



Proyecto	Reglamento eIDAS
Título	Perfiles Certificados

Realizado por	LLEIDANET PKI		
Dirigido a	Usuarios internos y externos		
Documento	DOC-200216.2152410		
Fecha aprobación	18/12/2025	Revisión	8

Calle Andarella 2, Bloque 2, Piso 3,
Puerta 8
46950 Xirivella
Tel. (34) 97 328 23 00
info@lleida.net
www.lleida.net

1	DATOS DEL DOCUMENTO	3
2	HISTORIA DEL DOCUMENTO	3
3	ELABORACIÓN, REVISIÓN Y APROBACIÓN	4
4	LISTADO DE LOS PERFILES	5
5	CERTIFICADOS DE LA JERARQUIA INDENOVA SL 003	9
5.1	CERTIFICATION AUTHORITY ROOT	9
5.2	INDENOVA SUB CA 003	14
5.3	INDENOVA OCSP 003	18
5.4	INDENOVA OCSP 003 TSA	23
5.5	INDENOVA OCSP 003 ROOT	28
5.6	INDENOVA TSA 003	33
5.7	INDENOVA TSU 003	38
6	PERFILES DE CERTIFICADOS DE INDENOVA SUB CA 003.....	42
6.1	PERSONA NATURAL	42
6.2	PERTENENCIA A EMPRESA	50
6.3	REPRESENTANTE LEGAL	57
6.4	SELLO ELECTRÓNICO	65
6.5	EMPLEADO PÚBLICO	72
6.6	REPRESENTANTE LEGAL SIN PERSONALIDAD JURÍDICA	80
6.7	EMPLEADO PÚBLICO CON SEUDÓNIMO	89

1 DATOS DEL DOCUMENTO

Proyecto	Reglamento eIDAS
Título	Perfiles Certificados
Código	DOC-200216.2152410
Tipo de documento	DOC - Documento genérico
Clasificación del documento	Público
Realizado por	LLEIDANET PKI
Dirigido a	Usuarios internos y externos
Fecha aprobación	18/12/2025
Revisión	8

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	24/05/2021	Creación del documento.	CJ
2	31/05/2021	Nueva ceremonia de claves de la PKI	CJ
3	10/08/2023	Actualizar campo "4.1 Description" del certificado de Representante Legal	CJ
4	09/09/2022	Se agregan perfiles de certificados: Empleado Público y Representante Legal Sin Personalidad Jurídica	CJ
5	09/06/2023	Se agrega el perfil de certificado Empleado Público con Seudónimo, también se cambia denominación de Indenova S.L.U. a Lleidanet PKI S.L. y se cambia eSigna ID por Lleida.net Wallet	CJ

6	10/08/2023	Se agrega nota en el apartado 3 especificando lo que debe contener los perfiles de certificados que podrán ser utilizados para la identificación y firma de las personas interesadas ante las Administraciones Públicas.	CJ
7	12/05/2025	Actualización a nueva plantilla	Compliance (CJ)
8	18/12/2025	Actualizar tamaño de la clave del certificado de usuario final Quitar el campo dirección del perfil de certificado de Persona Natural	Compliance (CJ)

3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de calidad Fecha: 18/12/2025
Revisado por:	Nombre: SB Cargo: Administrador del Servicio Fecha: 18/12/2025
Aprobado por:	Nombre: Comité de Seguridad Cargo: Comité de Seguridad Fecha: 18/12/2025

4 LISTADO DE LOS PERFILES

Nombre del certificado	OID	OID QCP	QCP
Políticas de Certificación Certificados de Persona Natural	1.3.6.1.4.1.49959.1.1.1		
Persona Natural Software	1.3.6.1.4.1.49959.1.1.1.1.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Persona Natural Hardware (qscd)	1.3.6.1.4.1.49959.1.1.1.2.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.1.3.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.1.3.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.1.3.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación de Certificados de Pertenencia a Empresa	1.3.6.1.4.1.49959.1.1.2		
Pertenencia a Empresa Software	1.3.6.1.4.1.49959.1.1.2.1.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Pertenencia a Empresa Hardware (qscd)	1.3.6.1.4.1.49959.1.1.2.2.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Pertenencia a Empresa Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.2.3.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)

Pertenencia a Empresa Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.2.3.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Pertenencia a Empresa Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.2.3.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificados Representante Legal	1.3.6.1.4.1.49959.1.1.3		
Persona Natural Representante Legal Software	1.3.6.1.4.1.49959.1.1.3.1.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Persona Natural Representante Legal Hardware (qscd)	1.3.6.1.4.1.49959.1.1.3.2.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Representante Legal Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.3.3.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Representante Legal Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.3.3.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Representante Legal Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.3.3.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificado de Sello Electrónico	1.3.6.1.4.1.49959.1.1.3.4		
Sello Electrónico Software	1.3.6.1.4.1.49959.1.1.3.4.1	0.4.0.194112.1.1	QCP-l- (inDenova SUB CA 003)
Sello Electrónico Hardware	1.3.6.1.4.1.49959.1.1.3.4.2	0.4.0.194112.1.3	QCP-l-qscd (inDenova SUB CA 003)

Sello Electrónico Lleida.net Wallet	1.3.6.1.4.1.49959.1.1.3.4.3	0.4.0.194112.1.3	QCP-l-qscd (inDenova SUB CA 003)
Sello Electrónico Centralizado UP	1.3.6.1.4.1.49959.1.1.3.4.4	0.4.0.194112.1.3	QCP-l-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificado de Empleado Público	1.3.6.1.4.1.49959.1.1.3.5		
Empleado Público Software	1.3.6.1.4.1.49959.1.1.3.5.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Empleado Público Hardware	1.3.6.1.4.1.49959.1.1.3.5.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público Lleida.net Wallet	1.3.6.1.4.1.49959.1.1.3.5.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público Centralizado UP	1.3.6.1.4.1.49959.1.1.3.5.4	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público Centralizado Huella dactilar	1.3.6.1.4.1.49959.1.1.3.5.5	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificado de Representante Legal Sin Personalidad Jurídica	1.3.6.1.4.1.49959.1.1.3.6		
Representante Legal Sin Personalidad Jurídica Software	1.3.6.1.4.1.49959.1.1.3.6.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Representante Legal Sin Personalidad Jurídica Hardware	1.3.6.1.4.1.49959.1.1.3.6.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)

Representante Legal Sin Personalidad Jurídica Lleida.net Wallet	1.3.6.1.4.1.49959.1.1.3.6.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Representante Legal Sin Personalidad Jurídica Centralizado UP	1.3.6.1.4.1.49959.1.1.3.6.4	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Representante Legal Sin Personalidad Jurídica Centralizado Huella dactilar	1.3.6.1.4.1.49959.1.1.3.6.5	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)

5 CERTIFICADOS DE LA JERARQUIA INDENOVA SL 003

5.1 CERTIFICATION AUTHORITY ROOT

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Version	V3	√	X	
1.2 Serial number	1a7d8fcd5a36	√	X	
1.3 Signature algorithm	Sha256RSA	√	X	
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Common Name (CN)	Certification Authority Root Indenova SL	√	X	
2.2 Organization (O)	Indenova SL	√	-	
2.3 Serial Number (SERIALNUMBER)	B97458996	√	-	
2.4 Organizational Unit (OU)	Certification Authority Indenova SL	√	-	
2.5 Locality (L)	Valencia	√	-	
2.6 Country (C)	ES	√	X	
3 Validity				
3.1 notBefore	lunes, 31 de mayo de 2021 10:19:47	√	X	
3.2 notAfter	viernes, 31 de mayo de 2041 10:19:47	√	X	
4 Subject				
4.1 Common Name (CN)	Certification Authority Root Indenova SL	√	X	
4.2 Organization (O)	Indenova SL	√	-	
4.3 Serial Number (SERIALNUMBER)	B97458996	√	-	
4.4 Organizational Unit (OU)	Certification Authority Indenova SL	√	-	
4.5 Locality (L)	Valencia	√	-	
4.6 Country (C)	ES	√	X	

