
1. Índice

1. Índice.....	1
2. Objetivos y organización de la memoria.....	5
2.1. Objetivos.....	5
2.2. Organización de la memoria.....	6
2.2.1. Bloque I: Introducción teórica.....	6
2.2.2. Bloque II: Desarrollo de la aplicación.....	6
2.2.3. Bloque III: Temporización y presupuesto, Referencias y Apéndice.....	7
3. XMLDSig.....	8
3.1. Introducción a XML.....	8
3.1.1. Modelo de datos jerárquico de XML.....	9
3.1.2. Documentos XML, DTD y XML Schema.....	11
3.1.2.1. Documentos bien formados y válidos.....	11
3.1.2.2. XML DTD.....	12
3.1.2.3. XML Schema.....	13
3.1.3. Consulta XML.....	16
3.1.3.1. XPath.....	16
3.1.3.2. XQuery.....	18
3.2. Introducción a XMLDSig.....	19
3.3. Formatos de firma XMLDSig.....	19
3.3.1. Enveloped Signature.....	19
3.3.2. Enveloping Signature.....	20
3.3.3. Detached Format.....	20
3.4. Estructura y esquema de XMLDSig.....	20
3.4.1. Elemento <SignedInfo>.....	22
3.4.1.1. Elemento <CanonicalizationMethod>.....	22
3.4.1.2. Elemento <SignatureMethod>.....	22
3.4.1.3. Elemento <Reference>.....	23
3.4.1.3.1. Elemento <Transforms>.....	23
3.4.1.3.2. Elemento <DigestMethod>.....	26
3.4.1.3.3. Elemento <DigestValue>.....	26
3.4.2. Elemento <SignatureValue>.....	26
3.4.3. Elemento <KeyInfo>.....	26
3.4.3.1. Elemento <KeyName>.....	27
3.4.3.2. Elemento <KeyValue>.....	27
3.4.3.2.1. Elemento <DSAPublicValue>.....	27
3.4.3.2.2. Elemento <RSAPublicValue>.....	28

3.4.3.3. Elemento <RetrievalMethod>.....	28
3.4.3.4. Elemento <X509Data>.....	28
3.4.3.5. Elemento <PGPData>.....	28
3.4.3.6. Elemento <SPKIData>.....	29
3.4.3.7. Elemento <MgmtData>.....	29
3.4.4. Elemento <Object>.....	29
3.5. Codificación base64.....	29
3.6. Identificadores de <i>Algorithm</i>	30
3.7. Proceso de creación y validación de firmas en XML.....	31
3.7.1. Creación de una firma digital.....	31
3.7.2. Proceso de validación de una firma digital.....	32
3.8. Implementaciones de la especificación XMLDSig.....	32
3.9. Conclusiones.....	33
4. DNI electrónico.....	35
4.1. Descripción física del DNIe.....	36
4.2. Descripción del chip del DNIe.....	38
4.2.1. La información contenida en el chip.....	39
4.2.2. Tipos de datos.....	40
4.2.3. Certificados digitales.....	40
4.3. Funciones básicas.....	41
4.4. Certificados de Identidad Pública.....	41
4.4.1. Uso de los certificados.....	41
4.4.2. Validez de los certificados.....	42
4.5. Requisitos. Elementos software, hardware y estándares.....	42
4.5.1. Software.....	42
4.5.2. Dispositivo hardware necesario para la lectura de la tarjeta-chip.....	43
4.6. Instalación del software.....	45
4.7. Clave de acceso personal PIN.....	46
4.8. El certificado digital asociado al DNI electrónico.....	47
4.9. Escenarios de uso del DNI electrónico.....	48
4.9.1. Autenticación con organismo público o entidad privada.....	49
4.9.2. Firma digital de documentos.....	50
4.10. Infraestructura de Certificación del DNI electrónico.....	51
4.11. Certificados de usuario.....	52

