

Índice

Prólogo.....	13
Introducción.....	15
Capítulo I Nuestro nuevo DNI electrónico.....	17
1. Nuestra identidad en la Red.....	17
2. Como usar el DNI electrónico.....	19
Capítulo II Criptografía y firma electrónica.....	23
1. Fundamentos de la comunicación.....	23
2. El origen de la criptografía.....	24
3. La criptografía desde su inicio hasta nuestros días.....	26
4. Criptografía en la Segunda Guerra Mundial.....	34
5. Criptografía moderna.....	36
Un estándar de cifrado.....	36
El problema de la distribución de claves.....	38
Y por fin, llegó la criptografía asimétrica.....	39
6. ¿Y qué tiene esto que ver con la firma electrónica?.....	43
Capítulo III La gestión de las claves públicas.....	45
1. Estándar UIT-T x.509v3.....	47



2. Infraestructura de Clave Pública (PKI).....	49
3. Prestador de Servicios de Certificación (PSC)	50
4. La Autoridad de Registro.....	52
5. La Autoridad de Certificación	54
La política de certificación	56
Modelos de relación entre Autoridades de Certificación.....	57
6. La Autoridad de Validación.....	59
7. La Autoridad de Sellado de Tiempo	63
8. Otros tipos de certificados digitales.....	64
9. Dispositivos de creación de firma.....	65
Capítulo IV Las tarjetas inteligentes (Smart Cards).....	69
1. Tipos de tarjetas inteligentes	70
2. Cronología de las Smart Cards	72
3. Características físicas de las tarjetas.....	74
Tamaños de las tarjetas.....	74
Material de fabricación	76
Encapsulado del chip	78
4. Estructura interna del chip	79
5. Los contactos de la tarjeta.....	80
6. Señales eléctricas y protocolos de transmisión.....	81
7. Almacenamiento de la información.....	81
8. Comandos (dando órdenes al chip).....	85
9. Estándares	88
ISO/IEC (International Standards Organization).....	88
EMV	89
PC/SC	89
RSA Laboratories	90



10. Certificaciones de seguridad.....	91
FIPS (Federal Information Processing Standard)	91
Common Criteria	91
Capítulo V La firma digital	93
1. Firma electrónica, firma digital y otras firmas	93
2. El proceso de firma digital.....	95
3. La funciones hash	97
La utilidad de las funciones hash.....	99
Tipos de funciones hash	100
Construcción de Merkle–Damgård.....	101
Funciones hash (criptográficas) más empleadas.....	102
El futuro de las funciones hash criptográficas.....	107
Algunos links de interés	108
4. Formatos de firma digital	108
CMS (Cryptographic Message Syntax)	108
S/MIME	110
PDF Signature.....	112
XML Signature	113
XAdES.....	116
CAAdES	118
PAdES	119
Capítulo VI Características del DNI electrónico	121
1. Características físicas	122
2. Impresiones de seguridad	124
Seguridad física del DNI electrónico.....	126
3. Características electrónicas.....	127
4. Contenido del chip.....	129
Datos biométricos	131
5. Certificados digitales	132



Certificado de autenticación	133
Certificado de firma.....	135
Certificado de componente	136
Uso apropiados de estos certificados.....	136
6. Autoridades de Registro	137
Proceso de expedición	138
Documentación necesaria para la expedición del DNIE	138
7. Autoridad de Validación.....	140
8. Como utilizar el DNI electrónico.....	142
Elementos hardware.....	142
Elementos software.....	144
Aplicaciones compatibles con el DNI electrónico.....	145
Otros componentes necesarios.....	146
9. La contribución clave de la FNMT-RCM.....	148
CERES, la FNMT-RCM como PSC.....	148
Participación en el DNI electrónico.....	149
10. Certificaciones de seguridad del DNI electrónico	149
Capítulo VII Legislación aplicable.....	153
1. Directiva Europea de firma electrónica (1999/93/CE)	153
2. La Ley de firma electrónica. (Ley 59/2003)	155
Certificado electrónico reconocido.....	157
Dispositivo seguro de creación de firma.....	158
Firma electrónica simple, avanzada y reconocida	158
3. Ley de Medidas de Impulso de la Sociedad de la Información	160
Principales aspectos.....	160
4. Ley de acceso electrónico de los ciudadanos a los servicios públicos.....	164
Derechos de los ciudadanos.....	165
Obligaciones de las Administraciones Públicas	166
Estructura de la ley	167
Reglamento. Real Decreto de 27 de Enero de 2009	168



Identificación y autenticación.....	168
Capítulo VIII Beneficios del DNI electrónico.....	171
1. Beneficios generales.....	171
2. Beneficios para el ciudadano.....	173
3. Beneficios para la empresa.....	176
4. Beneficios para el administrador de sistemas.....	178
5. Beneficios para el desarrollador de aplicaciones.....	180
6. Beneficios para las Administraciones Públicas.....	180
Capítulo IX Aplicaciones y servicios.....	181
1. Comprobar el funcionamiento del DNI electrónico.....	181
2. Aplicaciones de escritorio para la firma de documentos.....	182
eCoFirma del Ministerio de Industria, Turismo y Comercio.....	183
Explorador ESecure de KSI Tecnología Digital.....	184
XolidoSign de Xolido Systems.....	185
clickSign de iSigma.....	186
ProSign de Firmaprofesional.....	186
ProFirma de Albalia Interactiva.....	187
Plataformas de firma electrónica.....	187
3. Factura electrónica.....	188
FACCIL de Albalia Interactiva.....	188
ecoFACTURA de Edatalia Data Solutions.....	189
Digitalización Certificada.....	190
4. Autenticación de usuarios.....	193
IDOne® Professional de SmartAccess.....	193
SmartID® Corporate Logon de SmartAccess.....	194
5. Otras aplicaciones.....	194
Firma de contratos.....	194
Registro automático de visitantes con el DNI electrónico.....	195



Índice de imágenes	197
Índice alfabético	201
Libros publicados.....	203