4.7 Subject Public Key Info - RSA (4096 Bits)	<pre> 30 82 02 0a 02 82 02 01 00 ba 83 81 4f 24 38 3a 1f 91 18 61 0d 41 50 3c 9b e9 ed 7e 3a ad 75 7d c5 b6 09 81 a6 99 02 70 f1 fc ad 84 49 ab ca d4 ca 5f da 53 5a 1c 83 57 a0 70 09 da 1b 0d d0 97 e3 6f 43 f6 90 4b af ca 98 77 8b f0 4a 6d cf 63 02 8e 69 5a 87 d5 a3 16 0a 33 22 fb 37 5b 83 92 e8 68 db 68 34 f5 9e a1 68 f0 98 e7 c5 c5 37 31 5a 21 27 c8 15 e6 b0 1c c6 7a be 10 0e 2b 5e ec a0 6e 0e 3f 54 9a f1 79 2a 6c db 4c 92 df a3 bf c1 76 95 eb cb 0b d6 7a 48 c5 33 88 7e 45 fb d4 c9 66 a9 af cd 75 aa 0d 0a ce 57 81 e0 f4 d6 34 f8 26 96 f7 7b 64 a7 00 72 ab 10 c0 23 92 20 79 d8 6b 05 61 65 3d 27 52 10 00 8d 21 f9 fa 95 e7 7a 02 c2 87 4b ef 3c 5c 1c 0c 54 95 47 41 60 e0 eb df 92 a1 6c 7d 27 ac 00 fa 8e bd 77 be 64 b9 3d 40 f7 2f 3a 88 4a fb e8 60 87 e5 66 9b 4b c0 ad 34 07 26 0f 6d 2a cb af 9b d8 81 09 fe 85 9a 82 b2 cf 35 c2 7d f3 90 66 9a cb 49 7d c4 5f 6c af 68 c9 c5 35 14 0c 36 4d 6c 7c 66 87 c5 4a e6 15 29 e2 a5 2a 65 9f b1 e2 7c c0 06 27 f0 f8 27 d1 5e 18 b5 db 1f 97 3a 81 aa ff 6f d3 b9 59 f9 6f dc d5 52 f1 00 59 de 78 33 d3 3f 09 8e 7b 9a d5 ef 56 5b 61 92 bb 56 26 0f e4 24 3a f8 55 0f 92 04 f6 86 fa c0 2f 83 9f bd 60 05 22 89 30 4f 06 c0 66 e1 8e 02 41 b6 89 be 42 7a 76 be 09 81 32 94 42 15 3f ca 24 4b 6b 4e 69 8e cf 33 91 d6 09 b8 24 b0 c2 95 46 a8 d4 87 60 da b2 73 a7 0d 29 96 16 72 ba c9 32 54 95 06 dd 0f 00 9f 85 bd c1 85 f2 dc d7 99 af d4 4b 3a 1f c7 ba 4a 43 b7 08 88 3b 94 b8 b1 28 0b 9e 83 57 cd 76 dd 19 07 af 5d 4e 14 0b 5f 7c 63 86 48 21 25 7a d7 10 15 fc da 9c 30 11 38 8b 1c 14 cb 9f bf 6d ab </pre>	<p style="text-align: center;">√</p>	<p style="text-align: center;">X</p>
--	--	--------------------------------------	--------------------------------------

	5e f6 f3 21 fe 45 3b a3 67 a2 fb 02 03 01 00 01			
4.8 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	
5.1.1.1 keyIdentifier	b9a1b78314f5dad8bc108901c0e 2d2c5f7a03f1b	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier	b9a1b78314f5dad8bc108901c0e 2d2c5f7a03f1b	√	-	
5.1.3 Key Usage		√	-	
5.1.3.1 digitalSignature	0	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	0	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	

5.1.3.6 keyCertSign	1	√	-
5.1.3.7 cRLSign	1	√	-
5.1.3.8 encipherOnly	0	X	-
5.1.3.9 decipherOnly	0	X	-
5.1.4 Certificate Policies		√	X
5.1.4.1 Policy Identifier	2.5.29.32.0	√	-
5.1.4.2 Policy Qualifier ID	CPS	√	-
5.1.4.2.1 CPS Pointer	URI:https://www.indenova.com/acreditaciones/	√	-
5.1.4.2.2 User Notice		X	-
5.1.5 Subject Alternative Name	No está presente	X	X
5.1.6 Issuer Alternative Name	No está presente	X	X
5.1.7 Subject Directory Attributes	No está presente	X	X
5.1.8 Basic Constraints		√	√
5.1.8.1 cA	Entidad de certificación (CA)	√	-
5.1.8.2 pathLenConstraint	Ninguno	√	-
5.1.9 Name Constraints	No está presente	X	X
5.1.10 Policy Constraints	No está presente	X	X
5.1.11 Extended Key Usage	No está presente	X	X
5.1.11.1 serverAuth	0	-	-
5.1.11.2 clientAuth	0	-	-
5.1.11.3 codeSigning	0	-	-
5.1.11.4 emailProtection	0	-	-
5.1.11.5 timeStamping	0	-	-
5.1.11.6 OCSPSigning	0	-	-
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	0	-	-
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	0	-	-

5.1.12 CRL Distribution Points	No está presente	-	-	
5.1.12.1 CRL Distribution Point 1	-	-	-	
5.1.12.2 CRL Distribution Point 2	-	-	-	
5.1.13 qcStatements	No está presente	-	-	
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	-	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.esigna.es/root/ca_root_indenova_sl.crt	√	-	
5.2.2 Authority Information Access 2	No está presente	-	-	
5.2.2.1 accessMethod		-	-	
5.2.2.2 accessLocation		-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name	ca_root_indenova_sl	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint	103827020875f64987104a55a466c45fe6f6b9e4	√	X	

5.2 INDENOVA SUB CA 003

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Version	V3	√	X	
1.2 Serial number	10f6920d39d8	√	X	
1.3 Signature algorithm	Sha256RSA	√	X	
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Common Name (CN)	Certification Authority Root Indenova SL	√	X	
2.2 Organization (O)	Indenova SL	√	-	
2.3 Serial Number (SERIALNUMBER)	B97458996	√	-	
2.4 Organizational Unit (OU)	Certification Authority Indenova SL	√	-	
2.5 Locality (L)	Valencia	√	-	
2.6 Country (C)	ES	√	X	
3 Validity				
3.1 notBefore	lunes, 31 de mayo de 2021 10:32:46	√	X	
3.2 notAfter	viernes, 31 de mayo de 2041 10:32:46	√	X	
4 Subject				
4.1 Description (Description)	inDenova Subordinate CA 003	√	X	
4.2 Common Name (CN)	inDenova SUB CA 003	√	-	
4.3 Organization (O)	inDenova SL	√	-	
4.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
4.5 Serial Number (SERIALNUMBER)	B97458996	√	-	
4.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	
4.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	
4.8 Locality (L)	VALENCIA	√	X	
4.9 Country (C)	ES	√	-	

