbYes And Not LstVieCertificados.SelectedItem Is Nothing Then
        cert.Import (LstVieCertificados.SelectedItem.SubItems(13))
        nombreCert = LstVieCertificados.SelectedItem.SubItems(4) & "_" &
            CStr(LstVieCertificados.SelectedItem)
        If cert.HasPrivateKey Then
            cert.Save RUTA_CERTIFICADOS & nombreCert & ".pfx", "123",
                CAPICOM_CERTIFICATE_SAVE_AS_PFX, CAPICOM_CERTIFICATE_INCLUDE_END_ENTITY_ONLY
        Else
            cert.Save RUTA_CERTIFICADOS & nombreCert & ".cer", ,
                CAPICOM_CERTIFICATE_SAVE_AS_CER, CAPICOM_CERTIFICATE_INCLUDE_END_ENTITY_ONLY
        End If
    End If
End Sub
```

```
Private Sub mnuExpP12_Click()
    frmPkcs12.Show vbModal, Me
End Sub
```

```
Private Sub mnuPublicaCert_Click()
Dim respuesta
    respuesta = MsgBox("¿Esta seguro que desea publicar los certificados?" & vbCrLf & vbCrLf &
        "Se publicaran todos los certificados emitidos", vbQuestion + vbYesNo, "Confirmar
        publicación de certificados")
    If respuesta = vbYes Then
        Call publicaCertificados
    End If
End Sub
```

```
Private Sub mnuPublicarCRL_Click()
Dim respuesta
    respuesta = MsgBox("¿Esta seguro que desea emitir la CRL?" & vbCrLf & vbCrLf & "La CRL
        contendra todos los certificados actualmente revocados.", vbQuestion + vbYesNo +
        vbDefaultButton1, "Confirme publicación CRL")
    If respuesta = vbYes Then
        Call publicarCRL
    End If
End Sub
```

```
Private Sub mnuRevocaCert_Click()
    If Not LstVieCertificados.SelectedItem Is Nothing Then
```

```

        frmConfirRevoca.PARAM_FORMA = CStr(frmPrincipal.LstVieCertificados.SelectedItem)
        frmConfirRevoca.Show vbModal, Me
        Call llenaLista("E")
    End If
End Sub

```

```

Private Sub mnuAcerca_Click()
    frmAcerca.Show vbModal, Me
End Sub

```

```

Private Sub mnuBloquear_Click()
    frmPrincipal.Hide
    frmLogin.BLOQUEAR_CA = True
    frmLogin.Show vbModal, Me
End Sub

```

```

Private Sub mnuBuscar_Click()
    frmBuscaCert.Show vbModal, Me
End Sub

```

```

Private Sub mnuCerrar_Click()
    Unload Me
    Set frmPrincipal = Nothing
End Sub

```

```

Private Sub mnuContrasena_Click()
    frmCambioContra.Show vbModal, Me
End Sub

```

```

Private Sub mnucreeaCA_Click()
    frmConfigClavesCA.Show
End Sub

```

```

Private Sub mnuEmitir_Click()
    frmEmitirCert.Show vbModal, Me
End Sub

```

```

Private Sub mnuLog_Click()
    frmMuestraLog.Show vbModal, Me
End Sub

```

```

Private Sub mnuOpciones_Click()
    frmOpciones.Show vbModal, Me
End Sub

```

```

Private Sub TlbarPrincipal_ButtonClick(ByVal Button As MSComctlLib.Button)
Dim respuesta
    Select Case Button.Key
        Case Is = "EmiteCert"
            frmEmitirCert.Show vbModal, Me
        Case Is = "EmiteCRL"
            respuesta = MsgBox("¿Esta seguro que desea emitir la CRL?" & vbCrLf & vbCrLf & "La  
CRL contendrá todos los certificados actualmente revocados.", vbQuestion + vbYesNo +  
vbDefaultButton1, "Confirme publicación CRL")
            If respuesta = vbYes Then
                Call publicarCRL
            End If
        Case Is = "BuscaCert"
            frmBuscaCert.Show vbModal, Me
        Case Is = "Configura"
            frmOpciones.Show vbModal, Me
        Case Is = "BloquearCA"
            frmPrincipal.Hide
            frmLogin.BLOQUEAR_CA = True
            frmLogin.Show vbModal, Me
        Case Is = "PublicarTodos"

```

```

        respuesta = MsgBox("¿Esta seguro que desea publicar los certificados?" & vbCrLf &
vbCrLf & "Se publicaran todos los certificados emitidos", vbQuestion + vbYesNo,
"Confirmar publicación de certificados")
    If respuesta = vbYes Then
        Call publicaCertificados
    End If
    Case Is = "FirmaLog"
        Call firmaArchivoLog
    Case Is = "PKCS12"
        frmPkcs12.Show vbModal, Me
    End Select
End Sub

```

```

Private Sub TrVieArbol_NodeClick(ByVal Node As MSComctlLib.Node)
Dim itmx As ListItem
    Select Case Node
    '-----
        Case Is = "Certificados"
            'limpia cabeceras
            LstVieCertificados.ColumnHeaders.Clear
            'limpia filas
            LstVieCertificados.ListItems.Clear
            'establece cabecera
            LstVieCertificados.ColumnHeaders.Add , , "Carpetas"
            'establece filas
            Set itmx = LstVieCertificados.ListItems.Add( , , "Emitidos", , 3)
            Set itmx = LstVieCertificados.ListItems.Add( , , "Revocados", , 3)
            Set itmx = LstVieCertificados.ListItems.Add( , , "Solicitudes", , 3)
            StBarPrincipal.Panels(1).Text = ""
        '-----
        Case Is = "Emitidos"
            'limpia cebeceras
            LstVieCertificados.ColumnHeaders.Clear
            'establece encabezados de la listview
            LstVieCertificados.ColumnHeaders.Add , , "ID"          LstVieCertificados.ColumnHeaders.Add
            , , "Fecha Emisión"
            LstVieCertificados.ColumnHeaders.Add , , "Tipo"
            LstVieCertificados.ColumnHeaders.Add , , "Rut"
            LstVieCertificados.ColumnHeaders.Add , , "Nombre"  LstVieCertificados.ColumnHeaders.Add
            , , "Ciudad"      LstVieCertificados.ColumnHeaders.Add , , "Region"
            LstVieCertificados.ColumnHeaders.Add , , "Unidad Organizacional"
            LstVieCertificados.ColumnHeaders.Add , , "Organización"
            LstVieCertificados.ColumnHeaders.Add , , "Correo" ',
            LstVieCertificados.ColumnHeaders.Add , , "Telefono"
            LstVieCertificados.ColumnHeaders.Add , , "Direccion"
            LstVieCertificados.ColumnHeaders.Add , , "Solicitud"
            LstVieCertificados.ColumnHeaders.Add , , "Certificado" ',
            Call llenaLista("E")
            StBarPrincipal.Panels(1).Text = CStr(LstVieCertificados.ListItems.Count) + "
Certificados Emitidos"
        '-----
        Case Is = "Revocados"
            'limpia cabeceras de listview
            LstVieCertificados.ColumnHeaders.Clear
            'establece encabezados de la listview
            LstVieCertificados.ColumnHeaders.Add , , "ID"  LstVieCertificados.ColumnHeaders.Add , ,
"Fecha Emisión"  LstVieCertificados.ColumnHeaders.Add , , "Tipo"
            LstVieCertificados.ColumnHeaders.Add , , "Rut"  LstVieCertificados.ColumnHeaders.Add ,
, "Nombre"  LstVieCertificados.ColumnHeaders.Add , , "Ciudad"
            LstVieCertificados.ColumnHeaders.Add , , "Region"
            LstVieCertificados.ColumnHeaders.Add , , "Unidad Organizacional"
            LstVieCertificados.ColumnHeaders.Add , , "Organización"
            LstVieCertificados.ColumnHeaders.Add , , "Correo" LstVieCertificados.ColumnHeaders.Add
            , , "Telefono"      LstVieCertificados.ColumnHeaders.Add , , "Dirección"
            LstVieCertificados.ColumnHeaders.Add , , "Solicitud"
            LstVieCertificados.ColumnHeaders.Add , , "Certificado"
            LstVieCertificados.ColumnHeaders.Add , , "Causa Revocación"
            Call llenaLista("R")
            StBarPrincipal.Panels(1).Text = CStr(LstVieCertificados.ListItems.Count) + "
Certificados Revocados"
        '-----
        Case Is = "Solicitudes"
            LstVieCertificados.ListItems.Clear
            StBarPrincipal.Panels(1).Text = CStr(LstVieCertificados.ListItems.Count) + "
Certificados Solicitados"
    End Select
End Sub

```

▪ frmEmitirCert.frm

En este Form se han programado las funciones para emitir los certificados de los usuarios y de servidor.

Option Explicit

Const TIPO_SERVIDOR = 2

Const TIPO_PERSONA = 1

```
Private Sub Form_Load()
'centrar el formulario
    Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
    'inicia combo box politica
    cmbPolitica.ListIndex = 0
    'inicia combo region
    cmbRegion.AddItem ("Primera")
    cmbRegion.AddItem ("Segunda")
    cmbRegion.AddItem ("Tercera")
    cmbRegion.AddItem ("Cuarta")
    cmbRegion.AddItem ("Quinta")
    cmbRegion.AddItem ("R.M.")
    cmbRegion.AddItem ("Sexta")
    cmbRegion.AddItem ("Septima")
    cmbRegion.AddItem ("Octaba")
    cmbRegion.AddItem ("Novena")
    cmbRegion.AddItem ("Decima")
    cmbRegion.AddItem ("Undecima")
    cmbRegion.AddItem ("Duodecima")
    cmbRegion.ListIndex = 0
    'inicia combo region servidor
    cmbServRegion.AddItem ("Primera")
    cmbServRegion.AddItem ("Segunda")
    cmbServRegion.AddItem ("Tercera")
    cmbServRegion.AddItem ("Cuarta")
    cmbServRegion.AddItem ("Quinta")
    cmbServRegion.AddItem ("R.M.")
    cmbServRegion.AddItem ("Sexta")
    cmbServRegion.AddItem ("Septima")
    cmbServRegion.AddItem ("Octaba")
    cmbServRegion.AddItem ("Novena")
    cmbServRegion.AddItem ("Decima")
    cmbServRegion.AddItem ("Undecima")
    cmbServRegion.AddItem ("Duodecima")
    cmbServRegion.ListIndex = 0
End Sub
```

```
Private Sub cmbPolitica_click()
    Select Case cmbPolitica.Text
        Case "Personal"
            txtOrganizacion.Enabled = False
            txtOrganizacion.BackColor = &H8000000F
            txtUniOrg.Enabled = False
            txtUniOrg.BackColor = &H8000000F
        Case "Organizacional"
            txtOrganizacion.Enabled = True
            txtOrganizacion.BackColor = &H80000005
            txtUniOrg.Enabled = True
            txtUniOrg.BackColor = &H80000005
    End Select
End Sub
```

```
Private Sub cmdAceptar_Click()
Dim mensaje
Dim cadenaSolicitud As String
Dim cadenaCertificado As String
Dim cadenaServCertificado As String

    On Error GoTo manejaError
    Select Case STabEmiteCert.Tab
        'solicitud certificado persona
        Case 0
            If txtNombre.Text = "" Then
```

