

Índice de contenido

1. INTRODUCCIÓN Y OBJETIVOS.....	10
2. ESTADO DEL ARTE.....	13
2.1 Tecnologías hardware.....	14
2.1.2 Tecnologías basadas en la tarjeta SIM.....	14
2.1.2.1 SMS.....	15
2.1.2.2 SAT – USAT.....	15
2.1.2.3 WIM.....	16
2.2 Tecnologías software.....	16
2.2.1 Sistema Operativo Windows Mobile.....	17
2.2.1 Sistema Operativo Symbian.....	18
2.2.2 Java ME.....	18
2.3 Tecnologías híbridas.....	20
2.3.1 SATSA.....	20
2.4 Soluciones independientes del dispositivo	21
2.4.1 Firmas basadas en un servidor.....	21
2.4.2 Servicio de firma móvil.....	22
3. J2ME.....	24
3.1 Análisis comparativo.....	24
3.2 Nociones básicas de J2ME.....	26
3.2.1 Máquinas virtuales J2ME.....	27
3.2.2 Configuraciones.....	28
3.2.3 Perfiles.....	30
3.3 Configuración CDLC.....	32
3.3.1 Introducción.....	33
3.3.2 Objetivos.....	33
3.3.3 Requerimientos.....	34
3.3.4 Seguridad.....	35
3.3.5 Librerías CDLC.....	35
3.4 Los MIDlets.....	37
3.4.1 Introducción.....	37
3.4.2 Ciclo de vida de un MIDlet.....	37
3.4.3 Estados de un MIDlet.....	39
3.4.4 Librerías MIDlet.....	39

4. SERVICIOS WEB SOBRE AXIS2.....	44
4.1 Introducción.....	44
4.2 Factores que influyen en la aparición de los servicios web.....	44
4.3 Objetivos.....	45
4.4 Arquitectura.....	45
4.5 Lenguaje XML.....	46
4.5.1 Introducción.....	46
4.5.2 Principales conceptos.....	47
4.5.3 Definición de Tipos de Documentos DTD.....	48
4.5.4 Modelo de documentos DOM	50
4.6 Protocolo SOAP.....	50
4.6.1 Principales conceptos.....	50
4.6.2 Estructura y contenido de un mensaje SOAP.....	51
4.6.2.1 Codificación SOAP.....	55
4.6.3 Protocolo de transporte.....	56
4.7 Descripción del servicio WSDL.....	56
4.7.1 Principales conceptos.....	56
4.7.2 Arquitectura WSDL.....	57
4.8 UDDI (Universal Description Discovery and Integration).....	59
4.8.1 Principales conceptos.....	59
4.8.2 Estructuras de datos	60
4.8.3 API del registro UDDI.....	61
4.9 Implementación de servicios web xml.....	62
4.9.1 Uso de WSDL con AXIS.....	63
4.10 Uso de servicios web en un cliente móvil: JSR-172.....	64
4.10.1 Principales conceptos.....	64
4.10.2 JSR-172 Runtime	65
4.10.3 La API JSR-172 JAX-RPC.....	66
5. CRIPTOGRAFÍA EN DISPOSITIVOS MÓVILES	68
5.1 Principales conceptos sobre criptografía.....	68
5.1.1 Algoritmos de cifrado.....	68
5.1.1.1 Algoritmos de clave secreta o simétricos.....	69
5.1.1.2 Algoritmos de clave pública o asimétricos.....	71
5.1.2 Firma digital.....	72
5.1.3 Certificados digitales.....	74
5.1.4 Infraestructura de clave pública.....	74
5.2 X.509.....	75

5.2.1	Introducción.....	75
5.2.2	Estructura de un certificado X.509 v3.....	75
5.2.3	Extensión de certificados.....	78
5.3	Estándar PKCS7.....	79
5.3.1	Tipo de contenido Data.....	79
5.3.2	Tipo de contenido SignedData.....	79
5.3.3	Tipo de contenido EnvelopedData.....	81
5.3.4	Tipo de contenido SignedEnvelopedData.....	82
5.4	Librería Bouncy Castle.....	83
6.	PROTOCOLO WEBDAV.....	86
6.1	Principales conceptos.....	86
6.2	Métodos utilizados.....	87
6.2.1	PROPFIND.....	87
6.2.2	PROPPATCH.....	90
6.2.3	GET.....	91
6.2.4	PUT.....	92
6.2.5	Propiedades DAV.....	93
6.2.6	Privilegios	93
6.3	Ejemplo práctico de Servidor WebDAV.....	95
6.4	Clientes WebDAV.....	96
7.	@FIRMA.....	99
7.1	Introducción.....	99
7.2	Servicios proporcionados.....	99
7.2.1	Validación de firmas electrónicas.....	99
7.2.3	Almacenar un documento	100
7.2.4	Firma electrónica de usuario en tres fases.....	101
8.	APLICACIÓN DESARROLLADA I.....	103
8.1	Introducción.....	103
8.2	Desarrollo del servidor	104
8.2.1	Servidor Web XML.....	104
8.2.2	Comunicación entre servidor WebDAV y Servidor Web.....	104
8.2.3	Comunicación entre servidor WebDAV y Servidor de Aplicaciones de @firma.....	104
8.3	Desarrollo del cliente.....	105
8.4	Comunicación Cliente Móvil-Servidor Web.....	105
9.	APLICACIÓN DESARROLLADA II.....	108
9.1	Introducción.....	108

9.2 Escenario de prueba.....	108
9.3 Desarrollo de los servicios web.....	109
9.3.1 Introducción.....	109
9.3.2 Desarrollo de los métodos de los servicios web.....	111
9.3.2.1 Servicio web Autenticar.....	111
9.3.2.2 Servicio web Lista de Documentos.....	113
9.3.2.3 Servicio web Obtiene Documento	116
9.3.2.4 Servicio web Obtener Hash.....	118
9.3.2.5 Servicio web Custodiar Documento.....	120
9.3.3 Despliegue de los servicios web.....	124
9.3.4 Desarrollo del cliente.....	127
9.3.4.1 Introducción.....	127
9.3.4.2 Bouncy Castle en J2ME.....	128
9.3.4.3 Manejo de ficheros.....	129
9.3.4.4 Certificados. Extracción de claves.....	133
9.3.4.5 Implementación de la firma electrónica.....	137
9.3.4.6 GUI.....	141
9.3.5 Simulación del cliente.....	157
10. CONCLUSIONES.....	174
11. TEMPORIZACIÓN.....	176
12. PRESUPUESTO.....	178
12.1 Coste de recursos humanos.....	178
12.2 Coste hardware.....	178
12.3 Coste software.....	178
12.4 Resumen de costes totales.....	179
13. GUIA DE INSTALACIÓN.....	180
13.1 Introducción.....	180
13.2 Servidor Web Apache Tomcat 5.25.....	180
13.2.1 Instalación.....	180
13.2.2 Funcionamiento.....	181
13.3 Módulo Apache Axis2 versión 1.3.....	182
13.3.1 Instalación.....	182
13.3.2 Funcionamiento.....	183
13.3.3 Despliegue de servicios.....	185
13.4 NetBeans IDE 6.0.1 con Mobility Pack.....	189
13.4.1 Introducción.....	189

13.4.2 Instalación.....	190
13.4.3 Funcionamiento.....	191
14. BIBLIOGRAFÍA.....	196
14.1 Libros de consultas.....	196
14.2 Proyectos fin de carrera.....	196
14.3 Enlaces web.....	196
14.4 Artículos publicados.....	198