4.10 Subject Public Key Info	30 82 02 0a 02 82 02 01 00 b7 2f a3 17 d4 c4 a2 22 5f 21 d8 c5 f1 fc 00 9f 16 58 a0 59 e6 8b 1f 71 d8 09 9a 48 41 ce 92 cf 29 ab df cc 56 6e 05 98 b3 09 ad 61 a9 5c bb 2f 46 23 0f 79 e6 2f 5e 3c 62 0e 6e 70 42 14 4e 9f 0f 06 d1 e8 d1 b2 3e 4b 81 7f a2 9d 21 15 bc 13 82 57 7f 24 5d ae bc 86 b4 8d 83 a8 a1 37 50 3c 91 86 57 a9 4b 4e 4a 28 25 6a 11 4b d8 90 7c 8f f6 1b 59 df bc 93 20 df 0b 52 f0 3f 35 35 44 e6 16 7e e3 65 07 e7 76 03 0a 33 cf 55 85 44 8c b8 3d ec 76 95 43 5f 36 f9 f1 ea 16 ea bb 6b ea 38 ad c3 62 4d a7 0b 18 40 a6 98 16 fd 57 a1 f6 0d c4 8a da 2f 5c a8 c4 4c f8 d2 5d a0 8f 5f 7d 55 e7 ea 4a 80 38 de 6a 95 8f fe 58 23 1c 90 be 55 c8 51 b4 d9 e2 d3 8a a3 f7 0f 67 65 5a a2 16 68 91 24 49 11 2d 35 71 86 14 3d 5f c0 af 6d 62 1b eb ba 1d 49 c9 9c a7 8f ee f8 d8 64 aa 2a bc 2c 02 1f 7e bd 28 3c 1d cf 1f d5 f3 ba 71 b5 80 dc 32 a3 90 3f 5d b0 5e a9 f5 e5 67 de 76 0e e9 5e 1e 43 1e fb 9e 80 38 b9 ee 7a db 06 e9 1c 55 9a 92 4b 59 e2 f6 98 2e 2a 46 79 15 67 70 d4 3a 20 b6 79 d0 7b 31 58 41 72 60 85 09 29 d7 21 5f f7 85 34 94 86 bb b6 3c 11 b4 23 11 3b e8 91 a7 2b 73 71 d8 ab ea ec 88 68 18 0b a2 29 a8 5a f7 95 36 fb 00 ac 85 37 dc d1 17 89 62 14 51 b1 a5 46 48 9b d2 23 22 b0 53 ba e9 f8 ba b4 5d 36 31 d1 49 11 dc 27 13 a4 dd 3d be 47 40 69 24 fd 24 1c 33 39 02 3e 19 30 d2 d6 b8 cd 60 03 b4 d3 7f b8 90 1a f2 04 c9 87 8f c0 e9 6f 53 ec 11 ab 09 14 d5 c7 0b 8e 22 9c 40 d9 91 88 ec 56 c0 30 10 e0 0a f2 55 e3 d4 c8 52 e6 74 57 38 8b c7 93 b4 c6 4e 09 09 fb 30 c4 c6 43 04 1c 48 6f c4 2b 13 5a 18 2d 50 f1 2c 1b 34 9e df 94 1c a3 20 96 19 3f 02 03 01 00 01	√	X	
4.11 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	
5.1.1.1 keyIdentifier	b9a1b78314f5dad8bc108901c0e2d2c5f7a0 3f1b	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	

5.1.2 Subject Key Identifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-	
5.1.3 Key Usage		√	-	
5.1.3.1 digitalSignature	0	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	0	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	1	√	-	
5.1.3.7 cRLSign	1	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	
5.1.4.1 Policy Identifier	2.5.29.32.0	√	-	
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	URI:http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	
5.1.4.2.2 User Notice		X	-	
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	
5.1.7 Subject Directory Attributes	No está presente	X	X	
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	Entidad de certificación (CA)	√	-	
5.1.8.2 pathLenConstraint	0	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	
5.1.11.1 serverAuth	0	-	-	
5.1.11.2 clientAuth	1	-	-	
5.1.11.3 codeSigning	0	-	-	
5.1.11.4 emailProtection	1	-	-	
5.1.11.5 timeStamping	0	-	-	
5.1.11.6 OCSPSigning	0	-	-	
5.1.11.7 Microsoft Smart Card Logon for Windows	0	-	-	
1.3.6.2.1.311.20.2.2				
5.1.11.8 Microsoft Commercial Code Signing	0	-	-	
1.3.6.2.1.311.2.1.22				

5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	0	-	-	
5.1.12 CRL Distribution Points		√	-	
5.1.12.1 CRL Distribution Point 1	URL=http://crl.esigna.es/root/ca_root_inde nova_sl.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.esigna.es/root/ca_root_ind enova_sl.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URL=http://certs.esigna.es/root/ca_root_in denova_sl.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp2.esigna.es	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint	71cbfc6733eac701cc74a542548168bf30adf ba4	√	X	

5.3 INDENOVA OCSP 003

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Version	V3	√	X	
1.2 Serial number	2e56e89f8e9c	√	X	
1.3 Signature algorithm	Sha256RSA	√	X	
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	
2.3 Organization (O)	inDenova SL	√	-	
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	
2.8 Locality (L)	VALENCIA	√	X	
2.9 Country (C)	ES	√	-	
3 Validity				
3.1 notBefore	lunes, 31 de mayo de 2021 11:09:19	√	X	
3.2 notAfter	sábado, 31 de mayo de 2031 11:09:19	√	X	
4 Subject				
4.1 Description (Description)	inDenova SL OCSP Responder Certificate 003	√	X	
4.2 Common Name (CN)	inDenova OCSP 003	√	-	
4.3 Organization (O)	inDenova SL	√	-	
4.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
4.5 Serial Number (SERIALNUMBER)	B97458996			
4.6 Organizational Unit (OU)	Online Certificate Status Protocol inDenova SL	√	-	
4.7 Title (T)	OCSP Service inDenova SL	√	-	
4.8 Locality (L)	VALENCIA	√	X	
4.9 Country (C)	ES	√	-	

4.10 Subject Public Key Info	<pre> 30 82 02 0a 02 82 02 01 00 9f 7a 1c dc 1a c3 7b 88 85 e9 0a 15 87 e0 58 2f 3a c2 0c f9 d2 42 22 5d e0 2d 15 5b 02 7c 81 41 7d c9 f1 25 9f fc 2a 6c e1 88 0e 42 67 8b 09 b6 a0 36 37 ad 3e a8 9a 76 86 9d f2 a4 96 52 12 54 42 aa f4 15 6e 6a a2 65 b4 68 67 bd 12 a1 c9 70 8e 69 dd a0 82 d8 c5 1d b3 bd d6 a2 c6 0e 55 fa 3f 77 2e 04 4f 62 2e 82 6d 0a 0e 36 31 e2 3a 2d af 0f 8f 9e bb 65 ca 66 d3 16 59 f0 78 57 e2 de bc 7f fc c5 16 9d 9c 95 55 ac 08 74 0d 2b 94 84 ba 46 45 f2 9d ab 94 24 02 c6 8b 7c e2 a5 ab f8 92 a0 3b 18 0d 20 c4 b5 0a da f0 95 e2 d6 36 ac 6d 20 87 e5 48 0c 79 57 8a ec c7 92 06 39 59 40 1d 3d 78 b6 54 e9 ae da 15 89 35 73 ba 2c 90 44 7f d8 98 da 93 41 e5 ee 82 49 b1 09 64 19 77 af c1 4e 0f 0b 38 3b a0 8f 19 38 fe ff b9 c0 58 85 03 00 ee a5 47 2c b2 dd c5 f4 1b ed 00 e6 87 d5 bf 72 40 72 06 71 bb b5 c5 04 06 32 ac 41 85 a7 55 ca d1 aa d6 df a4 a3 62 bb 51 c7 f7 8f 2b 7a 67 3d 6a 00 ce 6d 3c 87 06 33 c5 86 17 80 21 2c cb d2 91 52 b6 13 b9 34 55 8d e2 3b 2e ef c7 3b 08 1c b8 d2 bb 03 b5 06 bf c4 12 1c b4 62 00 06 62 3b 08 87 30 e4 21 80 6d 67 68 81 1d f8 75 3a 9c 8b 3d 64 a2 05 43 9f e1 21 7d aa 7f dc 59 ec 69 77 ca ea 7d d9 cb 52 dc ab dc 25 41 5c e2 6c 9b f5 40 96 64 5d 08 31 a9 d2 8c 0d de 7a dd d0 bd 62 44 70 6e e6 38 73 ff cd 4e f6 2b c0 fe da 31 27 91 ca 00 c5 1d c8 b0 a5 f7 4e 78 4f ca ee f1 05 e7 97 66 cc 1a 69 52 0f 73 c6 56 b6 c2 8a 61 35 c6 e3 c8 4c dd aa fd 76 0a 4d 53 b1 fb 48 3e 1f 55 05 66 dd bc 60 60 41 4c e2 e5 11 55 dc 47 87 09 9d 3f 40 88 22 57 db b4 aa 93 25 43 9d c8 9d 02 76 68 c6 7e a1 10 27 4d a6 ff e8 e6 87 02 03 01 00 01 </pre>	√	X	
4.11 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	