```

        mensaje = MsgBox("Debe ingresar el nombre del titular", vbInformation, "Error en
        datos de usuario")
        txtNombre.SetFocus
    ElseIf txtRut.Text = "" Then
        mensaje = MsgBox("Debe ingresar el rut del titular", vbInformation, "Error en datos
        de usuario")
        txtRut.SetFocus
    ElseIf txtCorreo.Text = "" Then
        mensaje = MsgBox("Debe ingresar una dirección de correo electronico",
        vbInformation, "Error en datos de usuario")
        txtCorreo.SetFocus
    ElseIf txtDireccion.Text = "" Then
        mensaje = MsgBox("Debe ingresar la dirección del titular", vbInformation, "Error en
        datos de usuario")
        txtDireccion.SetFocus
    ElseIf txtTelefono.Text = "" Then
        mensaje = MsgBox("Debe ingresar un número telefonico", vbInformation, "Error en
        datos de usuario")
        txtTelefono.SetFocus
    ElseIf txtCiudad.Text = "" Then
        mensaje = MsgBox("Debe ingresar la ciudad del titular", vbInformation, "Error en
        datos de usuario")
        txtCiudad.SetFocus
    ElseIf cmbRegion.Text = "" Then
        mensaje = MsgBox("Debe ingresar la región del titular", vbInformation, "Error en
        datos de usuario")
        cmbRegion.SetFocus
    ElseIf cmbPolitica.Text = "Organizacional" And txtUniOrg.Text = "" Then
        mensaje = MsgBox("Debe ingresar el nombre de su unidad organizacional",
        vbInformation, "Error en datos de usuario")
        txtUniOrg.SetFocus
    ElseIf cmbPolitica.Text = "Organizacional" And txtOrganizacion.Text = "" Then
        mensaje = MsgBox("Debe ingresar el nombre de su organización", vbInformation,
        "Error en datos de usuario")
        txtOrganizacion.SetFocus
    Else
        If cmbPolitica.Text = "Personal" Then
            cadenaSolicitud = GeneraSolicitud(txtNombre.Text, txtRut.Text, txtCorreo.Text,
            txtCiudad.Text, cmbRegion.Text)
            cadenaCertificado = generaCertificado(cadenaSolicitud, TIPO_PERSONA)
            Call guardaEmisionCertificado("P", txtNombre.Text, txtRut.Text,
            txtDireccion.Text, txtCiudad.Text, cmbRegion.Text, _
            txtCorreo.Text, txtTelefono.Text, cadenaSolicitud, cadenaCertificado)
            Call almacenaCertificado(cadenaCertificado)
            Unload Me
        ElseIf cmbPolitica.Text = "Organizacional" Then
            cadenaSolicitud = GeneraSolicitud(txtNombre.Text, txtRut.Text, txtCorreo.Text,
            txtCiudad.Text, cmbRegion.Text, txtUniOrg.Text, txtOrganizacion.Text)
            cadenaCertificado = generaCertificado(cadenaSolicitud, TIPO_PERSONA)
            Call guardaEmisionCertificado("O", txtNombre.Text, txtRut.Text,
            txtDireccion.Text, txtCiudad.Text, cmbRegion.Text, _
            txtCorreo.Text, txtTelefono.Text, cadenaSolicitud, cadenaCertificado,
            txtUniOrg.Text, txtOrganizacion.Text)
            Call almacenaCertificado(cadenaCertificado)
            Unload Me
        End If
    End If
'solicitud certificado servidor
Case 1
    If txtServNombre.Text = "" Then
        mensaje = MsgBox("Debe ingresar el nombre del titular", vbInformation, "Error en
        datos de usuario")
        txtServNombre.SetFocus
    ElseIf txtServRut.Text = "" Then
        mensaje = MsgBox("Debe ingresar el rut del titular", vbInformation, "Error en datos
        de usuario")
        txtServRut.SetFocus
    ElseIf txtServCorreo.Text = "" Then
        mensaje = MsgBox("Debe ingresar una dirección de correo electronico",
        vbInformation, "Error en datos de usuario")
        txtServCorreo.SetFocus
    ElseIf txtServDireccion.Text = "" Then
        mensaje = MsgBox("Debe ingresar la dirección del titular", vbInformation, "Error en
        datos de usuario")
        txtServDireccion.SetFocus
    ElseIf txtServTelefono.Text = "" Then
        mensaje = MsgBox("Debe ingresar un número telefonico", vbInformation, "Error en
        datos de usuario")
        txtServTelefono.SetFocus
    ElseIf txtServCiudad.Text = "" Then

```

```

        mensaje = MsgBox("Debe ingresar la ciudad del titular", vbInformation, "Error en
        datos de usuario")
        txtServCiudad.SetFocus
    ElseIf cmbServRegion.Text = "" Then
        mensaje = MsgBox("Debe ingresar la región del titular", vbInformation, "Error en
        datos de usuario")
        cmbServRegion.SetFocus
    ElseIf txtServOrgani.Text = "" Then
        mensaje = MsgBox("Debe ingresar la región del titular", vbInformation, "Error en
        datos de usuario")
        txtServOrgani.SetFocus
    ElseIf txtServSolicitud.Text = "" Then
        mensaje = MsgBox("Debe ingresar la región del titular", vbInformation, "Error en
        datos de usuario")
        txtServSolicitud.SetFocus
    Else
        cadenaServCertificado = generaCertificado(txtServSolicitud.Text, TIPO_SERVIDOR)
        Call guardaEmisionCertificado("S", txtServNombre.Text, txtServRut.Text,
        txtServDireccion.Text, txtServCiudad.Text, cmbServRegion.Text, _
        txtServCorreo.Text, txtServTelefono.Text, txtServSolicitud.Text,
        cadenaServCertificado, , txtServOrgani.Text)
        almacenaCertificado(cadenaServCertificado)
        Unload Me
    End If
End Select
manejaError:
    If Err.Number <> 0 Then
        Dim describeError As String
        describeError = "Se ha producido el error, " & CStr(Err.Number) & ", " & Err.Description
        & ", " & Err.Source & ", en el modulo cmdAceptar_Click()"
        Call guardaError(describeError)
        Err.Clear
    End If
End Sub

```

```

Private Sub cmdCancelar_Click()
    Unload Me
End Sub

```

▪ frmPkcs12.frm

En este Form de ha programado la función de exportar las claves de los usuarios y sus certificados en un archivo bajo el formato PKCS #12.

Option Explicit

```

Private Sub Form_Load()
    'centrar el formulario
    Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
    'inicializa los iconos para listview
    LstViePkcs12.SmallIcons = ImgLstPkcs12
    'inicia vista de listview
    LstViePkcs12.View = lvwReport
    'cabeceras listview
    LstViePkcs12.ColumnHeaders.Add , , "ID"
    LstViePkcs12.ColumnHeaders.Add , , "Sujeto"
    LstViePkcs12.ColumnHeaders.Add , , "Emisor"
    LstViePkcs12.ColumnHeaders.Add , , "Valido desde"
    LstViePkcs12.ColumnHeaders.Add , , "Valido Hasta"
    LstViePkcs12.ColumnHeaders.Add , , "Número de serie"
    LstViePkcs12.ColumnHeaders.Add , , "Certificado"
End Sub

```

```

Private Sub cmdCancelar_Click()
    Unload Me
End Sub

```

```

Private Sub cmdExportar_Click()
    Dim mensaje
    Dim respuesta
    Dim nombreCert As String

```

```

Dim describeLog As String
If Not LstViePkcs12.SelectedItem Is Nothing Then
    respuesta = MsgBox("¿Esta seguro que desea exportar el certificado y las claves  
asociadas?" & vbCrLf & vbCrLf _  
& "El certificado sera exportado al directorio Exportados", vbQuestion + vbYesNo,  
"Confirmar exportar certificado")
    If respuesta = vbYes Then
        nombreCert = LstViePkcs12.SelectedItem.SubItems(1) & "_" &  
CStr(LstViePkcs12.SelectedItem)
        If LstViePkcs12.SelectedItem.Tag.HasPrivateKey Then
            LstViePkcs12.SelectedItem.Tag.Save RUTA_EXPORTADOS & nombreCert & ".pfx", "123456",  
CAPICOM_CERTIFICATE_SAVE_AS_PFX, CAPICOM_CERTIFICATE_INCLUDE_END_ENTITY_ONLY
            describeLog = Format(Now(), "d_m_yyyy hh:mm:ss") & " Se ha exportado el  
certificado: " & CStr(LstViePkcs12.SelectedItem)  
Call guardaLog(describeLog)
        Else
            mensaje = MsgBox("El certificado no tiene una clave privada asociada",  
vbExclamation + vbOKOnly, "Error al exportar")
        End If
    End If
End If
End Sub

```

```

Private Sub LstViePkcs12_DblClick()
Dim cert As New certificate
If Not LstViePkcs12.SelectedItem Is Nothing Then
    LstViePkcs12.SelectedItem.Tag.Display
End If
End Sub

```

```

Private Sub cmdBuscar_Click()
Dim baseDatos As Database
Dim tablaDatos As Recordset
Dim consultaSQL As String
Dim cert As New certificate
Dim itmx As ListItem
Dim st As New Store 'almacen win
Dim certs As Certificates
LstViePkcs12.ListItems.Clear
consultaSQL = "SELECT * FROM Certificados WHERE Estado='E' "
Set baseDatos = OpenDatabase(RUTA_BASEDATOS_CA)
Set tablaDatos = baseDatos.OpenRecordset(consultaSQL, dbOpenDynaset)
With tablaDatos
    While Not .EOF
        If Not IsNull(.Fields("Certificado").value) Then
            cert.Import (.Fields("Certificado").value)
            st.Open CAPICOM_CURRENT_USER_STORE, CAPICOM_MY_STORE "My" 'abre almacen win
            Set certs = st.Certificates 'extrae todos lo certificados de ese almacen
            Set certs = certs.Find(CAPICOM_CERTIFICATE_FIND_SHA1_HASH, cert.Thumbprint)
            'encuentro certificados con ese hash deberia ser solo uno
            If txtNombSujeto.Text <> "" Then
                Set certs = certs.Find(CAPICOM_CERTIFICATE_FIND_SUBJECT_NAME,  
txtNombSujeto.Text)
            End If
            If certs.Count <> 0 Then
                For Each cert In certs
                    Set itmx = LstViePkcs12.ListItems.Add(, , .Fields("ID").value, , 2)
                    Set itmx.Tag = cert
                    itmx.SubItems(1) = cert.GetInfo(CAPICOM_CERT_INFO_SUBJECT_SIMPLE_NAME)  
'SubjectName
                    itmx.SubItems(2) = cert.GetInfo(CAPICOM_CERT_INFO_ISSUER_SIMPLE_NAME)  
'IssuerName
                    itmx.SubItems(3) = cert.ValidFromDate
                    itmx.SubItems(4) = cert.ValidToDate
                    itmx.SubItems(5) = cert.SerialNumber
                    itmx.SubItems(6) = .Fields("certificado").value
                Next cert
            End If
        End If
        .MoveNext
    Wend
    .Close
    baseDatos.Close
End With
txtNombSujeto.SetFocus
StBarPkcs12.Panels(1).Text = IIf(IsNull(LstViePkcs12.ListItems.Count), 0,  
LstViePkcs12.ListItems.Count) & " Certificados encontrados"

```

End Sub

▪ mdlFunciones.bas

```
Option Explicit
Public RUTA_LOG_APP As String 'ruta al archivo de acciones relizadas por la aplicación
Public RUTA_LOG_ERROR_APP As String 'ruta al archivo de errores de la aplicación
Public RUTA_BASEDATOS_PASS As String 'ruta a la base de datos con los password
Public RUTA_BASEDATOS_CA As String ' ruta a la base de datos de la CA
Public RUTA_CERTIFICADOS As String 'ruta directorio de certificados
Public RUTA_ALMACEN_CA As String
Public RUTA_CRL As String 'ruta directorio crl
Public RUTA_EXPORTADOS As String
Public NOMBRE_SESSION As String
```

```
Public Sub guardaError(describeError As String)
'Guarda descripcion del error producido por la aplicación
Dim numArchivo As Integer
Dim mensaje As String
numArchivo = FreeFile
On Error Resume Next
Open RUTA_LOG_ERROR_APP For Append Access Write As #numArchivo
Print #numArchivo, Format(Now, "d_m_yyyy hh:mm:ss") & " " & describeError & vbCrLf
Close #numArchivo
mensaje = MsgBox("Se produjo un error y fue almacenado en el archivo de errores",
vbExclamation + vbOKOnly, "Error de Aplicación")
If Err.Number <> 0 Then
mensaje = MsgBox("Error, " + CStr(Err.Number) + " en guardaError(), no se pudo almacenar"
+ " un error en archivo de errores", vbCritical, "Error aplicación")
End If
Err.Clear
End Sub
```

```
Public Sub guardaEmisionCertificado(tipo As String, nombre As String, Rut As String, direccion
As String, ciudad As String, _
region As String, correo As String, telefono As String, solicitud As String, certificado As
String, _
Optional UniOrg As String, Optional organizacion As String)
Dim baseDatos As Database
Dim tablaDatos As Recordset
Dim tablaMaxId As Recordset
Dim describeLog As String
Set baseDatos = OpenDatabase(RUTA_BASEDATOS_CA)
'Open the Contact table
Set tablaDatos = baseDatos.OpenRecordset("SELECT * FROM Certificados", dbOpenDynaset)
Set tablaMaxId = baseDatos.OpenRecordset("SELECT Max(certificados.id) as ID FROM
certificados", dbOpenDynaset)
With tablaDatos
.AddNew
.Fields("ID").value = IIf(IsNull(tablaMaxId.Fields("ID")), 0, tablaMaxId.Fields("ID")) +
1
tablaMaxId.Close
.Fields("Tipo").value = tipo
.Fields("Fecha").value = Date
.Fields("Rut").value = Rut
.Fields("Nombre").value = nombre
.Fields("Direccion").value = direccion
.Fields("Ciudad").value = ciudad
.Fields("Region").value = region
.Fields("Pais").value = "CL"
.Fields("correo").value = correo
.Fields("Telefono").value = telefono
.Fields("Solicitud").value = solicitud
.Fields("Certificado").value = certificado
.Fields("Estado").value = "E"
If Not UniOrg = "" Then
.Fields("Unidad").value = UniOrg
End If
If Not organizacion = "" Then
.Fields("Organizacion").value = organizacion
End If
.Update
.Close
End With
baseDatos.Close
```