4.11.1. Campos del Certificado.....	52
4.12. Pautas a seguir para el desarrollo de aplicaciones con el DNIE....	53
4.12.1. Acceso al DNI electrónico.....	54
4.12.2. Acceso al almacén de certificados.....	54
4.12.3. Selección del certificado de firma (contentCOMMITMENT).....	54
4.12.4. Descomposición del Subject.....	55
4.12.5. Operaciones criptográficas.....	56
4.12.6. Resumen realización firma electrónica.....	56
4.12.7. Verificación de firmas electrónicas.....	56
4.12.8. Resumen verificación operación criptográfica.....	57
4.13. Servicio de autenticación web mediante DNIE.....	58
4.13.1. ¿Qué es la autenticación?.....	58
4.13.2. Autenticación web.....	59
4.13.3. Requisitos.....	61
4.13.4. Configuración.....	62
4.13.4.1. Configuración del servidor.....	62
4.13.4.2. Configuración del cliente.....	63
4.14. Conclusiones.....	64
5. Desarrollo de la aplicación de Firma Digital XML.....	66
5.1. Requisitos de diseño de la aplicación.....	66
5.2. Proceso de creación de firmas con la API JSR 105.....	67
5.2.1. Instanciar el documento que se va firmar.....	67
5.2.2. Ensamblar la firma XML.....	68
5.2.3. Crear una pareja de claves pública-privada.....	69
5.2.4. Crear un contexto de firma.....	69
5.2.5. Crear la firma digital XML.....	70
5.2.6. Generar la salida del documento resultante XML.....	70
5.3. Proceso de validación de firmas con la API JSR 105.....	70
5.3.1. Instanciar el documento que contiene la firma.....	70
5.3.2. Especificar el elemento Signature para validar.....	71
5.3.3. Crear un contexto de validación.....	71
5.3.4. Unmarshalling de la firma XML.....	71
5.3.5. Validar la firma digital XML.....	72
5.3.6. ¿Qué ocurre si la firma no se valida?.....	72
5.3.7. Uso de KeySelectors.....	73
5.4. Entorno de desarrollo y pruebas de la aplicación.....	75
5.4.1. JSR 105 API.....	75
5.4.2. Compilación y ejecución de la aplicación.....	76
5.4.3. Ejemplos de prueba.....	79
5.5. Requisitos legales.....	86

5.6. Proveedores españoles de tecnología PKI.....	86
5.6.1. Componentes de firma (MITyC).....	88
5.6.2. @firma. Plataforma de validación y firma electrónica.....	90
5.6.2.1. Servicios ofrecidos por la Plataforma.....	91
5.6.2.2. Certificados reconocidos por la Plataforma.....	93
5.6.2.3. Cliente de Firma.....	93
5.6.3. CryptoAplet.....	94
5.6.4. Factura electrónica.....	95
5.6.5. Viafirma.....	97
5.6.6. Izenpe.....	97
5.6.6.1. ZAIN.....	97
5.6.6.2. ef4ktur.....	99
5.6.6.3. id@zki.....	99
5.6.6.4. Servicio de verificación.....	99
5.6.6.5. Servicio de sellado de tiempo.....	100
5.6.7. OpenDNI.....	100
5.6.8. Otras empresas.....	101
5.7. Conclusiones.....	102
 6. Planos de código.....	 104
 7. Mejoras y líneas de continuación del proyecto.....	 131
7.1. XAdES.....	131
7.2. Facturae.....	131
7.3. API de firma con el DNIE.....	132
7.4. Servicios web.....	132
 8. Temporización y presupuesto.....	 133
8.1. Fases del proyecto.....	133
8.2. Presupuesto.....	135
8.2.1. Coste de recursos humanos.....	135
8.2.2. Coste herramientas de trabajo: hardware y software.....	135
8.2.3. Coste servicios.....	135
8.2.4. Tabla de costes.....	136
 9. Referencias.....	 137
 Apéndice - Conceptos de seguridad.....	 139