5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-
5.1.1.2 authorityCertIssuer		X	-
5.1.1.3 authorityCertSerialNumber		X	-
5.1.2 Subject Key Identifier	03de508f7e6a5c3ed9e7e5a436fe41f6fc04782a	√	-
5.1.3 Key Usage		√	-
5.1.3.1 digitalSignature	1	X	-
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-
5.1.3.3 keyEncipherment	1	X	-
5.1.3.4 dataEncipherment	0	X	-
5.1.3.5 keyAgreement	0	X	-
5.1.3.6 keyCertSign	0	√	-
5.1.3.7 cRLSign	0	√	-
5.1.3.8 encipherOnly	0	X	-
5.1.3.9 decipherOnly	0	X	-
5.1.4 Certificate Policies		√	X
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.4	√	-
5.1.4.2 Policy Qualifier ID	CPS	√	-
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-
5.1.4.2.2 User Notice	Warranty limitations of this certificate can be found in the CPS	√	-
5.1.5 Subject Alternative Name	No está presente	X	X
5.1.6 Issuer Alternative Name	No está presente	X	X
5.1.7 Subject Directory Attributes	No está presente	X	X
5.1.8 Basic Constraints		√	√
5.1.8.1 cA	End Entity	√	-
5.1.8.2 pathLenConstraint	No está presente	√	-
5.1.9 Name Constraints	No está presente	X	X
5.1.10 Policy Constraints	No está presente	X	X
5.1.11 Extended Key Usage		X	X
5.1.11.1 serverAuth	0	-	-
5.1.11.2 clientAuth	0	-	-
5.1.11.3 codeSigning	0	-	-
5.1.11.4 emailProtection	0	-	-
5.1.11.5 timeStamping	0	-	-
5.1.11.6 OCSPSigning	1	-	-

5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	0	-	-	
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	0	-	-	
5.1.12 CRL Distribution Points		√	-	
5.1.12.1 CRL Distribution Point 1	URL=http://crl.esigna.es/sub/indenova_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.esigna.es/sub/indeno va_pki_003.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URL=http://certs.esigna.es/ca/indeno va_pki_003.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp2.esigna.es	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	

7.2 Thumbprint	028a8572a101f28975a8d6f0ad42f4c23 c7b5b62	√	X	
-----------------------	--	---	---	--

5.4 INDENOVA OCSP 003 TSA

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Version	V3	√	X	
1.2 Serial number	4999981b06e6	√	X	
1.3 Signature algorithm	Sha256RSA	√	X	
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova SL Timestamping Certificate 003	√	X	
2.2 Common Name (CN)	inDenova TSA 003	√	-	
2.3 Organization (O)	inDenova SL	√	-	
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
2.5 Serial Number (SERIALNUMBER)	B97458996			
2.6 Organizational Unit (OU)	Trusted Timestamp Service inDenova SL	√	-	
2.7 Title (T)	Service Timestamping inDenova SL	√	-	
2.8 Locality (L)	VALENCIA	√	X	
2.9 Country (C)	ES	√	-	
3 Validity				
3.1 notBefore	lunes, 31 de mayo de 2021 11:12:02	√	X	
3.2 notAfter	sábado, 31 de mayo de 2031 11:12:02	√	X	
4 Subject				
4.1 Description (Description)	inDenova SL OCSP Responder Certificate 003 TSA	√	X	
4.2 Common Name (CN)	inDenova OCSP 003 TSA	√	-	
4.3 Organization (O)	inDenova SL	√	-	
4.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
4.5 Serial Number (SERIALNUMBER)	B97458996	√	-	
4.6 Organizational Unit (OU)	Online Certificate Status Protocol inDenova SL	√	-	
4.7 Title (T)	OCSP Service inDenova SL	√	-	
4.8 Locality (L)	VALENCIA	√	X	
4.9 Country (C)	ES	√	-	

4.10 Subject Public Key Info	<pre> 30 82 02 0a 02 82 02 01 00 e2 e9 ce 58 3b 3f 93 15 f4 8e e1 06 22 94 c4 4d 3a f6 1a 07 63 a4 61 b0 6b 5f ee aa 34 2a 02 85 f1 67 2a 4d 46 71 7f 0c f8 a0 45 33 27 2b ab 82 08 28 db 09 3a df d8 8a 27 56 ae 48 ed dc 47 f9 2f a2 af ba 09 10 26 c9 d9 31 03 af cf 74 73 cd 7a 0f e8 a7 34 32 9b 43 4f 7a 86 2c 66 76 90 e0 0c 4f 53 fd 04 36 c9 66 dd 19 d9 0f 1b 22 cb bd 87 e5 1c a1 22 39 5a 62 c8 8b 47 e5 76 f9 73 4a ad df e1 9d a5 53 69 f2 ee 9d 70 70 24 62 c5 74 93 8b 9e 58 a2 67 10 66 16 ae 4b 66 2c d2 30 3f 49 27 26 22 58 0c 7d 5b 79 de 5c 03 11 64 c6 1f 17 e5 08 ea 03 6f 79 c3 92 d4 a6 f9 a0 4d ea 83 06 f6 c6 25 63 04 ed 03 f2 c3 5b 95 44 18 39 dd a3 eb 97 34 ab 42 e1 64 0a ce 93 2d 5d 18 47 f6 96 24 37 72 de 6c f2 0e 7e 61 bb 7b 27 8d 0b 69 f7 6c 58 6b 61 36 85 64 5b 7c 58 53 4d e4 04 ac 73 38 3c 4f 05 cd 6b c2 33 8b a8 58 80 97 ad 5f ab bd e4 26 cb b3 51 86 08 17 d1 ef df 50 19 95 86 95 7c eb b0 e2 82 38 74 02 6b 7b 30 01 cd 1a ea 05 14 8d 53 d5 d1 f3 b1 7e 63 0d 8b e0 2d 41 8d c6 e4 24 1a 78 db 68 95 77 cd a3 9f 8b c0 62 36 d2 dc 9e e0 50 4e c9 7c 6f c7 56 e0 f1 82 a0 dd 5a 9d 7b 49 43 18 1b 42 da 73 8e e4 33 3c 58 2c 2d 7d 30 17 63 bb 8a fa 8a f2 af 90 fc 41 0a fa fb c7 e7 14 49 32 4c b1 4a ab 74 46 41 61 40 36 26 55 af 89 ab d0 e8 3d b9 b5 c4 3e b9 c7 0e fd fb b0 ca ab ff 35 26 c1 28 c3 4a b7 ae 90 53 f7 86 cc 7b 8d a2 4b 20 39 ab f9 6f ff fa 30 93 9b 16 62 0f 37 4f 83 f4 ea 6f 0f d4 7b d5 9f 04 ed 98 d9 de b2 b4 54 4e 64 c9 27 bd 0a d9 d5 14 cf 8f 2e ce a6 bb ee fe 0b 7b 6f 87 0f 3b dd ea 1c 21 1e 30 94 37 </pre>	√	X
-------------------------------------	---	---	---

	4e 49 34 ee 5d 5a 7f fa d8 b1 02 03 01 00 01			
4.11 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	
5.1.1.1 keyIdentifier	2b6e5ef1da667db6e7ae1f606e9e da3a3fb3efb1	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier	c58ce47ed2d08f7978bf165c8650d 4e0f58797a0	√	-	
5.1.3 Key Usage		√	-	
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	1	X	-	