```

        describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " Se ha almacenado un nuevo certificado en
        la base de datos"
        Call guardaLog(describeLog)
    End Sub

```

```

Function obtieneRegistroPass(regisBusqueda As String, regisDevolver As String) As String
Dim baseDatos As Database
Dim tablaDatos As Recordset
Set baseDatos = OpenDatabase(RUTA_BASEDATOS_PASS)
Set tablaDatos = baseDatos.OpenRecordset("SELECT " + regisDevolver + " FROM Usuarios WHERE
Login = '" & regisBusqueda & "'", dbOpenDynaset)
If tablaDatos.EOF = True And tablaDatos.EOF Then
    ' no se encontro registro
    obtieneRegistroPass = ""
Else
    obtieneRegistroPass = tablaDatos.Fields("Password").value
End If
tablaDatos.Close
baseDatos.Close
End Function

```

```

Public Sub eliminaCertificado(id As String)
Dim baseDatos As Database
Dim tablaDatos As Recordset
Dim describeLog As String
Set baseDatos = OpenDatabase(RUTA_BASEDATOS_CA)
Set tablaDatos = baseDatos.OpenRecordset("Select * from Certificados Where ID=" & id,
dbOpenDynaset)
With tablaDatos
    .Delete
    describeLog = Format(Now(), "d_m_yyyy hh:mm:ss") & " Se ha eliminado el certificado " &
    id
    .Close
    baseDatos.Close
End With
Call guardaLog(describeLog)
End Sub

```

```

Public Sub revocaCertificado(id As String, causaRevoca As String)
Dim baseDatos As Database
Dim tablaDatos As Recordset
Dim mensajeConfirma
Dim describeLog As String
Set baseDatos = OpenDatabase(RUTA_BASEDATOS_CA)
Set tablaDatos = baseDatos.OpenRecordset("SELECT * FROM Certificados WHERE ID=" & id,
dbOpenDynaset)
With tablaDatos
    .Edit
    .Fields("Estado").value = "R"
    .Fields("Causa").value = causaRevoca
    .Update
    .Close
End With
baseDatos.Close
describeLog = Format(Now, "d_m_yyyy hh:mm:ss") & " Se ha revocado un certificado: " & id
Call guardaLog(describeLog)
End Sub

```

```

Public Function iffTipo(cadIn As String) As String
Select Case cadIn
    Case "O"
        iffTipo = "Organizacional"
    Case "P"
        iffTipo = "Personal"
    Case "S"
        iffTipo = "Servidor"
End Select
End Function

```

```

Public Sub publicarCRL()
Dim errorLib As Long
Dim rutaAlmacen As String
Dim almacenClaves As Long

```

```

Dim clavePriv As Long
Dim objCRL As Long
Dim objCertificado As Long
Dim cadenaCertificado As String
Dim cadenaCrl As String
Dim largoCrl As Long
Dim baseDatos As Database
Dim tablaDatos As Recordset
Dim causaRevoca As Integer
Call cryptInit
'-----ABRE ALMACEN DE CLAVES PRIV/PUB
'abre almacen
errorLib = cryptKeysetOpen(almacenClaves, CRYPT_UNUSED, CRYPT_KEYSET_FILE, RUTA_ALMACEN_CA,
CRYPT_KEYOPT_READONLY)
If errorLib Then Err.Raise 1000 - errorLib, "cryptKeysetOpen", "No se pudo abrir el
almacen de la CA"
errorLib = cryptCreateContext(clavePriv, CRYPT_UNUSED, CRYPT_ALGO_RSA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateContext", "No se pudo crear el
objeto clave privada"
'obtinene clave privada
errorLib = cryptGetPrivateKey(almacenClaves, clavePriv, CRYPT_KEYID_NAME, "Label",
"password")
If errorLib Then Err.Raise 1000 - errorLib, "cryptGetPrivateKey", "No se pudo obtener la
clave privada"
'cierra el almacen
errorLib = cryptKeysetClose(almacenClaves)
If errorLib Then Err.Raise 1000 - errorLib, "cryptKeysetClose", "No se pudo cerrar el
almacen"
'-----CREA OBJETO CERTIFICADO TIPO CRL
errorLib = cryptCreateCert(objCRL, CRYPT_UNUSED, CRYPT_CERTTYPE_CRL)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateCert", "No se pudo crear el
objeto CRL"
Set baseDatos = OpenDatabase(RUTA_BASEDATOS_CA)
Set tablaDatos = baseDatos.OpenRecordset("SELECT * FROM Certificados WHERE Estado='R'",
dbOpenDynaset)
With tablaDatos
While Not .EOF
cadenaCertificado = .Fields("Certificado").value
Select Case .Fields("causa")
Case Is = "Compromiso de la clave"
causaRevoca = CRYPT_CRLREASON_KEYCOMPROMISE
Case Is = "Compromiso de la CA"
causaRevoca = CRYPT_CRLREASON_CACOMPROMISE
Case Is = "Cambio de afiliación"
causaRevoca = CRYPT_CRLREASON_AFFILIATIONCHANGED
Case Is = "Sin especificación"
causaRevoca = CRYPT_CRLREASON_UNSPECIFIED
Case Is = "Cese de operación"
causaRevoca = CRYPT_CRLREASON_CESSATIONOFOPERATION
End Select
'-----CREA OBJETO CERTIFICADO TIPO CERTIFICADO--- errorLib =
cryptCreateCert(objCertificado, CRYPT_UNUSED, CRYPT_CERTTYPE_CERTIFICATE)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateCert", "No se pudo crear el
objeto certificado"
errorLib = cryptImportCert(cadenaCertificado, Len(cadenaCertificado), CRYPT_UNUSED,
objCertificado)
If errorLib Then Err.Raise 1000 - errorLib, "cryptImportCert", "No se pudo importar el
certificado al objeto certificado"
'-----FIJA CERTIFICADO EN LA CRL-----
errorLib = cryptSetAttribute(objCRL, CRYPT_CERTINFO_CERTIFICATE, objCertificado)
If errorLib Then Err.Raise 1000 - errorLib, "cryptSetAttribute", "No se pudo revocar
el certificado"
errorLib = cryptSetAttribute(objCRL, CRYPT_CERTINFO_CRLREASON, causaRevoca)
If errorLib Then Err.Raise 1000 - errorLib, "cryptSetAttribute", "No se pudo fijar el
atributo causa de revocación"
errorLib = cryptDestroyCert(objCertificado)
If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyCert", "No se pudo destruir
el objeto"
.MoveNext
Wend
.Close
End With
baseDatos.Close
'*****FIRMA LA CRL*****
errorLib = cryptSignCert(objCRL, clavePriv)
If errorLib Then Err.Raise 1000 - errorLib, "cryptSignCert", "No se pudo firmar el objeto
CRL"
'*****VERIFICA FIRMA*****
errorLib = cryptCheckCert(objCRL, clavePriv)

```

```

        If errorLib Then Err.Raise 1000 - errorLib, "cryptCheckCert", "No se pudo verificar la
        firma del objeto CRL"
    errorLib = cryptDestroyContext(clavePriv)
    If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyContext", "No se pudo destruir el
    contexto clave privada"
    '*****EXPORTA CRL*****
    cadenaCrl = String(3000, " ")
    errorLib = cryptExportCert(cadenaCrl, largoCrl, CRYPT_CERTFORMAT_CERTIFICATE, objCRL)
    If errorLib Then Err.Raise 1000 - errorLib, "cryptExportCert", "No se pudo exportar el
    objeto CRL"
    '*****DESTRUYE CONTEXTO CLAVES Y CERTIFICADO*****
    errorLib = cryptDestroyCert(objCRL)
    If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyCert", "no se pudo destruir el
    objero CRL"
    Call cryptEnd
    '*****GUARDA CERTIFICADO EN ARCHIVO*****
    Dim numArchivo As Long
    numArchivo = FreeFile
    Open RUTA_CRL & "CRL" & CStr(Format(Date, "d_m_yyyy")) & ".crl" For Output As #numArchivo
    Print #numArchivo, Left(cadenaCrl, largoCrl);
    Close #numArchivo
End Sub

```

```

Public Sub guardaLog(descripcionLog As String)
    Dim numArchivo As Long
    numArchivo = FreeFile
    On Error GoTo CapturaError
    Open RUTA_LOG_APP For Append Access Write Shared As #numArchivo
    Print #numArchivo, descripcionLog
    Close #numArchivo
CapturaError:
    If Err.Number <> 0 Then
        Dim describeError As String
        describeError = "se ha producido el error" & CStr(Err.Number) & ", " & Err.Description &
        ", en el modulo guadaLog()"
        Call guardaError(describeError)
    End If
    Err.Clear
End Sub

```

```

Function EditaRegistroPass(regisBusqueda As String, nuevoValor As String) As Integer
    Dim baseDatos As Database
    Dim tablaDatos As Recordset
    Dim describeLog As String
    Dim consultaSQL As String
    Set baseDatos = OpenDatabase(RUTA_BASEDATOS_PASS)
    consultaSQL = "SELECT * FROM Usuarios WHERE Login = '" + regisBusqueda + "'"
    Set tablaDatos = baseDatos.OpenRecordset(consultaSQL, dbOpenDynaset)
    With tablaDatos
        If .BOF = True And .EOF = True Then
            EditaRegistroPass = 0
        Else
            .Edit
            .Fields("Password").value = nuevoValor
            .Update
            .Close
            EditaRegistroPass = 1
        End If
    End With
    baseDatos.Close
    describeLog = Format(Now(), "d_m_yyyy hh:mm:ss") & " Se ha actualizado la contraseña de
    administración "
    Call guardaLog(describeLog)
End Function

```

```

Public Sub publicaCertificados()
    Dim baseDatos As Database
    Dim tablaDatos As Recordset
    Dim cert As New certificate
    Dim consultaSQL As String
    Dim nombreCert As String
    Dim describeLog As String
    Set baseDatos = OpenDatabase(RUTA_BASEDATOS_CA)
    consultaSQL = "SELECT Nombre, ID, Certificado FROM Certificados WHERE Estado='E' AND
    Certificado IS NOT null"
    Set tablaDatos = baseDatos.OpenRecordset(consultaSQL, dbOpenDynaset)

```

```

With tablaDatos
While Not .EOF
cert.Import (.Fields("Certificado").value)
nombreCert = .Fields("Nombre") & "_" & CStr(.Fields("ID")) & ".cer"
cert.Save RUTA_CERTIFICADOS & nombreCert, , CAPICOM_CERTIFICATE_SAVE_AS_CER,
CAPICOM_CERTIFICATE_INCLUDE_END_ENTITY_ONLY
describeLog = Format(Now(), "d_m_yyyy hh:mm:ss") & " Se ha publicado el certificado: "
& CStr(.Fields("ID"))
Call guardaLog(describeLog)
.MoveNext
Wend
.Close
End With
baseDatos.Close
End Sub

```

```

Function creaArchLog() As String
Dim numArchivo As Long
Dim nombreArchivo As String
numArchivo = FreeFile
nombreArchivo = App.Path & "\Logs\CA_" & Format(Date, "ddmmyyyy") & ".log"
Open nombreArchivo For Append As #numArchivo
Close #numArchivo
creaArchLog = nombreArchivo
End Function

```

```

Public Sub llenaLista(estadoCertificado As String)
Dim itmx As ListItem
Dim baseDatos As Database
Dim tablaDatos As Recordset
Dim iconoCertificado As Integer
'limpia filas listview
frmPrincipal.LstVieCertificados.ListItems.Clear
If estadoCertificado = "R" Then
iconoCertificado = 2
Else
iconoCertificado = 1
End If
Set baseDatos = OpenDatabase(RUTA_BASEDATOS_CA)
'Abre la tabla
Set tablaDatos = baseDatos.OpenRecordset("SELECT * FROM Certificados WHERE Estado='" &
estadoCertificado & "'", dbOpenDynaset)
With tablaDatos
While Not .EOF
'agrega filas y campos a listview
Set itmx = frmPrincipal.LstVieCertificados.ListItems.Add(, , .Fields("ID").value, ,
iconoCertificado)
itmx.SubItems(1) = .Fields("Fecha").value
itmx.SubItems(2) = iffTipo(.Fields("Tipo").value)
itmx.SubItems(3) = .Fields("Rut").value
itmx.SubItems(4) = .Fields("Nombre").value
itmx.SubItems(5) = .Fields("Ciudad").value
itmx.SubItems(6) = .Fields("Region").value
itmx.SubItems(7) = IIf(IsNull(.Fields("Unidad").value), "", .Fields("Unidad").value)
itmx.SubItems(8) = IIf(IsNull(.Fields("Organizacion").value), "",
.Fields("Organizacion").value)
itmx.SubItems(9) = .Fields("Correo").value
itmx.SubItems(10) = .Fields("Telefono").value
itmx.SubItems(11) = .Fields("Direccion").value
itmx.SubItems(12) = .Fields("Solicitud").value
itmx.SubItems(13) = .Fields("Certificado").value
If estadoCertificado = "R" Then
itmx.SubItems(14) = IIf(IsNull(.Fields("Causa").value), "", .Fields("Causa").value)
End If
.MoveNext
Wend
.Close
baseDatos.Close
End With
End Sub

```

▪ MdIFuncionesCAPI.bas

```

Const oidAutenServidor = "1.3.6.1.5.5.7.3.1"
Const oidAutenCliente = "1.3.6.1.5.5.7.3.2"
Const oidFirmaCodigo = "1.3.6.1.5.5.7.3.3"

```

```

Const oidProtecCorreo = "1.3.6.1.5.5.7.3.4"
Const oidIPSecUsuario = "1.3.6.1.5.5.7.3.7"
Const oidEstampTiempo = "1.3.6.1.5.5.7.3.8"
Option Explicit

```

```

Public Function GeneraSolicitud(Nomb As String, Rut As String, Corr As String, Loc As String,
Reg As String, Optional UniOrg As String, Optional Org As String) As String
Dim objEnroll As Object
Dim DN As String
Dim cadenaSolicitud As String
Dim usoClaves As String
Set objEnroll = CreateObject("CEnroll.CEnroll.1")
objEnroll.ProviderType = 1
'proveedor que permite claves de 1024
objEnroll.ProviderName = "Microsoft Enhanced Cryptographic Provider v1.0"
' define las claves como exportables y seguridad media
objEnroll.GenKeyFlags = 3
'define key exchange osea cifrado de claves y datos
objEnroll.KeySpec = 1
'nombre del solicitante
DN = "cn=" & Nomb _
& ", E=" & Corr _
& ", G=" & Rut
If Not UniOrg = "" Then
DN = DN & ", OU=" & UniOrg
End If
If Not Org = "" Then
DN = DN & ", O=" & Org
End If
DN = DN & ", L=" & Loc _
& ", S=" & Reg _
& ", C=CL"
'define el uso de las claves
usoClaves = oidAutenCliente & "," & oidProtecCorreo & "," & oidFirmaCodigo & "," &
oidEstampTiempo
'genera la solicitud
cadenaSolicitud = objEnroll.createPKCS10(DN, usoClaves)
'completa la solicitud
GeneraSolicitud = "-----BEGIN NEW CERTIFICATE REQUEST-----" + vbCrLf + cadenaSolicitud + "---
---END NEW CERTIFICATE REQUEST-----"
Set objEnroll = Nothing
End Function

```

```

Public Sub almacenaCertificado(certificadoPKCS7 As String)
Dim objEnroll As Object
Set objEnroll = CreateObject("CEnroll.CEnroll.1")
objEnroll.acceptPKCS7 (certificadoPKCS7)
Set objEnroll = Nothing
End Sub

```

▪ MdIFunCrypLib.bas

```

Public Sub generaAlmacen(rutaAlmacen As String, tamañoClave As String, etiquetaClave As String,
contraseñaClave As String)
Dim errorLib As Long
Dim contextoRSA As Long
Dim almacenClaves As Long
'*****CREA LAS CLAVES*****
Call cryptInit
'crea contexto de claves públicas y genera las claves
errorLib = cryptCreateContext(contextoRSA, CRYPT_UNUSED, CRYPT_ALGO_RSA)
If errorLib Then Err.Raise 1000 - errorLib, , " cryptCreateContext() en generaAlmacen(),
genero Error Número: " & Str(errorLib)
'fija las propiedades identificacion de clave y tamaño
errorLib = cryptSetAttributeString(contextoRSA, CRYPT_CTXINFO_LABEL, etiquetaClave,
Len(etiquetaClave))
If errorLib Then Err.Raise 1000 - errorLib, , " cryptSetAttributeString() en
generaAlmacen(), genero Error Número: " & Str(errorLib)
'fija el tamaño de las claves (hasta 4096 solamente)
errorLib = cryptSetAttribute(contextoRSA, CRYPT_CTXINFO_KEYSIZE, CLng(tamañoClave) / 8)
If errorLib Then Err.Raise 1000 - errorLib, , " cryptSetAttributeString() en
generaAlmacen(), genero Error Número: " & Str(errorLib)
'genera las claves
errorLib = cryptGenerateKey(contextoRSA)
If errorLib Then Err.Raise 1000 - errorLib, , " cryptGenerateKey() en generaAlmacen(),
genero Error Número: " & Str(errorLib)

```

```

'*****CREA EL ALMACEN DE CLAVES*****
'crea almacen de claves
errorLib = cryptKeysetOpen(almacenClaves, CRYPT_UNUSED, CRYPT_KEYSET_FILE, rutaAlmacen,
CRYPT_KEYOPT_CREATE)
If errorLib Then Err.Raise 1000 - errorLib, , " cryptKeysetOpen() en generaAlmacen(),
genero Error Número: " & Str(errorLib)
'agrega la clave privada y publica al almacen
errorLib = cryptAddPrivateKey(almacenClaves, contextoRSA, contraseñaClave)
If errorLib Then Err.Raise 1000 - errorLib, , " cryptAddPrivateKey() en generaAlmacenCA(),
genero Error Número: " & Str(errorLib)
'destruye contexto rsa
errorLib = cryptDestroyContext(contextoRSA)
If errorLib Then Err.Raise 1000 - errorLib, , " cryptDestroyContext() en
generaAlmacenCA(), genero Error Número: " & Str(errorLib)
'cierra almacen
errorLib = cryptKeysetClose(almacenClaves)
Call cryptEnd
End Sub

```

```

Public Sub generaCertificadoCA(rutaAlmacen As String, contraseñaClave As String, etiquetaClave
As String)
'genera un almacen que contiene las claves privada y pública de la CA
'junto con el certificado digital de esta

Dim errorLib As Long
Dim rutaArchivo As String
Dim almacenClaves As Long
Dim clavePriv As Long
Dim clavePub As Long
Dim objCertificado As Long
Dim DNCertificado As String
Dim certificado As String
Dim largoCertif As Long
Dim numArchivo As Integer

Call cryptInit
'*****BRE ALMACEN DE CLAVES CA*****
errorLib = cryptKeysetOpen(almacenClaves, CRYPT_UNUSED, CRYPT_KEYSET_FILE, rutaArchivo,
CRYPT_KEYOPT_NONE)
If errorLib Then Call determinaError(errorLib, "cryptKeysetOpen")
'crea contexto clave privada
errorLib = cryptCreateContext(clavePriv, CRYPT_UNUSED, CRYPT_ALGO_RSA)
If errorLib Then Call determinaError(errorLib, "cryptCreateContext")
'extrae clave privada
errorLib = cryptGetPrivateKey(almacenClaves, clavePriv, CRYPT_KEYID_NAME, "Label",
"password")
If errorLib Then Call determinaError(errorLib, "cryptGetPublicKey")
'*****CREA OBJETO CERTIFICADO*****
errorLib = cryptCreateCert(objCertificado, CRYPT_UNUSED, CRYPT_CERTTYPE_CERTIFICATE)
If errorLib Then Call determinaError(errorLib, "cryptCreateCert")
'agrega clave publica
errorLib = cryptSetAttribute(objCertificado, CRYPT_CERTINFO_SUBJECTPUBLICKEYINFO, clavePriv)
If errorLib Then Call determinaError(errorLib, "cryptSetAttribute")
'agrega atributos de nombre
DNCertificado = "cn=cvallejos CA CryptLib, ou=investigacion y desarrollo,o=EftGroup, c=CL,
t=Ingeniero Civil Informatico, email=cvallejos@eftbanca.cl, oid.2.5.4.20=(02)-3731393"
errorLib = cryptSetAttributeString(objCertificado, CRYPT_CERTINFO_DN, DNCertificado,
Len(DNCertificado))
If errorLib Then Call determinaError(errorLib, "")
'define certificado autofirmado
errorLib = cryptSetAttribute(objCertificado, CRYPT_CERTINFO_SELF_SIGNED, 1)
If errorLib Then Call determinaError(errorLib, "cryptSetAttribute self signed")
'define certificado es de CA
errorLib = cryptSetAttribute(objCertificado, CRYPT_CERTINFO_CA, 1)
If errorLib Then Call determinaError(errorLib, "cryptSetAttribute")
'agregar atributo duracion
'agregar atributo politicas
'*****FIRMA EL CERTIFICADO*****
errorLib = cryptSignCert(objCertificado, clavePriv)
If errorLib Then Call determinaError(errorLib, "cryptSignCert")
'*****VERIFICA FIRMA (cryptlib entiende que debe usar la parte publica)*****
errorLib = cryptCheckCert(objCertificado, clavePriv)
If errorLib Then Call determinaError(errorLib, "cryptCheckCert")
'*****AGREGA CERTIFICADO KEYSET*****
errorLib = cryptAddPublicKey(almacenClaves, objCertificado)
If errorLib Then Call determinaError(errorLib, "cryptAddPublicKey")
'*****EXPORTA CERTIFICADO*****

```

```

errorLib = cryptExportCert("", largoCertif, CRYPT_CERTFORMAT_TEXT_CERTIFICATE,
objCertificado)
If errorLib Then Call determinaError(errorLib, "")
certificado = String(largoCertif, " ")
errorLib = cryptExportCert(certificado, largoCertif, CRYPT_CERTFORMAT_TEXT_CERTIFICATE,
objCertificado)
If errorLib Then Call determinaError(errorLib, "cryptExportCert")
'***DESTRUYE CONTEXTO CLAVE PRIVADA Y CIERRA ALMACEN**
errorLib = cryptDestroyContext(clavePriv)
errorLib = cryptKeysetClose(almacenClaves)
errorLib = cryptDestroyCert(objCertificado)
Call cryptEnd
txtSolicitud.Text = certificado
txtLargo.Text = "varObj: " + CStr(Len(certificado)) + " varLargo: " + CStr(largoCertif) + "
caja: " + CStr(Len(txtSolicitud.Text))
'*****GUARDA CERTIFICADO EN ARCHIVO*****
numArchivo = FreeFile
Open "certificadoCA.cer" For Output As #numArchivo
Print #numArchivo, certificado;
Close #numArchivo
End Sub

```

```

Public Function generaCertificado(cadenaSolicitud As String, tipoSolicitud As Integer) As
String
Dim errorLib As Long
Dim objSolicitud As Long
Dim objCertificado As Long
Dim almacenCA As Long
Dim contextoRSACA As Long
Dim cadenaCertificado As String
Dim largoCer As Long
Dim numArchivo As Integer
Call cryptInit
'*****CREA OBJETO SOLICITUD*****
errorLib = cryptCreateCert(objSolicitud, CRYPT_UNUSED, CRYPT_CERTTYPE_CERTREQUEST)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateCert", "no se pudo crear el objeto
solicitud"
'*****IMPORTA LA SOLICITUD*****
'importa la solicitud al objeto
errorLib = cryptImportCert(cadenaSolicitud, Len(cadenaSolicitud), CRYPT_UNUSED,
objSolicitud)
If errorLib Then Err.Raise 1000 - errorLib, "cryptImportCert", "no se pudo importar la
solicitud al objeto"
'reviza firma solicitud con la clave publica que esta contiene
errorLib = cryptCheckCert(objSolicitud, CRYPT_UNUSED)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCheckCert", "no se pudo verificar la
firma de la solicitud"
'*****CREA EL CERTIFICADO Y AGREGA SOLICITUD*****
errorLib = cryptCreateCert(objCertificado, CRYPT_UNUSED, CRYPT_CERTTYPE_CERTIFICATE)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateCert", "no se pudo crear el objeto
certificado"
'agregar atributo politicas
errorLib = cryptSetAttributeString(objCertificado, CRYPT_CERTINFO_CERTPOLICYID, "1.2.3.3.3",
Len("1.2.3.3.3"))
If errorLib Then Err.Raise 1000 - errorLib, "cryptSetAttributeString", "no se pudo agregar
el atributo CRYPT_CERTINFO_CERTPOLICYID"
'ubicacion de las CPS
errorLib = cryptSetAttributeString(objCertificado, CRYPT_CERTINFO_CERTPOLICY_CPSURI,
"cvallejos/vallcert/politicas", Len("cvallejos/vallcert/politicas"))
If errorLib Then Err.Raise 1000 - errorLib, "cryptSetAttributeString", "no se pudo agregar
el atributo CRYPT_CERTINFO_CERTPOLICY_ORGANIZATION"
'agrega la información de la solicitud
errorLib = cryptSetAttribute(objCertificado, CRYPT_CERTINFO_CERTREQUEST, objSolicitud)
If errorLib Then Err.Raise 1000 - errorLib, "cryptSetAttribute", "no se pudo agregar la
informacion del objeto solicitud al objeto certificado"
'destruye solicitud
errorLib = cryptDestroyCert(objSolicitud)
If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyCert", "no se pudo destruir el
objeto solicitud"
'*****ABRE ALMACEN CLAVES CA*****
errorLib = cryptKeysetOpen(almacenCA, CRYPT_UNUSED, CRYPT_KEYSET_FILE, App.Path &
"\Claves\ca.p15", CRYPT_KEYOPT_READONLY)
If errorLib Then Err.Raise 1000 - errorLib, "cryptKeysetOpen", "no se pudo abrir el
almacen de la CA"
errorLib = cryptCreateContext(contextoRSACA, CRYPT_UNUSED, CRYPT_ALGO_RSA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateContext", "no se pudo crear el
contexto para las claves de la CA"

```