5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.4	√	-	
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/tsa/cps_tsa003.pdf	√	-	
5.1.4.2.2 User Notice	Warranty limitations of this certificate can be found in the CPS	√	-	
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	
5.1.7 Subject Directory Attributes	No está presente	X	X	
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	X	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	
5.1.11.1 serverAuth	0	-	-	
5.1.11.2 clientAuth	0	-	-	
5.1.11.3 codeSigning	0	-	-	
5.1.11.4 emailProtection	0	-	-	
5.1.11.5 timeStamping	0	-	-	
5.1.11.6 OCSPSigning	1	-	-	
5.1.11.7 Microsoft Smart Card Logon for Windows	0	-	-	
1.3.6.2.1.311.20.2.2				
5.1.11.8 Microsoft Commercial Code Signing	0	-	-	
1.3.6.2.1.311.2.1.22				
5.1.11.9 Microsoft Encrypting File System	0	-	-	
1.3.6.2.1.31136.10.3.4				
5.1.12 CRL Distribution Points		√	-	
5.1.12.1 CRL Distribution Point	URL=http://crl.esigna.es/tsa/index_nova_tsa_003.crl	√	-	
1				
5.1.12.2 CRL Distribution Point	URL=http://crl1.esigna.es/tsa/index_nova_tsa_003.crl	√	-	
2				

5.1.13 qcStatements	No está presente	-	-	
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URL=http://certs.esigna.es/tsa/in denova_tsa_003.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp2.esigna.es	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint	b23f0e86869a9935c215f21963ec752c8fb74e54	√	X	

5.5 INDENOVA OCSP 003 ROOT

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Version	V3	√	X	
1.2 Serial number	2a792fe51872	√	X	
1.3 Signature algorithm	Sha256RSA	√	X	
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Common Name (CN)	Certification Authority Root Indenova SL	√	X	
2.2 Organization (O)	Indenova SL	√	-	
2.3 Serial Number (SERIALNUMBER)	B97458996	√	-	
2.4 Organizational Unit (OU)	Certification Authority Indenova SL	√	-	
2.5 Locality (L)	Valencia			
2.6 Country (C)	ES	√	-	
3 Validity				
3.1 notBefore	lunes, 31 de mayo de 2021 11:02:07	√	X	
3.2 notAfter	sábado, 31 de mayo de 2031 11:02:07	√	X	
4 Subject				
4.1 Description (Description)	inDenova SL OCSP Responder Certificate 003	√	X	
4.2 Common Name (CN)	inDenova OCSP 003 ROOT	√	-	
4.3 Organization (O)	inDenova SL	√	-	
4.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
4.5 Serial Number (SERIALNUMBER)	B97458996	√	-	
4.6 Organizational Unit (OU)	Online Certificate Status Protocol inDenova SL	√	-	
4.7 Title (T)	OCSP Service inDenova SL	√	-	
4.8 Locality (L)	VALENCIA	√	X	
4.9 Country (C)	ES	√	-	

4.10 Subject Public Key Info	<pre> 30 82 02 0a 02 82 02 01 00 e9 b9 2c 3d e2 9c 2a ce 2e 38 64 d4 c7 59 36 3f e8 9f c0 c7 36 44 56 16 b8 d7 1e 30 40 d0 97 87 0e 8d a7 80 0a f9 ba 78 4c d6 31 97 4f d7 1c 0b 32 c9 14 28 13 8b 9a 8d 09 74 0e c8 f0 dc 6c d2 4f 9d 03 9a 69 6c 74 87 11 58 74 26 29 13 6d 29 35 ef e8 82 8d 70 db 6f 88 32 7c 28 c4 38 8f 1a a4 54 a4 dc 1d d4 e7 65 e3 36 a1 65 fb 1b 06 e0 60 47 4c ea 84 32 1f 32 56 e1 7d 61 58 67 c2 e6 df 2a 92 55 1f 21 fd 26 64 e5 c7 75 d0 4d 8c f0 17 d6 b3 35 23 d5 df 61 8d c1 5a 61 cf ca ac 46 d9 15 e1 90 b8 ab b5 13 fc 67 20 42 6f a6 20 a3 56 30 26 89 af a5 08 9e 50 11 8f 2a af b6 76 a8 8f c3 30 d8 ec 21 1a 49 e4 f6 9f af 20 77 41 5a 0a a7 74 fe a7 95 74 54 83 e6 0b a0 6b 6e f2 81 ca 2a 4e d7 3b 4f 76 46 a8 ef 4e 37 c9 4a 15 4b 14 6b 0b 81 2f 44 1f 43 82 33 bf 8d ce ab 21 49 ca 73 30 3b ec 23 f9 55 28 fa 2c e6 b9 10 11 7f f0 ac 96 d5 ca fc 12 6a 78 71 33 77 72 37 42 67 96 d8 84 d0 b2 87 5e 97 ed 3d bc ad 3d af 5d b3 c0 55 15 99 8a dc 07 a1 ec 50 2b 37 5e b4 ce fb cc 75 87 6d 48 13 61 1f eb ac 66 78 14 e7 68 2d 4e 56 21 fd bc 8d a6 d6 01 48 c9 0a 3e 12 45 8a de fb 27 f7 31 70 da 23 f7 c3 5a 10 60 85 77 f7 d7 d1 6c 83 ef 12 51 27 7f 51 c6 41 a1 6a d1 d1 11 fe a9 5d 6f dd 00 0b bd bf b2 70 79 fc 9d 02 cd c0 8d 81 15 61 ab 67 8e fd 2b b3 38 1d 9f 7f bb f2 3b 41 c2 99 43 48 c9 99 77 fa 06 78 82 4a 04 9d 9f a7 e4 31 d5 ef 98 0b f3 a7 df 8d 5d d0 2c d6 37 d1 ed 41 86 76 20 a2 32 26 b1 e1 85 75 db 76 24 23 12 7a de 75 9d 38 0a aa 1c c5 aa 58 6d bd 73 08 4c cc 9f a1 d4 2e 45 46 90 52 c6 08 4a 8a f4 29 28 89 99 0b 1b d4 d4 e8 a7 c9 da b9 02 03 01 00 01 </pre>	√	X	
4.11 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				

5.1.1 Authority Key Identifier		√	X	
5.1.1.1 keyIdentifier	b9a1b78314f5dad8bc108901c0e2d2c5f7a03f1b	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier	933032cd429da8f2dc0dc9e7e610f43cb47e941c	√	-	
5.1.3 Key Usage		√	-	
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	1	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.4	√	-	
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	https://www.indenova.com/acreditaciones/	√	-	
5.1.4.2.2 User Notice	Warranty limitations of this certificate can be found in the CPS	√	-	
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	
5.1.7 Subject Directory Attributes	No está presente	X	X	
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	X	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	
5.1.11.1 serverAuth	0	-	-	
5.1.11.2 clientAuth	0	-	-	

5.1.11.3 codeSigning	0	-	-	
5.1.11.4 emailProtection	0	-	-	
5.1.11.5 timeStamping	0	-	-	
5.1.11.6 OCSPSigning	1	-	-	
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	0	-	-	
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	0	-	-	
5.1.12 CRL Distribution Points		√	-	
5.1.12.1 CRL Distribution Point 1	URL=http://crl.esigna.es/root/ca_root_indenova_sl.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.esigna.es/root/ca_root_indenova_sl.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URL=http://certs.esigna.es/root/ca_root_indenova_sl.crt	√	-	
5.2.2 Authority Information Access 2		-	-	

5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp2.esigna.es	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint	0cc5a0e29a48bbc9ab24f36ed645d30b1793ffee	√	X	

5.6 INDENOVA TSA 003

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Version	V3	√	X	
1.2 Serial number	56de6c771d42	√	X	
1.3 Signature algorithm	Sha256RSA	√	X	
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Common Name (CN)	Certification Authority Root Indenova SL	√	X	
2.2 Organization (O)	Indenova SL	√	-	
2.3 Serial Number (SERIALNUMBER)	B97458996	√	-	
2.4 Organizational Unit (OU)	Certification Authority Indenova SL	√	-	
2.5 Locality (L)	Valencia	√	-	
2.6 Country (C)	ES	√	X	
3 Validity				
3.1 notBefore	lunes, 31 de mayo de 2021 10:43:01	√	X	
3.2 notAfter	viernes, 31 de mayo de 2041 10:43:01	√	X	
4 Subject				
4.1 Description (Description)	inDenova SL Timestamping Certificate 003	√	-	
4.2 Common Name (CN)	inDenova TSA 003	√	X	
4.3 Organization (O)	inDenova SL	√	-	
4.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
4.5 Serial Number (SERIALNUMBER)	B97458996	√	-	
4.6 Organizational Unit (OU)	Trusted Timestamp Service inDenova SL	√	-	
4.7 Title (T)	Service Timestamping inDenova SL	√	-	
4.8 Locality (L)	VALENCIA	√	-	
4.9 Country (C)	ES	√	X	