```

errorLib = cryptGetPrivateKey(almacenCA, contextoRSACA, CRYPT_KEYID_NAME, "Label",
"password")
If errorLib Then Err.Raise 1000 - errorLib, "cryptGetPrivateKey", "no se pudo recuperar la
clave privada desde el almacen de la CA"
errorLib = cryptKeysetClose(almacenCA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptKeysetClose", "no se pudo cerrar el
almacen de la CA"
'*****FIRMA EL CERTIFICADO*****
errorLib = cryptSignCert(objCertificado, contextoRSACA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptSignCert", "no se pudo firmar el
certificado"
'*****VERIFICA FIRMA*****
errorLib = cryptCheckCert(objCertificado, contextoRSACA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCheckCert", "no se pudo verificar la
firma"
errorLib = cryptDestroyContext(contextoRSACA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyContext", "no se pudo destruir el
contexto de la clave de la CA"
'*****EXPORTA CERTIFICADO A CADENA*****
'reserva espacio para el certificado
cadenaCertificado = String(3000, " ")
errorLib = cryptExportCert(cadenaCertificado, largoCer, CRYPT_CERTFORMAT_TEXT_CERTIFICATE,
objCertificado)
If errorLib Then Err.Raise 1000 - errorLib, "cryptExportCert", "no se pudo exportar el
certificado a la cadena"
errorLib = cryptDestroyCert(objCertificado)
If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyCert", "no se pudo destruir el
objeto certificado"
Call cryptEnd
generaCertificado = Left(cadenaCertificado, largoCer)
End Function

```

```

Function Hash_MD5(Source As String) As String
' calcula hash MD5 de una cadena
Dim context As Long
Dim MyLength As Long
Dim MyString As String
Dim errCode As Long
Call cryptInit
errCode = cryptCreateContext(context, CRYPT_UNUSED, CRYPT_ALGO_MD5)
If (errCode < CRYPT_OK) Then
Err.Raise 1000 - errCode, , "cryptCreateContext returned " & Str(errCode)
End If
errCode = cryptEncrypt(context, Source, Len(Source))
If (errCode < CRYPT_OK) Then
Err.Raise 1000 - errCode, , "cryptEncrypt returned " & Str(errCode)
End If
'indica que no se ingresaran mas datos
errCode = cryptEncrypt(context, "", 0)
If (errCode < CRYPT_OK) Then
Err.Raise 1000 - errCode, , "cryptEncrypt returned " & Str(errCode)
End If
MyString = String(CRYPT_MAX_HASHSIZE, " ")
errCode = cryptGetAttributeString(context, CRYPT_CTXINFO_HASHVALUE, MyString, MyLength)
If (errCode < CRYPT_OK) Then
Err.Raise 1000 - errCode, , "cryptGetAttributeString returned " & Str(errCode)
End If
errCode = cryptDestroyContext(context)
If (errCode < CRYPT_OK) Then
Err.Raise 1000 - errCode, , "cryptDestroyContext returned " & Str(errCode)
End If
Call cryptEnd
Hash_MD5 = Left$(MyString, MyLength)
End Function

```

```

Function HexString(Source As String) As String
'convierte una cadena en una secuencia de codigo hexa
Dim Result As String
Dim i As Integer
Result = ""
For i = 1 To Len(Source)
Result = Result & Right$("00" & Hex(Asc(Mid$(Source, i, 1))), 2) & " "
Next i
HexString = Result
End Function

```

```

Public Sub firmaArchivoLog()
Dim errorLib As Long
Dim almacenCA As Long
Dim contextoRSACA As Long
Dim contextoHash As Long
Dim hashBin As String 'firma en binario
Dim largoHash As Long
Dim hashHexa As String
Dim firmaBin As String
Dim largoFirma As Long
Dim numArchivo As Long
Dim lineaArchivo As String 'linea del log
Dim cadenaFirmar As String 'cadena de texto que se firmara
Dim firmaLog As String 'resultado de la firma en hexa
numArchivo = FreeFile
Open RUTA_LOG_APP For Input As #numArchivo
While Not EOF(numArchivo)
Line Input #numArchivo, lineaArchivo
cadenaFirmar = cadenaFirmar & lineaArchivo & vbCrLf
Wend
Close #numArchivo
If Not IsNull(cadenaFirmar) Then
Call cryptInit
'*****ABRE ALMACEN CLAVES CA*****
errorLib = cryptKeysetOpen(almacenCA, CRYPT_UNUSED, CRYPT_KEYSET_FILE, RUTA_ALMACEN_CA,
CRYPT_KEYOPT_READONLY)
If errorLib Then Err.Raise 1000 - errorLib, "cryptKeysetOpen", "no se pudo abrir el
almacen de la CA"
errorLib = cryptCreateContext(contextoRSACA, CRYPT_UNUSED, CRYPT_ALGO_RSA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateContext", "no se pudo crear el
contexto para las claves de la CA"
errorLib = cryptGetPrivateKey(almacenCA, contextoRSACA, CRYPT_KEYID_NAME, "Label",
"password")
If errorLib Then Err.Raise 1000 - errorLib, "cryptGetPrivateKey", "no se pudo recuperar la
clave privada desde el almacen de la CA"
errorLib = cryptKeysetClose(almacenCA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptKeysetClose", "no se pudo cerrar el
almacen de la CA"
'*****CREA EL RESUMEN*****
errorLib = cryptCreateContext(contextoHash, CRYPT_UNUSED, CRYPT_ALGO_MD5)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateContext", "No se pudo crear el
contexto Hash"
errorLib = cryptEncrypt(contextoHash, cadenaFirmar, Len(cadenaFirmar))
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateContext", "No se pudo cargar los
datos en el contexto Hash"
errorLib = cryptEncrypt(contextoHash, cadenaFirmar, 0)
If errorLib Then Err.Raise 1000 - errorLib, "cryptEncrypt", "No se pudo crear el contexto
MD5"
'*RESERVA ESPACIO PARA FIRMA Y CREA RESUMEN
firmaBin = String(1000, " ")
errorLib = cryptCreateSignature(firmaBin, largoFirma, contextoRSACA, contextoHash)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCreateSignature", "No se pudo crear la
firma"
'*****VERIFICA FIRMA*****
errorLib = cryptCheckSignature(Left(firmaBin, largoFirma), contextoRSACA, contextoHash)
If errorLib Then Err.Raise 1000 - errorLib, "cryptCheckSignature", "No se pudo verificar
la firma"
errorLib = cryptDestroyContext(contextoRSACA)
If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyContext", "No se pudo destruir el
contexto RSACA"
errorLib = cryptDestroyContext(contextoHash)
If errorLib Then Err.Raise 1000 - errorLib, "cryptDestroyContext", "No se pudo destruir el
contexto Hash"
Call cryptEnd
firmaLog = Trim(HexString(Left(firmaBin, largoFirma)))
numArchivo = FreeFile
Open RUTA_LOG_APP For Append As #numArchivo
Print #numArchivo, "-----INICIO FIRMA-----"
Print #numArchivo, firmaLog
Close #numArchivo
End If
End Sub

```

PROTOTIPO AUTENTIFICADOR DE DOCUMENTOS

La aplicación de firma y cifrado de documentos digitales esta compuesto principalmente de los siguientes Forms.

- **frmPrincipal.frm**

Este es el formulario que contiene todas las funcionalidades del prototipo.

```
Option Explicit
Dim almacen As New Store
Dim certs As Certificates
Dim selectedCerts As Certificates
Dim certificado As Certificate
Dim firmante As New Signer
Public firmaCodigo As New SignedCode

Private Sub drvDisco_Change()
    On Error GoTo manejaError
    dirCarpetas.Path = drvDisco.Drive & "\"
    Exit Sub
manejaError:
    MsgBox Hex(Err.Number) & ": " & Err.Description
    Exit Sub
End Sub

Private Sub fleArchivos_Click()
    On Error GoTo manejaError
    txtRuta.Text = fleArchivos.Path & "\" & fleArchivos.FileName
    Exit Sub
manejaError:
    MsgBox Hex(Err.Number) & ": " & Err.Description
    Exit Sub
End Sub

Private Sub Form_Load()
    'centrar el formulario
    Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
    'filtro tipo de archivos aceptados
    fleArchivos.Pattern = "*.txt"
    'rut al archivo de errores
    RUTA_LOG_ERROR_APP = App.Path & "\error.log"
    'abre el almacen del usuario actual y extrae los certificados
    almacen.Open CAPICOM_CURRENT_USER_STORE, CAPICOM_MY_STORE, CAPICOM_STORE_OPEN_READ_ONLY
    Set certs = almacen.Certificates
End Sub

Private Sub mnuAcerca_Click()
    frmAcerca.Show vbModal, Me
End Sub

Private Sub mnuSalir_Click()
    Unload Me
End Sub

Private Sub cmdSalir_Click()
    Set almacen = Nothing
    Set certs = Nothing
    Set selectedCerts = Nothing
    Set certificado = Nothing
    Set firmante = Nothing
    Set firmaCodigo = Nothing
    Unload Me
End Sub
```

```

Private Sub TlbarOpciones_ButtonClick(ByVal Button As MSComctlLib.Button)
Dim mensaje
Dim respuesta
On Error GoTo manejaError
Select Case Button.Key
'-----
Case Is = "Firmar"
If txtRuta.Text <> "" Then
If fleArchivos.Pattern = "*.exe;*.dll" Then
firmaCodigo.FileName = txtRuta.Text
frmInfo.FIJAR = True
frmInfo.Show vbModal, Me
Set certs = certs.Find(CAPICOM_CERTIFICATE_FIND_KEY_USAGE,
CAPICOM_DIGITAL_SIGNATURE_KEY_USAGE).Find(CAPICOM_CERTIFICATE_FIND_TIME_VALID).Find
(CAPICOM_CERTIFICATE_FIND_EXTENDED_PROPERTY, CAPICOM_PROPID_KEY_SPEC)
firmante.Certificate = certs.Select.Item(1)
firmaCodigo.Sign firmante
If Err.Number = 0 Then
mensaje = MsgBox("El archivo ha sido firmado exitosamente", vbInformation +
vbOKOnly, "Proceso terminado")
End If
ElseIf fleArchivos.Pattern = "*.txt" Then
frmArchivo.RUTA_ARCHIVO = txtRuta.Text
frmArchivo.FIRMAR = True
frmArchivo.Show vbModal, Me
End If
End If
'-----
Case Is = "Verificar"
If txtRuta.Text <> "" Then
firmaCodigo.FileName = txtRuta.Text
If fleArchivos.Pattern = "*.exe;*.dll" Then
firmaCodigo.Verify
respuesta = MsgBox("La firma del archivo ha sido verificada " & vbCrLf & vbCrLf _
& "¿Desea ver información del firmante?", vbInformation + vbYesNo, "Verificación de
firma digital")
If respuesta = vbYes Then
If Not firmaCodigo.Signer Is Nothing Then
frmInfo.FIJAR = False
frmInfo.Show vbModal, Me
firmaCodigo.Signer.Certificate.Display
Else
mensaje = MsgBox("El archivo no ha sido firmado", vbInformation + vbOKOnly,
"Error en el procedimiento")
End If
End If
ElseIf fleArchivos.Pattern = "*.txt" Then
frmArchivo.RUTA_ARCHIVO = txtRuta.Text
frmArchivo.FIRMAR = False
frmArchivo.Show vbModal, Me
End If
End If
'-----
Case Is = "Cifrar"
If txtRuta.Text <> "" And fleArchivos.Pattern <> "*.env" Then
frmEnvolver.RUTA_ARCHIVO = txtRuta.Text
frmEnvolver.Show vbModal, Me
End If
'-----
Case Is = "Descifrar"
If txtRuta.Text <> "" Then
If fleArchivos.Pattern = "*.env" Then
frmDescifrar.RUTA_ARCHIVO = txtRuta.Text
frmDescifrar.Show vbModal, Me
End If
End If
'-----
Case Is = "Tipo"
txtRuta.Text = ""
fleArchivos.Pattern = "*.txt"
End Select
manejaError:
If Err.Number <> 0 Then
Dim describeError As String
Select Case Err.Number
Case -2146762486
mensaje = MsgBox("No se encontro una autoridad de confianza que avale este
certificado", vbExclamation + vbOKOnly, "Error en la cadena de certificación")
Case -2146762748

```

```

        mensaje = MsgBox("Ha decidido no confiar en este codigo", vbInformation +
        vbOKOnly, "Error en el certificado")
    Case -2138570157
        mensaje = MsgBox("El certificado no es valido para firmar codigo, debe solicitar
        un certificado digital", vbInformation + vbOKOnly, "Error en el certificado")
    Case -2138570191
        mensaje = MsgBox("El almacen esta vacio, debe solicitar un certificado digital",
        vbInformation + vbOKOnly, "Error en el procedimiento")
    Case -2138569887
        mensaje = MsgBox("Este archivo no ha sido firmado", vbInformation + vbOKOnly,
        "Error en la verificación")
    Case CAPICOM_E_CANCELLED
        mensaje = MsgBox("para firmar debe seleccionar un certificado ", vbInformation +
        vbOKOnly, "Error en el procedimiento")
    Case Else
        mensaje = MsgBox("Se ha encontrado un error, " _
        & Err.Description, vbCritical + vbOKOnly, "Error en la aplicación")
        describeError = "Error en de aplicación, N°: " & CStr(Err.Number) & ", " &
        Err.Description & ", " & Err.Source
        Call guardaError(describeError)
    End Select
    Err.Clear
End If
End Sub

```

```

Private Sub dirCarpetas_Change()
    On Error GoTo manejaError
    fleArchivos.Path = dirCarpetas.Path
    txtRuta.Text = ""
    Exit Sub
manejaError:
    MsgBox Hex(Err.Number) & ": " & Err.Description
End Sub

```

```

Private Sub TlbarOpciones_ButtonMenuClick(ByVal ButtonMenu As MSComctlLib.ButtonMenu)
    Select Case ButtonMenu.Key
        Case Is = "Datos"
            txtRuta.Text = ""
            fleArchivos.Pattern = "*.txt"
        Case Is = "Codigo"
            txtRuta.Text = ""
            fleArchivos.Pattern = "*.exe;*.dll"
        Case Is = "Cifrado"
            txtRuta.Text = ""
            fleArchivos.Pattern = "*.env"
    End Select
End Sub

```

▪ frmArchivo.frm

Este Form se encarga de verificar o de firmar los archivos de texto.

```

Option Explicit
Public RUTA_ARCHIVO As String
Public FIRMAR As Boolean
Const CABECERAFIRMA = "-----INICIO FIRMA-----"
Const CIERRAFIRMA = "-----FIN FIRMA-----"
Dim ESTA_FIRMADO As Boolean

```

```

Private Sub Form_Load()
    Dim numArchivo As Long
    Dim lineaArchivo As String
    Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
    If FIRMAR Then
        cmdAceptar.Caption = "&Firmar"
        frmArchivo.Icon = LoadPicture(App.Path + "\firmadoc.ico")
    Else
        cmdAceptar.Caption = "&Verificar"
        frmArchivo.Icon = LoadPicture(App.Path + "\verificadoc.ico")
    End If
    numArchivo = FreeFile
    Open RUTA_ARCHIVO For Input As #numArchivo
    While Not EOF(numArchivo)

```

```

        Input #numArchivo, lineaArchivo
        txtArchivo.Text = txtArchivo.Text & lineaArchivo & vbCrLf
    Wend
    Close #numArchivo
End Sub

```

```

Private Sub cmdCerrar_Click()
    Unload Me
End Sub

```

```

Private Sub cmdAceptar_Click()
    Dim numArchivoLee As Long
    Dim numArchivoFirma As Long
    Dim lineaArchivo As String
    Dim textoFirmar As String
    Dim textoVerificar As String
    Dim textoFirma As String
    Dim firmante As New Signer
    Dim almacen As New Store
    Dim certs As New Certificates
    Dim objetoFirma As New SignedData
    Dim estampadoTiempo As New CAPICOM.Attribute
    Dim finTextoVerificar As Boolean
    Dim finTextoFirma As Boolean
    Dim mensaje
    Dim respuesta
    On Error GoTo manejaError
    If FIRMAR Then
        numArchivoLee = FreeFile
        Open RUTA_ARCHIVO For Input As #numArchivoLee
        While Not EOF(numArchivoLee)
            Input #numArchivoLee, lineaArchivo
            If lineaArchivo = "-----INICIO FIRMA-----" Then ESTA_FIRMADO = True
            textoFirmar = textoFirmar & lineaArchivo & vbCrLf
        Wend
        Close #numArchivoLee
        If textoFirmar = "" Then
            mensaje = MsgBox("El archivo no tiene datos a firmar", vbInformation + vbOKOnly, "Error en archivo")
        ElseIf Not ESTA_FIRMADO Then
            almacen.Open CAPICOM_CURRENT_USER_STORE, CAPICOM_MY_STORE, CAPICOM_STORE_OPEN_READ_ONLY
            'busca certificados validos para firmar
            Set certs = almacen.Certificates.Find(CAPICOM_CERTIFICATE_FIND_KEY_USAGE, CAPICOM_DIGITAL_SIGNATURE_KEY_USAGE).Find(CAPICOM_CERTIFICATE_FIND_TIME_VALID).Find(CAPICOM_CERTIFICATE_FIND_EXTENDED_PROPERTY, CAPICOM_PROPID_KEY_SPEC)
            firmante.Certificate = certs.Select().Item(1) 'muestra ventana seleccion cert con los validos
            If Not IsNull(firmante.Certificate) Then
                objetoFirma.Content = textoFirmar
                estampadoTiempo.Name = CAPICOM_AUTHENTICATED_ATTRIBUTE_SIGNING_TIME
                estampadoTiempo.Value = Now
                firmante.AuthenticatedAttributes.Add estampadoTiempo
                textoFirma = objetoFirma.Sign(firmante, True, CAPICOM_ENCODE_BASE64)
                numArchivoFirma = FreeFile
                Open RUTA_ARCHIVO For Append As #numArchivoFirma
                Print #numArchivoFirma, CABECERAFIRMA
                Print #numArchivoFirma, textoFirma
                Print #numArchivoFirma, CIERRAFIRMA
                Close #numArchivoFirma
                mensaje = MsgBox("El proceso de firma a termiando corectamente", vbInformation + vbOKOnly, "Proceso finalizado")
            End If
        Else
            mensaje = MsgBox("El archivo ya esta firmado", vbInformation + vbOKOnly, "información de aplicación")
        End If
    Else 'Verificar el archivo
        numArchivoLee = FreeFile
        Open RUTA_ARCHIVO For Input As #numArchivoLee
        While Not EOF(numArchivoLee) 'And lineaArchivo <> CABECERAFIRMA
            Input #numArchivoLee, lineaArchivo
            If lineaArchivo = CABECERAFIRMA Then
                finTextoVerificar = True
            ElseIf lineaArchivo = CIERRAFIRMA Then
                finTextoFirma = True
            End If
        Wend
    End Sub

```

```

        If Not finTextoVerificar Then
            textoVerificar = textoVerificar & lineaArchivo & vbCrLf
        ElseIf Not finTextoFirma And lineaArchivo <> CABECERAFIRMA Then
            textoFirma = textoFirma & lineaArchivo
        End If
    Wend
Close #numArchivoLee
If Not finTextoVerificar Or Not finTextoFirma Then
    mensaje = MsgBox("El archivo no tiene el formato requerido o no esta firmado ",
        vbInformation + vbOKOnly, "Error en el archivo")
Else
    objetoFirma.Content = textoVerificar
    objetoFirma.Verify textoFirma, True, CAPICOM_VERIFY_SIGNATURE_AND_CERTIFICATE
    If Err.Number = 0 Then
        respuesta = MsgBox("La verificación ha sido realizada en forma correcta" & vbCrLf &
            & "¿Desea ver el certificado del firmante?", vbInformation + vbYesNo, "Proceso
            finalizado")
        If respuesta = vbYes Then
            objetoFirma.Certificates.Item(1).Display
        End If
    End If
End If
End If
Set objetoFirma = Nothing
Set almacen = Nothing
Set certs = Nothing
Set firmante = Nothing
Set estampadoTiempo = Nothing
manejaError:
If Err.Number <> 0 Then
    Dim describeError As String
    Select Case Err.Number
        Case -2146762486
            mensaje = MsgBox("No se encontro una autoridad de confianza que avale este
            certificado", vbExclamation + vbOKOnly, "Error en la cadena de certificación")
        Case -2147024809
            mensaje = MsgBox("El archivo debe contener datos", vbExclamation + vbOKOnly, "Error en
            el archivo a firmar")
        Case -2146893802
            mensaje = MsgBox("Error al abrir el almacen de certificados", vbExclamation +
            vbOKOnly, "Error en el proceso")
        Case -2146881277
            mensaje = MsgBox("No se pudo verificar la firma, la firma ha sido alterada",
            vbExclamation + vbOKOnly, "Verificación de firma incorrecta")
        Case -2146889721
            mensaje = MsgBox("No se pudo verificar la firma, el valor hash no concuerda",
            vbExclamation + vbOKOnly, "Verificación de firma incorrecta")
        Case -2138569887
            mensaje = MsgBox("Este archivo no ha sido firmado", vbInformation + vbOKOnly, "Error
            en la verificación")
        Case CAPICOM_E_CANCELLED
            mensaje = MsgBox("Debe seleccionar un certificado para firmar", vbInformation +
            vbOKOnly, "Error en el procedimiento")
        Case Else
            mensaje = MsgBox("Se ha encontrado un error en el archivo" & Err.Description & ", " &
            Err.Source, vbCritical + vbOKOnly, "Error en el archivo")
            describeError = "Error de aplicación, N°: " & CStr(Err.Number) & ", " &
            Err.Description & ", " & Err.Source
            Call guardaError(describeError)
        End Select
    End If
    Err.Clear
End If
End Sub

```

▪ frmEnvolver.frm

En este Form se encuentran las funciones de cifrado de los mensajes de texto.

```

Option Explicit
Public RUTA_ARCHIVO As String
Dim RUTA_ARCHIVO_DESTINO As String

```

```

Private Sub Form_Load()
    Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
    'inicia cuadro dialogo

```

```

    With CnDDestino
        .DialogTitle = "Archivo destino de envoltura"
        .DefaultExt = "*.env"
        .Flags = cdloFNOverwritePrompt Or cdloFNPathMustExist Or cdloFNExtensionDifferent
        .Filter = "Envoltura (*.env)|*.env"
        .InitDir = App.Path
    End With
End Sub

```

```

Private Sub cmdDestino_Click()
    With CnDDestino
        .ShowSave
        txtArchDestino.Text = .FileName
    End With
    RUTA_ARCHIVO_DESTINO = txtArchDestino.Text
End Sub

```

```

Private Sub cmdAceptar_Click()
Dim numArchivoEnv As Long
Dim numArchivoGuardar As Long
Dim ruta_archivo_salida As String
Dim lineaArchivo As String
Dim archEnvolver As String
Dim mensajeEnvuelto As String
Dim almacen As New Store
Dim almacenIntermedios As New Store
Dim Envoltura As New EnvelopedData
Dim certs As Certificates
Dim certSeleccionados As Certificates
Dim certificado As Certificate
Dim i As Integer
Dim mensaje
    On Error GoTo manejaError
    If txtArchDestino.Text = "" Then
        mensaje = MsgBox("Debe seleccionar un archivo de destino para almacenar los datos cifrados", vbExclamation + vbOKOnly, "Solicitud de información")
    Else
        'abrir archivo a envolver
        numArchivoEnv = FreeFile
        Open RUTA_ARCHIVO For Input As #numArchivoEnv
        While Not EOF(numArchivoEnv)
            Line Input #numArchivoEnv, lineaArchivo
            archEnvolver = archEnvolver + lineaArchivo + vbCrLf
        Wend
        Close #numArchivoEnv
        If IsNull(archEnvolver) Then
            mensaje = MsgBox("el archivo esta vacio.", vbInformation + vbOKOnly, "Error en el archivo")
            Exit Sub
        End If
        'abre almacen de los posibles destinatarios del mensaje "almacen OTROS"
        almacen.Open CAPICOM_CURRENT_USER_STORE, CAPICOM_OTHER_STORE, CAPICOM_STORE_OPEN_READ_ONLY
        almacenIntermedios.Open CAPICOM_CURRENT_USER_STORE, CAPICOM_CA_STORE, CAPICOM_STORE_OPEN_READ_ONLY
        Set certs = almacen.Certificates
        Set almacen = Nothing
        If almacenIntermedios.Certificates.Count > 0 Then
            For i = 1 To almacenIntermedios.Certificates.Count
                certs.Add almacenIntermedios.Certificates.Item(i)
            Next i
            Set almacenIntermedios = Nothing
        End If
        If certs.Count < 1 Then
            mensaje = MsgBox("No hay certificados en almacen OTROS e INTERMEDIOS.", vbInformation + vbOKOnly, "Error al abri almacen")
            Exit Sub
        End If
        ' almacena el contenido a envolver
        Envoltura.Content = archEnvolver
        Set certSeleccionados = certs.Select("Destinatarios", "Determina los individuos que podran decifrar el archivo", True)
        For Each certificado In certSeleccionados
            Envoltura.Recipients.Add certificado
        Next certificado
        Envoltura.Algorithm.Name = CAPICOM_ENCRYPTION_ALGORITHM_3DES
        Envoltura.Algorithm.KeyLength = CAPICOM_ENCRYPTION_KEY_LENGTH_MAXIMUM
    End If
End Sub

```