4.10 Subject Public Key Info	<pre> 30 82 02 0a 02 82 02 01 00 9f 9f 34 0a d6 7f cb 99 a2 10 e6 01 e9 22 37 9a f3 08 c8 ce 1c 65 a2 a2 1a 96 eb 14 ad bc c5 21 ec 35 9d d7 ff 82 4c e9 db 4d 78 4b 09 8f 9b db 1b c9 34 32 ce e7 45 5b 07 7e 54 80 35 67 dd 13 e8 9d a9 bb d4 f1 76 40 57 39 c5 9d 44 10 21 d5 7c e6 cd 36 a7 ec 89 9c dc dd 9e 00 53 93 20 0a 11 89 51 2e 99 19 8b 70 c0 2a f2 9b 72 8c 38 e9 32 5e a2 08 ba 63 08 2a ed 25 01 e0 34 5a a5 8e 13 d6 46 eb 4a 9a 08 1f 44 f9 07 0b 55 60 fe 56 c7 a6 8b d9 f5 33 66 d4 4f 41 90 3f ec 05 af e6 fd 9e 9c 2d df 22 2b a4 db f6 94 93 8d 11 74 65 2b 21 9c ab 0f 79 62 30 0b 17 04 54 3e d0 13 66 b1 0f 8b 16 86 de bb 4f 1f 1f de c1 d8 e2 cf ad 3c a6 72 b2 36 42 0b ea 09 38 ed 05 b8 9a 14 90 86 c0 57 5d a3 0f e9 73 7e c1 6d 25 f3 0a 3e 08 d1 09 df bf c6 b7 c9 f2 54 7e 23 51 5c ab 6c db 17 88 b4 7e 8c bd a9 ed 82 02 bb 28 30 a2 23 46 c9 eb 09 6b 86 68 5b df 03 6c c3 4a 63 b0 9c 5b c3 9f c5 f2 96 f9 09 2c 39 52 da 51 cb 7f d5 e8 48 b6 ec c9 4e 32 63 9d 05 5b 1d 3b 4b 23 e3 3c 09 0c af e8 15 84 a6 b1 96 35 65 27 1c 22 2a 3e 76 fb 90 54 41 c7 cc fe 7b 8f 8a a3 48 22 93 eb c4 bf 14 1e 45 52 e7 5f 52 f7 04 1b 3d ce 50 85 8f 64 c0 b0 3b f5 30 05 37 15 ed 88 31 67 8c 89 a3 f8 0c ea f4 31 88 fd 30 b7 16 87 42 4a db cc 43 85 59 ab ab 65 eb 1b 5a 6a 8b f8 b3 80 6a 69 18 04 7f bc 2a 87 ff 24 0d 54 0d 9a e2 89 4e 2c 96 58 8b 96 6c 79 1c e3 8a d6 85 23 34 8f 74 34 03 cc 0f 98 97 27 41 3e ca 4f d6 ee 0d c0 b9 a2 ea b7 39 a2 38 6b 09 ff 88 f6 ee 19 f7 fa c3 13 71 16 15 1e 99 77 0c ab 08 e0 77 25 15 a9 fa e1 48 4e cb 6b 2f 07 da 11 7d 98 d0 1a 34 15 9b 4d 02 03 01 00 01 </pre>	√	X	
4.11 Public key parameters	05 00	√	X	
5 Extensions				

5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	
5.1.1.1 keyIdentifier	b9a1b78314f5dad8bc108901c0e2d2c5f7a03f1b	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier	2b6e5ef1da667db6e7ae1f606e9eda3a3fb3efb1	√	-	
5.1.3 Key Usage		√	-	
5.1.3.1 digitalSignature	0	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	0	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	1	√	-	
5.1.3.7 cRLSign	1	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	
5.1.4.1 Policy Identifier	2.5.29.32.0	√	-	
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	URI:http://cps.esigna.es/tsa/cps_tsa003.pdf	√	-	
5.1.4.2.2 User Notice	Warranty limitations of this certificate can be found in the CPS	√	-	
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	
5.1.7 Subject Directory Attributes	No está presente	X	X	
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	Entidad de certificación (CA)	√	-	
5.1.8.2 pathLenConstraint	0	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	
5.1.11.1 serverAuth	0	-	-	
5.1.11.2 clientAuth	0	-	-	
5.1.11.3 codeSigning	0	-	-	
5.1.11.4 emailProtection	0	-	-	

5.1.11.5 timeStamping	0	-	-	
5.1.11.6 OCSPSigning	0	-	-	
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	0	-	-	
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.2.2	0	-	-	
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	0	-	-	
5.1.12 CRL Distribution Points		√	-	
5.1.12.1 CRL Distribution Point 1	URL=http://crl.esigna.es/root/ca_ro ot_indenova_sl.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.esigna.es/root/ca_r oot_indenova_sl.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URL=http://certs.esigna.es/root/ca_ root_indenova_sl.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp2.esigna.es	-	-	
5.2.3 Subject Information Access	No está presente	-	-	

7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint	bc380488eb446c184a56e6562312e0 a91d928b73	√	X	

5.7 INDENOVA TSU 003

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Version	V3	√	X	
1.2 Serial number	33844e4d5ac4	√	X	
1.3 Signature algorithm	Sha256RSA	√	X	
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova SL Timestamping Certificate 003	√	X	
2.2 Common Name (CN)	inDenova TSA 003	√	-	
2.3 Organization (O)	inDenova SL	√	-	
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
2.5 Serial Number (SERIALNUMBER)	B97458996			
2.6 Organizational Unit (OU)	Trusted Timestamp Service inDenova SL	X	-	
2.7 Title (T)	Service Timestamping inDenova SL	√	-	
2.8 Locality (L)	VALENCIA	√	X	
2.9 Country (C)	ES	√	-	
3 Validity				
3.1 notBefore	lunes, 31 de mayo de 2021 10:53:49	√	X	
3.2 notAfter	sábado, 31 de mayo de 2031 10:53:49	√	X	
4 Subject				
4.1 Description (Description)	inDenova SL Timestamping Certificate 003	√	X	
4.2 Common Name (CN)	inDenova TSU 003	√	-	
4.3 Organization (O)	inDenova SL	√	-	
4.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	
4.5 Serial Number (SERIALNUMBER)	B97458996	√	-	
4.6 Organizational Unit (OU)	Trusted Timestamp Service inDenova SL	√	-	
4.7 Title (T)	Service Timestamping inDenova SL	√	-	
4.8 Locality (L)	VALENCIA	√	X	