```

'cifra el mensaje, la cadena tienen toda la información para descifrar
mensajeEnvuelto = Envoltura.Encrypt
If Len(mensajeEnvuelto) < 1 Then
    mensaje = MsgBox("el archivo no fue cifrado. ", vbCritical + vbOKOnly, "Error al
cifra rel archivo")
Else
    numArchivoGuardar = FreeFile
    Open RUTA_ARCHIVO_DESTINO For Output As #numArchivoGuardar
        Print #numArchivoGuardar, mensajeEnvuelto
    Close #numArchivoGuardar
    mensaje = MsgBox("El mensaje fue almacenado", vbInformation + vbOKOnly, "Fin del
proceso")
End If
Set Envoltura = Nothing
Set almacen = Nothing
Unload Me
End If
Exit Sub
manejaError:
If Err.Number <> 0 Then
    Dim describeError As String
    Select Case Err.Number
        Case -2138570109
            mensaje = MsgBox("No se encuentra una clave valida para descifrar este archivo",
vbExclamation + vbOKOnly, "Destinatario incorrecto")
        Case -2146762748
            mensaje = MsgBox("Ha decidido no confiar en este codigo", vbInformation + vbOKOnly,
"Error en el certificado")
        Case -2138570157
            mensaje = MsgBox("El certificado no es valido para firmar codigo, debe solicitar un
certificado digital", vbInformation + vbOKOnly, "Error en el certificado")
        Case -2138570191
            mensaje = MsgBox("El almacen esta vacio, debe solicitar un certificado digital",
vbInformation + vbOKOnly, "Error en el procedimiento")
        Case -2138569887
            mensaje = MsgBox("Este archivo no ha sido firmado", vbInformation + vbOKOnly, "Error
en la verificación")
        Case CAPICOM_E_CANCELLED
            mensaje = MsgBox("debe seleccionar un certificado como destinatario ", vbInformation
+ vbOKOnly, "Error en el procedimiento")
        Case Else
            mensaje = MsgBox("Se ha encontrado un error, " _
& Err.Description, vbCritical + vbOKOnly, "Error en la aplicación")
            describeError = "Error en de aplicación, N°: " & CStr(Err.Number) & ", " &
Err.Description & ", " & Err.Source
            Call guardaError(describeError)
    End Select
    Err.Clear
End If
End Sub

```

▪ frmDescifrar.frm

En este Form se almacena el código para el descifrado de los archivos.

```

Option Explicit
Public RUTA_ARCHIVO As String
Dim RUTA_ARCHIVO_DESTINO As String

Private Sub Form_Load()
    Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
    'inicia cuadro dialogo
    With CnDDestino
        .DialogTitle = "Archivo destino de envoltura"
        .DefaultExt = "*.env"
        .Flags = cdIOFNOOverwritePrompt Or cdIOFNPathMustExist Or cdIOFNExtensionDifferent
        .Filter = "texto (*.txt)|*.txt"
        .InitDir = App.Path
    End With
End Sub

Private Sub cmdDestino_Click()
    With CnDDestino
        .ShowSave
    End With
End Sub

```

```

        txtArchDestino.Text = .FileName
    End With
    RUTA_ARCHIVO_DESTINO = txtArchDestino.Text
End Sub

```

```

Private Sub cmdAceptar_Click()
Dim numArchivoCif As Long
Dim numArchivoGuardar As Long
Dim lineaArchivo As String
Dim archivoCifrado As String
Dim mensajeEnvuelto As New EnvelopedData
Dim mensaje
Dim Encrypted As String
On Error GoTo manejaError
If txtArchDestino.Text = "" Then
    mensaje = MsgBox("Debe seleccionar un archivo de destino para almacenar los datos cifrados", vbExclamation + vbOKOnly, "Solicitud de información")
Else
    numArchivoCif = FreeFile
    Open RUTA_ARCHIVO For Input As #numArchivoCif
    While Not EOF(numArchivoCif)
        Line Input #numArchivoCif, lineaArchivo
        archivoCifrado = archivoCifrado & lineaArchivo
    Wend
    Close #numArchivoCif
    'para descifrar el mensaje un certificado con acceso a una clave
    'privada valida debe estar disponible en el almacen
    If Len(archivoCifrado) > 0 Then
        Dim xx
        xx = mensajeEnvuelto.Recipients.Count
        mensajeEnvuelto.Decrypt archivoCifrado
        numArchivoGuardar = FreeFile
        Open RUTA_ARCHIVO_DESTINO For Output As #numArchivoGuardar
        Print #numArchivoGuardar, mensajeEnvuelto.Content
        Close #numArchivoGuardar
        mensaje = MsgBox("El mensaje fue decifrado y almacenado", vbInformation + vbOKOnly, "Fin del proceso")
    Else
        mensaje = MsgBox("No se leyo ningun mensaje cifrado.", vbInformation + vbOKOnly, "Error en el archivo cifrado")
    End If
    Set mensajeEnvuelto = Nothing
    Unload Me
    Exit Sub
End If
manejaError:
If Err.Number <> 0 Then
Dim describeError As String
Select Case Err.Number
Case -2138570109
    mensaje = MsgBox("No se encuentra una clave valida para descifrar este archivo", vbExclamation + vbOKOnly, "Destinatario incorrecto")
Case -2146762748
    mensaje = MsgBox("Ha decidido no confiar en este codigo", vbInformation + vbOKOnly, "Error en el certificado")
Case -2138570157
    mensaje = MsgBox("El certificado no es valido para firmar codigo, debe solicitar un certificado digital", vbInformation + vbOKOnly, "Error en el certificado")
Case -2138570191
    mensaje = MsgBox("El almacen esta vacio, debe solicitar un certificado digital", vbInformation + vbOKOnly, "Error en el procedimiento")
Case -2138569887
    mensaje = MsgBox("Este archivo no ha sido firmado", vbInformation + vbOKOnly, "Error en la verificación")
Case CAPICOM_E_CANCELLED
    mensaje = MsgBox("debe seleccionar un certificado como destinatario ", vbInformation + vbOKOnly, "Error en el procedimiento")
Case Else
    mensaje = MsgBox("Se ha encontrado un error, " & Err.Description, vbCritical + vbOKOnly, "Error en la aplicación")
    describeError = "Error en de aplicación, N°: " & CStr(Err.Number) & ", " & Err.Description & ", " & Err.Source
    Call guardaError(describeError)
End Select
Err.Clear
End If
End Sub

```

PROTOTIPO PORTAL WEB

Siguiendo con el formato de este apéndice, para el prototipo Portal Web se mostrarán sólo las paginas con funcionalidades más relevantes.

▪ valida_usuario.asp

Esta página se encarga de leer el certificado presentado por el usuario y validar el rut extraído contra la base de datos de clientes, también transforma el formato del certificado leído de binario a texto para su utilización posterior.

```
<object id="oCAPICOM" classid="clsid:A996E48C-D3DC-4244-89F7-AFA33EC60679"
codebase="capicom.cab#version=2,0,0,0">
</object>
```

```
<%
```

```
function Huella_cert(texto_certificado)
dim certificado
Set certificado = CreateObject("CAPICOM.Certificate")
certificado.Import (texto_certificado)
Huella_cert = certificado.Thumbprint
Set certificado = Nothing
end function
```

```
function Transforma_cer (cer)
uue = "ABCDEFGHIIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
CertBinarioTexto="-----BEGIN CERTIFICATE-----" + chr(13) + chr(10)
lcer = len(cer)
l = 0
for x = 1 to lcer step 3
a1 = asc(mid(cer,x,1))
if x+1 <= lcer then
a2 = asc(mid(cer,x+1,1))
if x+2 <= lcer then
a3 = asc(mid(cer,x+2,1))
else
a3 = 0
end if
else
a2 = 0
a3 = 0
end if
CertBinarioTexto=CertBinarioTexto + mid(uue, (a1 and 252)/4 +1 ,1)
CertBinarioTexto=CertBinarioTexto + mid(uue, (a1 and 3)*16 + (a2 and 240)/16 +1 ,1)
if x+1 <= lcer then
CertBinarioTexto=CertBinarioTexto + mid(uue, (a2 and 15)*4 + (a3 and 192)/64 +1 ,1)
if x+2 <= lcer then
CertBinarioTexto=CertBinarioTexto + mid(uue, (a3 and 63) +1 ,1)
else
CertBinarioTexto=CertBinarioTexto + "="
end if
else
CertBinarioTexto=CertBinarioTexto + "=="
end if
l = l +4
if l = 64 then
CertBinarioTexto=CertBinarioTexto + "" + chr(13)+chr(10)
l = 0
end if
next
if l > 0 then
CertBinarioTexto=CertBinarioTexto + "" + chr(13)+chr(10)
end if
CertBinarioTexto=CertBinarioTexto + "-----END CERTIFICATE-----" + chr(13)+chr(10)
Transforma_cer=CertBinarioTexto
end function
```

```

Response.Expires = 0
Dim rut, vector, hash_certificado,path, consulta_sql, certificado

session("sesion_nombre")= Request.ClientCertificate("subjectcn")
session("sesion_rut")=trim(Request.ClientCertificate("subjectOU"))
session("sesion_serial")=Request.ClientCertificate("SerialNumber")
session("certificado")=Huella_cert(Transforma_cer(Request.ClientCertificate("Certificate")))

path=server.MapPath("BaseDatos/BancoCAV.mdb")
set basedatos=server.CreateObject("ADODB.connection")
basedatos.open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & path

set tabla=server.createobject("ADODB.recordset")

consulta_sql="SELECT rut, numero_cuenta, saldo FROM Clientes WHERE rut='" +
session("sesion_rut") + "'"

tabla.open consulta_sql, basedatos
if tabla.eof and tabla.bof then
    response.redirect("../publico/error.htm")
else
    session("numero_cuenta")=cstr(tabla("numero_cuenta"))
    session("sesion_saldo")=cstr(tabla("saldo"))
    response.Redirect("todos_frame.htm")
end if

tabla.close
basedatos.close

set tabla=nothing
set basedatos= nothing
%>

```

▪ transferencias.asp

Esta página contiene un formulario de transferencias de fondos, dentro de este están los elementos que almacenan los datos introducidos por el usuario y que son firmados digitalmente mediante las funciones aquí también definidas.

```

<%
    Response.Expires = 0
    if session("sesion_rut")="" then
        response.Redirect("error.htm")
    end if
    resumen_certificado=session("certificado")
%>

<html>
<head>
<title>Transferencias de fondos</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="Estilos/estilos.css" rel="stylesheet" type="text/css">

<object id="oCAPICOM" classid="clsid:A996E48C-D3DC-4244-89F7-AFA33EC60679"
codebase="capicom.cab#version=2,0,0,0">
</object>

<script language="JavaScript">
// constantes CAPICOM
var CAPICOM_STORE_OPEN_READ_ONLY = 0;
var CAPICOM_CURRENT_USER_STORE = 2;
var CAPICOM_CERTIFICATE_FIND_SHA1_HASH = 0;
var CAPICOM_CERTIFICATE_FIND_EXTENDED_PROPERTY = 6;
var CAPICOM_CERTIFICATE_FIND_TIME_VALID = 9;
var CAPICOM_CERTIFICATE_FIND_KEY_USAGE = 12;
var CAPICOM_DIGITAL_SIGNATURE_KEY_USAGE = 0x00000080;
var CAPICOM_AUTHENTICATED_ATTRIBUTE_SIGNING_TIME = 0;
var CAPICOM_INFO_SUBJECT_SIMPLE_NAME = 0;
var CAPICOM_ENCODE_BASE64 = 0;
var CAPICOM_E_CANCELLED = -2138568446;
var CERT_KEY_SPEC_PROP_ID = 6;

```

```

//-----
function EstaCAPICOM()
{
    if(typeof(oCAPICOM) == "object") //devuelve el tipo de operador
    {
        if( (oCAPICOM.object != null) )
        {
            // se encontro CAPICOM
            return true;
        }
    }
}

//-----

function filtraCertificados()
{
    // instancia objeto CAPICOM
    // provee metodos y propiedades para manejar y usar almacenes de certificados

    var miAlmacen = new ActiveXObject("CAPICOM.Store");
    var certificadosFiltrados = new ActiveXObject("CAPICOM.Certificates");//representa
    colecciones de certificados

    try
    {
        // abre el almacen de certificados personales
        miAlmacen.Open(CAPICOM_CURRENT_USER_STORE, "My", CAPICOM_STORE_OPEN_READ_ONLY);
    }
    catch (e)
    {
        if (e.number != CAPICOM_E_CANCELLED)
        {
            alert("Error al intentar abrir su almacen de certificados personales");
            return false;
        }
    }
    // encuentra todos los certificados que:
    // * son adecuados para firmar datos
    // * tienen una clave privada asociada
    // * estan dentro de su periodo de validez
    var certificadosFiltrados =
    miAlmacen.Certificates.Find(CAPICOM_CERTIFICATE_FIND_KEY_USAGE, CAPICOM_DIGITAL_SIGNATURE_KEY
    _USAGE).Find(CAPICOM_CERTIFICATE_FIND_TIME_VALID).Find(CAPICOM_CERTIFICATE_FIND_EXTENDED_PRO
    PERTY, CERT_KEY_SPEC_PROP_ID);

    return certificadosFiltrados;

    miAlmacen = null;
    certificadosFiltrados = null;
}

//-----

function seleccionaCertificado()
{
    // recupera lista de certificados filtrados
    // entrega todos los certificados que cumplen con norma
    var certificadosFiltrados = filtraCertificados();
    //devuelve numero de certificados en objeto
    if (certificadosFiltrados.Count >= 1)
    {
        try
        {
            //despliega cuadro dialogo seleccionar certificados (titulo, strin,
            multipleseleccion) de los que entrego el filtro
            alert("Selecione el mismo certificado que utilizo para ingresar al sitio");
            var CertificadoSeleccionado = certificadosFiltrados.Select();

            //entrega string del hash del certificado
            document.frm_transaccion.txt_hash_certificado.value =
            CertificadoSeleccionado.Item(1).Thumbprint;

            //devuelve el certificado seleccionado

            return CertificadoSeleccionado.Item(1);
        }
        catch (e)
        {

```

```

        document.frm_transaccion.txt_hash_certificado.value = "";
        alert("error selecc cer" + e.description);
    }
    else
    {
        alert("Ud. no tienen un certificado valido");
    }
    CertificadoSeleccionado = null;
    certificadosFiltrados = null;
}

//-----

function lee()
{
    //extrae un textrange a un body, textarea, input sino encuentra devuelve null
    mitexto=document.body.createTextRange();
    //extrae el html valido de un textrange
    texto= mitexto.htmlText;
    return texto;
}

//-----

function firma()
{
    //provee propiedades y metodos para establecer el contenido a firmar
    var datosfirmar = new ActiveXObject("CAPICOM.SignedData");
    // establece el firmante de un objeto signed data
    var firmante = new ActiveXObject("CAPICOM.Signer");
    //fija atributo fecha en caso de tiempo
    var atributoTiempo = new ActiveXObject("CAPICOM.Attribute");

    datosfirmar.content=lee();
    document.frm_transaccion.txt_texto_firmado.value=datosfirmar.content;

    try
    {
        // fija el certificado que se utilizara para firmar
        firmante.Certificate = seleccionaCertificado()
        // fija la fecha en que se firma
        var Today = new Date();
        atributoTiempo.Name = CAPICOM_AUTHENTICATED_ATTRIBUTE_SIGNING_TIME;
        atributoTiempo.Value = Today.getVarDate();
        Today = null;
        //agrega atributo tiempo al objeto firmante
        firmante.AuthenticatedAttributes.Add(atributoTiempo);
        // realiza operacion firma
        var firma_documento = datosfirmar.Sign(firmante, true, CAPICOM_ENCODE_BASE64);
        document.frm_transaccion.txt_firma.value=firma_documento;
    }
    catch (e)
    {
        if (e.number != CAPICOM_E_CANCELLED)
        {
            alert("Un error a ocurrido al intentar firma el formulario, el error fue: " +
            e.description);
            return false;
        }
    }
}

//-----

function validar()
{
    var num_cuenta = document.frm_transaccion.txt_numero_cuenta.value;

    if (num_cuenta=="")
    {
        alert ("ingrese numero de cuenta");
        document.frm_transaccion.txt_numero_cuenta.focus();
        return;
    }
    var nombre=document.frm_transaccion.txt_nombre.value;
    if (nombre=="")
    {
        alert ("ingrese nombre benecionario");
        document.frm_transaccion.txt_nombre.focus();
    }
}

```

```

        return;
    }
    var rut=document.frm_transaccion.txt_rut.value;
    if (rut=="")
    {
        alert ("ingrese rut beneficiario");
        document.frm_transaccion.txt_rut.focus();
        return;
    }
    var monto=document.frm_transaccion.txt_monto.value;
    if (monto=="")
    {
        alert ("ingrese monto de la transaccion");
        document.frm_transaccion.txt_monto.focus();
        return;
    }
    if (EstaCAPICOM=true)
    {
        firma();
    }
    else
    {
        alert ("Ud no podra firmar");
    }
    if (document.frm_transaccion.txt_hash_certificado.value !=
    document.frm_transaccion.txt_certificado_autenticacion.value)
    {
        alert ("El certificado que selecciono no es el que utilizo para ingresar al sitio
        web");
        return;
    }
    document.frm_transaccion.submit();
}
</script>

```

```

</head>
<body>
<table align="center" width="600" height="104" border="0" cellpadding="0" cellspacing="0">
<tr class="header">
<td width="178"><div align="center"><strong><font size="2">Número
cuenta:</font></strong></div></td>
<td width="251"><div align="center"><strong><font size="2">Saldo:</font></strong></div></td>
<td width="171"><div align="center"><strong><font size="2">Fecha:</font></strong></div></td>
</tr>
<tr>
<td><div align="center"><font color="#009933" size="1"><strong><%=session("numero_cuenta")%>
</strong></font></div></td>
<td><div align="center"><font color="#009933"
size="1"><strong><%=session("sesion_saldo")%></strong></font></div></td>
<td><div align="center"><font color="#009933"
size="1"><strong><%=FormatDateTime(date(),2)%></strong></font></div></td>
</tr>
<tr>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
<tr>
<td colspan="3" class="header"> <div align="center"></div>
<div align="center"><font size="2"><strong>Datos beneficiario
transferencia</strong></font></div>
<div align="center"></div></td>
</tr>
<tr>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
<tr>
<td>&nbsp;</td>
<td><form name="frm_transaccion" method="post" action="procesa_transaccion.asp">
<table width="100%" border="0" cellspacing="0" cellpadding="0">
<tr>
<td class="celda"><strong><font color="#009933" size="2">Banco:</font></strong></td>
<td><select name="cmb_banco">
<option value="Banco Santander">Banco Santander</option>
<option value="Banco Chile">Banco Chile</option>
<option value="Banco CAV">Banco CAV</option>

```

```
</select></td>
</tr>
<tr>
<td class="celda"><strong><font color="#009933" size="2">N&deg; cuenta:</font></strong></td>
<td><input type="text" name="txt_numero_cuenta"></td>
</tr>
<tr>
<td class="celda"><strong><font color="#009933" size="2">Nombre:</font></strong></td>
<td><input type="text" name="txt_nombre"></td>
</tr>
<tr>
<td class="celda"><strong><font color="#009933" size="2">rut:</font></strong></td>
<td><input type="text" name="txt_rut"></td>
</tr>
<tr>
<td class="celda"><strong><font color="#009933" size="2">e-mail:</font></strong></td>
<td><input type="text" name="txt_correo"></td>
</tr>
<tr>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
<tr>
<td class="celda"><strong><font color="#009933" size="2">Monto:</font></strong></td>
<td><input type="text" name="txt_monto"></td>
</tr>
<tr>
<td>&nbsp;</td>
<td> <input type="hidden" name="txt_certificado_autenticacion" value = <%=
response.write(resumen_certificado)%> >
<input type="hidden" name="txt_hash_certificado" value=""> <input type="hidden"
name="txt_firma" value="" >
<input type="hidden" name="txt_texto_firmado" value=""> </td>
</tr>
<tr>
<td colspan="2" align="center" ><input type="button" name="cmd_enviar" value="Enviar y Firmar"
onClick="validar()" class="boton">
</td>
</tr>
</table>
</form></td>
<td>&nbsp;</td>
</tr>
<tr>
<td>&nbsp;</td>
<td>&nbsp;</td>
<td>&nbsp;</td>
</tr>
</table>
</body>
</html>
```

▪ **procesa_transaccion.asp**

Esta página se encarga del almacenamiento de las transacciones y de las firmas de estas en la base de datos del portal.

<%

```
Function FechaGenerica(fecha)
  If IsDate(fecha) = True Then
    DIM dteDay, dteMonth, dteYear
    dia = Day(fecha)
    mes = Month(fecha)
    ano = Year(fecha)
    FechaGenerica = ano & "/" & Right(Cstr(mes + 100),2) & "/" & Right(Cstr(dia + 100),2)
  Else
    FechaGenerica = Null
  End If
End Function
```

```
Response.Expires = 0
if session("sesion_rut")="" then
  response.redirect "error.htm"
```

else

```
nombre_titular=session("sesion_nombre")
cuenta_titular=session("numero_cuenta")
rut_titular=session("sesion_rut")

banco_destino=request.form("cmb_banco")
nombre_beneficiado=request.form("txt_nombre")
rut_beneficiado=request.form("txt_")
cuenta_beneficiado=request.form("txt_numero_cuenta")
monto=request.form("txt_monto")
correo=request.form("txt_correo")

hash_certificado=request.form("txt_hash_certificado")
firma_form=request.form("txt_firma")
texto_firmado=request.form("txt_texto_firmado")
```

'-----almacena transaccion-----'

```
ruta_db=server.MapPath("BaseDatos/BancoCAV.mdb")
set basedatos=server.CreateObject("ADODB.connection")
basedatos.open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & ruta_db

'extrae el numero actual de transaccion
set tablaMaxTrans=server.createobject("ADODB.recordset")

consulta_sql="SELECT Max(Transacciones.numero_transaccion) as numero_transaccion FROM
Transacciones"

tablaMaxTrans.open consulta_sql, basedatos
If IsNull(tablaMaxTrans.Fields("numero_transaccion")) then
    maximo_num_transaccion= 1
else
    maximo_num_transaccion= tablaMaxTrans.Fields("numero_transaccion") + 1
end if

tablaMaxTrans.close
set tablaMaxTrans=nothing
```

'-----inserta tranferencia de fondos

```
inserta = "INSERT INTO transacciones "
campos_i= "(numero_transaccion, fecha, monto, cuenta_origen, cuenta_destino, banco) "
valores_i=" VALUES (" & maximo_num_transaccion & ", #" & FechaGenerica(Date) & "#, " & _
monto & ", " & cuenta_titular & ", " & cuenta_beneficiado & ", " & banco_destino & "')"

inserta_sql=inserta & campos_i & valores_i
on error resume next
    basedatos.Execute inserta_sql,,adCmdText + adExecuteNoRecords
    if err.number <> 0 then
        response.write("No se pudo procesar la transaccion " + "<br>")
    end if
err.clear
```

'-----actualiza saldo

```
actualiza = "UPDATE clientes "
valores_a= "SET saldo= saldo -" & monto
campos_a= " WHERE RUT='" & rut_titular & "'"
actualiza_sql=actualiza & valores_a & campos_a

on error resume next
    basedatos.Execute actualiza_sql,,adCmdText + adExecuteNoRecords
    if err.number <> 0 then
        response.write("No se pudo procesar la transaccion " + "<br>")
    end if
err.clear
```

```
basedatos.close
set basedatos= nothing
```

'-----almacena firma transaccion

```
ini_firma="-----INICIO FIRMA-----" + chr(13) + chr(10)
fin_firma="-----FIN FIRMA-----" + chr(13) + chr(10)
firma_form=ini_firma & firma_form & fin_firma

ruta_db=server.MapPath("BaseDatos/BancoCAV.mdb")
set basedatos=server.CreateObject("ADODB.connection")
basedatos.open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & ruta_db
```

```

inserta = " INSERT INTO Firmas "
campos= "(numero_transaccion, datos, firma, hash_certificado) "
valores=" VALUES (" & maximo_num_transaccion & ", '" & texto_firmado & "', '" & _
firma_form & "', '" & hash_certificado & "')"

sentenciaSQL= inserta & campos & valores

on error resume next
basedatos.Execute sentenciaSQL,,adCmdText + adExecuteNoRecords
if err.number <> 0 then
    response.write("No se pudo realizar la insercion de la firma en la base de datos" +
        "<br>")
else
    response.write("<div align=center><font align=center>Su transacción se ha concretado
        satisfactoriamente" + "</font></div><br>")
end if
err.clear

basedatos.close
set basedatos=nothing
end if

%>

```