4.9 Country (C)	ES	√	-	
4.10 Subject Public Key Info	30 82 02 0a 02 82 02 01 00 b6 d9 ee e8 47 b3 ad 82 3e 88 43 83 8d 05 c0 2a f8 88 3b ea 52 2c df 48 68 7b f4 6f 32 65 ef ae 32 57 d6 57 72 2b da 3f c3 a3 22 d6 59 f6 39 74 6c d1 ee 8a b0 91 5e 72 2b 74 0c d5 1e 0c 54 98 45 5d 07 85 83 1f 0e ad ae 06 d3 1e e7 6c 53 34 99 74 13 be ab 12 a5 bf bf 29 91 73 66 78 83 5f 2a 2a ca d0 ce c6 02 f5 d5 80 36 64 cc de de 41 73 bb e2 76 3e 0a 2b e3 72 c3 33 80 fb 20 4d 72 2a ce 57 08 6d 73 49 3f d1 a3 be e6 33 33 7e 06 d8 81 bd 6d c1 bf da 02 38 55 05 8f b8 35 5b ab 3a d8 06 d5 ce 85 39 05 47 56 e6 ef 0c a2 0c 78 d2 04 af f2 81 c1 d2 34 9f 6f bc 36 e0 1a 1c 80 5b 28 34 a1 cb 81 00 89 21 22 fe 0e 26 cc 49 50 58 b3 1c c8 e1 e8 69 a6 c0 cf 0d 4a 8b 1e b0 45 2e d2 1d 30 0a b4 2d e2 c0 1d 07 9f 79 46 9f a0 4e 28 80 da f8 2c 21 fd a2 f8 9e 94 74 e5 31 d5 b5 18 66 f8 65 c4 e1 9f 18 f8 71 9e 94 e3 cb 70 26 cb b4 19 e3 31 14 37 9a c8 e2 1e 7a 39 b6 07 e8 33 62 1e 84 e8 80 5b 0a 16 c1 6e 79 78 da 25 6e 17 43 ee 7c 2c 8f e8 a7 c3 97 4a d3 f1 01 7c 64 ed 8e d3 b0 4a 4e fe de c0 a9 5d 52 9f bb 01 70 79 ff e2 f4 a6 db c6 48 21 53 74 3d 69 b8 16 8c cc 2f 72 8c 7b ef 22 a1 aa 00 fe 94 8a 2f 56 e4 9b d3 82 2d 7c 6c f7 9d dd 9b 4b 2f 30 98 0e c3 bf 5c 7f 2f 1a 58 3b 48 1d ad 50 97 41 23 34 83 ff a5 93 ae 71 7a 7e 52 a4 26 da 9a 1e 7e 40 85 c1 94 21 c3 c2 17 ec 6a 75 88 ae a5 83 40 7f 18 0c 95 2d 88 a5 43 43 49 94 98 f9 3b e9 29 40 72 c1 1e a4 de 80 bf e9 dc ef 8a d5 6b 24 ac de 6a 05 86 bd 07 0d f2 56 fe 29 4f f3 18 3b 11 c4 96 35 fe fa 35 a0 f6 99 b6 4a c5 22 68 70 65 89 4d 11 92 e8 7c 64 ee bd 30 25 c9 49 73 c6 df f9 02 03 01 00 01	√	X	
4.11 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				

5.1.1 Authority Key Identifier		√	X	
5.1.1.1 keyIdentifier	2b6e5ef1da667db6e7ae1f606e9eda3a3fb3efb1	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier	906912085cdac064ce860d60effa7a34752cebb8	√	-	
5.1.3 Key Usage		√	-	
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.5	√	-	
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/tsa/cps_tsa003.pdf	√	-	
5.1.4.2.2 User Notice	Warranty limitations of this certificate can be found in the CPS	√	-	
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	
5.1.7 Subject Directory Attributes	No está presente	X	X	
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	X	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	
5.1.11.1 serverAuth	0	-	-	
5.1.11.2 clientAuth	0	-	-	
5.1.11.3 codeSigning	0	-	-	
5.1.11.4 emailProtection	0	-	-	

5.1.11.5 timeStamping	1	-	-	
5.1.11.6 OCSPSigning	0	-	-	
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	0	-	-	
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.2.2	0	-	-	
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	0	-	-	
5.1.12 CRL Distribution Points		√	-	
5.1.12.1 CRL Distribution Point 1	URL=http://crl.esigna.es/tsa/indenova_tsa_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.esigna.es/tsa/indenova_tsa_003.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URL=http://certs.esigna.es/tsa/indenova_tsa_003.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp2.esigna.es	-	-	
5.2.3 Subject Information Access	No está presente	-	-	

7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint	0d43073ae0fd710291353564a8901536 c5f357a7	√	X	

6 PERFILES DE CERTIFICADOS DE INDENOVA SUBCA 003

De acuerdo al artículo 27.1 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos establece que “Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal que conste como tal de manera inequívoca.”

NOTA: Aquellos perfiles de certificados que no contengan al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal no podrán ser utilizados para la identificación y firma de las personas interesadas ante las Administraciones Públicas¹

6.1 PERSONA NATURAL

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	RFC 5280
1.2 Serial number		√	X	Establecido por la plataforma PKI al momento de generar el certificado

¹ Administraciones Públicas en el ámbito subjetivo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	OID 2.5.4.13
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	OID 2.5.4.3
2.3 Organization (O)	inDenova SL	√	-	OID 2.5.4.10
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	OID 2.5.4.97
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	OID 2.5.4.5
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	OID 2.5.4.11
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	OID 2.5.4.12
2.8 Locality (L)	VALENCIA	√	X	OID 2.5.4.7
2.9 Country (C)	ES	√	-	OID 2.5.4.6
3 Validity				
3.1 notBefore		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
3.2 notAfter		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
4 Subject				
4.1 Description (Description)	Persona Natural - Emitido por inDenova SUB CA 003	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Documento identificativo, nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 (DOCUMENTO IDENTIFICATIVO) NOMBRE APELLIDOS
4.3 Serial Number SERIALNUMBER)	Documento identificativo del responsable, según la norma técnica ETSI EN 319 412-1 (IDCES + NIF del responsable)	√	-	OID 2.5.4.5

4.4 Email Address (E)	Dirección de correo electrónico del suscriptor	√	-	Dirección de correo electrónico del suscriptor
4.5 Locality (L)	Distrito del suscriptor	√	-	OID 2.5.4.7 Distrito del suscriptor
4.6 Country (C)	Nacionalidad del suscriptor	√	-	OID 2.5.4.6 Nacionalidad del suscriptor. Código de país codificado de acuerdo al ISO 3166-1 alpha-2
4.7 StateOrProvinceName (S)	Provincia del suscriptor	√	-	OID 2.5.4.8 Provincia del suscriptor
4.8 Given Name (G)	Nombre del suscriptor	√	-	OID 2.5.4.42 NOMBRE
4.9 Surname (SN)	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDOS
4.10 Subject Public Key Info	RSAEncryption Clave pública de 4096 bits (RFC3279)	√	X	OID 1.2.840.113549.1.1.1 RSAEncryption Clave pública de 4096 bits (RFC3279)
4.11 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	

5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.1.X.Y	√	-	1.3.6.1.4.1.49959.1. 1.1.1.1 Persona Natural Software 1.3.6.1.4.1.49959.1. 1.1.2.1 Persona Natural Hardware 1.3.6.1.4.1.49959.1. 1.1.3.1 Persona Natural Lleida.net Wallet 1.3.6.1.4.1.49959.1. 1.1.3.2 Persona Natural Centralizado UP 1.3.6.1.4.1.49959.1. 1.1.3.3 Persona Natural Centralizado Huella dactilar
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	
5.1.4.3 Policy Identifier [2]	0.4.0.194112.1.X	√	-	0.4.0.194112.1.0 (qcp-natural) Persona Natural Software 0.4.0.194112.1.2

				(qcp-natural-qscd) Persona Natural Hardware 0.4.0.194112.1.2 (qcp-natural-qscd) Persona Natural Lleida.net Wallet 0.4.0.194112.1.2 (qcp-natural-qscd) Persona Natural Centralizado UP 0.4.0.194112.1.2 (qcp-natural-qscd) Persona Natural Centralizado Huella dactilar
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	X	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	OID 2.5.29.37
5.1.11.1 serverAuth	0	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	1	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	0	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	1	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	0	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	0	-	-	OID 1.3.6.1.5.5.7.3.9

5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	1	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	1	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl1.esigna.es/sub/indenov a_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl.esigna.es/sub/indenova_ pki_003.crl	√	-	
5.1.13 qcStatements		-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi- qcs-QcCompliance	1	√	-	
5.1.13.2 id-etsi- qcs-QcLimitValue	0	-	-	
5.1.13.3 id-etsi- qcs- QcRetentionPeriod	15	-	-	
5.1.13.4 id-etsi- qcs-QcSSCD	1	-	-	Únicamente aplica a los siguientes perfiles: 1.3.6.1.4.1.49959.1. 1.1.2.1 Persona Natural Hardware 1.3.6.1.4.1.49959.1. 1.1.3.1 Persona Natural Lleida.net Wallet 1.3.6.1.4.1.49959.1. 1.1.3.2 Persona Natural Centralizado UP 1.3.6.1.4.1.49959.1. 1.1.3.3 Persona Natural

				Centralizado Huella dactilar
5.1.13.5 id-etsi-qcs-QcPDS	[[https://pki.esigna.es/pds/EN_v1.0.pdf, en]]	√	-	
5.1.13.6 id-etsi-qcs-QcType	[0.4.0.1862.1.6.1]	√	-	id-etsi-qct-esign
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	√	-	
5.2.1.2 accessLocation	URI:http://ocsp2.esigna.es	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	
5.2.2.2 accessLocation	URL=http://certs.esigna.es/ca/indenova_pki_003.crt	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint		√	X	Establecido por la plataforma PKI al momento de generar el certificado

6.2 PERTENENCIA A EMPRESA

Campo	Contenido	Ob lig ati ori o	C rí ti c o	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	RFC 5280
1.2 Serial number		√	X	Establecido por la plataforma PKI al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	OID 2.5.4.13
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	OID 2.5.4.3
2.3 Organization (O)	inDenova SL	√	-	OID 2.5.4.10
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	OID 2.5.4.97
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	OID 2.5.4.5
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	OID 2.5.4.11
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	OID 2.5.4.12
2.8 Locality (L)	VALENCIA	√	X	OID 2.5.4.7
2.9 Country (C)	ES	√	-	OID 2.5.4.6
3 Validity				
3.1 notBefore		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)

3.2 notAfter		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
4 Subject				
4.1 Description (Description)	Pertenencia a Empresa - Emitido por inDenova SUB CA 003	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Documento identificativo, nombre y apellidos del suscriptor y documento identificativo de la organización	√	-	OID 2.5.4.3 (DOCUMENTO IDENTIFICATIVO SUSCRIPUTOR) NOMBRE APELLIDOS (DOCUMENTO IDENTIFICATIVO ORGANIZACIÓN)
4.3 Serial Number (SERIALNUMBER)	Documento identificativo del responsable, según la norma técnica ETSI EN 319 412-1 (IDCES + NIF del responsable)	√	-	OID 2.5.4.5
4.4 Organization Identifier (2.5.4.97)	Identificador de la organización distinto del nombre, según la norma técnica ETSI EN 319 412-1 (VATES + CIF de la entidad)	√	-	OID 2.5.4.97
4.5 Email Address (E)	Dirección de correo electrónico del suscriptor	√	-	Dirección de correo electrónico del suscriptor
4.6 Locality (L)	Distrito de la organización	√	-	OID 2.5.4.7 Distrito de la organización
4.7 Country (C)	País de la organización	√	-	OID 2.5.4.6 País de la organización. Código de país codificado de acuerdo al ISO 3166-1 alpha-2
4.8 StateOrProvinceName (S)	Provincia de la organización	√	-	OID 2.5.4.8 Provincia de la organización
4.9 Organization (O)	Nombre de la organización	√	-	OID 2.5.4.10 Nombre de la organización
4.10 Given Name (G)	Nombre suscriptor	√	-	OID 2.5.4.42 NOMBRE
4.11 Surname (SN)	Apellidos suscriptor	√	-	OID 2.5.4.4 APELLIDOS
4.12 Title (T)	Cargo o función del suscriptor en la organización	√	-	OID 2.5.4.12 Cargo o función del suscriptor en la organización
4.13 Organizational Unit (OU)	Área o dependencia de la organización	√	-	OID 2.5.4.11 Área o dependencia de la organización
4.14 Subject Public Key Info	RSAEncryption Clave pública de 4096 bits (RFC3279)	√	X	OID 1.2.840.113549.1.1.1 RSAEncryption Clave pública de 4096 bits (RFC3279)

4.15 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	

5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.2.X.Y	√	-	1.3.6.1.4.1.49959.1.1.2.1.1 Pertenencia a Empresa Software 1.3.6.1.4.1.49959.1.1.2.2.1 Pertenencia a Empresa Hardware 1.3.6.1.4.1.49959.1.1.2.3.1 Pertenencia a Empresa Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.2.3.2 Pertenencia a Empresa Centralizado UP 1.3.6.1.4.1.49959.1.1.2.3.3 Pertenencia a Empresa Centralizado Huella dactilar
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	
5.1.4.3 Policy Identifier [2]	0.4.0.194112.1.X	√	-	0.4.0.194112.1.0 (qcp-natural) Pertenencia a Empresa Software 0.4.0.194112.1.2 (qcp-natural-qscd) Pertenencia a Empresa Hardware 0.4.0.194112.1.2 (qcp-natural-qscd) Pertenencia a Empresa Lleida.net Wallet 0.4.0.194112.1.2 (qcp-natural-qscd) Pertenencia a Empresa Centralizado UP 0.4.0.194112.1.2 (qcp-natural-qscd) Pertenencia a Empresa Centralizado Huella dactilar
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	

5.1.8.2 pathLenConstraint	Ninguno	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	OID 2.5.29.37
5.1.11.1 serverAuth	0	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	1	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	0	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	1	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	0	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	0	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	1	-	-	OID 1.3.6.1.4.1.311.20.2.2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	OID 1.3.6.1.4.1.311.2.1.22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	1	-	-	OID 1.3.6.1.4.1.311.10.3.4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31

5.1.12.1 CRL Distribution Point 1	URL=http://crl1.esigna.es/sub/indexnova_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl.esigna.es/sub/indexnova_pki_003.crl	√	-	
5.1.13 qcStatements		-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs- QcCompliance	1	√	-	
5.1.13.2 id-etsi-qcs- QcLimitValue	0	-	-	
5.1.13.3 id-etsi-qcs- QcRetentionPe riod	15	-	-	
5.1.13.4 id-etsi-qcs- QcSSCD	1	-	-	Únicamente aplica a los siguientes perfiles: 1.3.6.1.4.1.49959.1.1.2.2.1 Pertenencia a Empresa Hardware 1.3.6.1.4.1.49959.1.1.2.3.1 Pertenencia a Empresa Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.2.3.2 Pertenencia a Empresa Centralizado UP 1.3.6.1.4.1.49959.1.1.2.3.3 Pertenencia a Empresa Centralizado Huella dactilar
5.1.13.5 id-etsi-qcs- QcPDS	[[https://pki.esigna.es/pds/EN_v1.0.pdf,en]]	√	-	
5.1.13.6 id-etsi-qcs- QcType	[0.4.0.1862.1.6.1]	√	-	id-etsi-qct-esign
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	

5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	√	-	
5.2.1.2 accessLocation	URI:http://ocsp2.esigna.es	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	
5.2.2.2 accessLocation	URL=http://certs.esigna.es/ca/ind enova_pki_003.crt	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint		√	X	Establecido por la plataforma PKI al momento de generar el certificado

6.3 REPRESENTANTE LEGAL

Campo	Contenido	Obligato rio	Críti co	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	RFC 5280
1.2 Serial number		√	X	Establecido por la plataforma PKI al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	OID 2.5.4.13
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	OID 2.5.4.3
2.3 Organization (O)	inDenova SL	√	-	OID 2.5.4.10
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	OID 2.5.4.97
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	OID 2.5.4.5
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	OID 2.5.4.11
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	OID 2.5.4.12
2.8 Locality (L)	VALENCIA	√	X	OID 2.5.4.7
2.9 Country (C)	ES	√	-	OID 2.5.4.6
3 Validity				
3.1 notBefore		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
3.2 notAfter		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)

4 Subject				
4.1 Description (Description)	<p>Codificación del documento público que acredita las facultades del firmante o los datos registrales. Se presentan varias opciones, según si se ha consultado el Registro Mercantil o un Poder Notarial, u otro tipo de registro o documento oficial.</p> <ul style="list-style-type: none"> • En el Registro Mercantil: Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX • Poder Notarial: Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa • En el caso de que las facultades vengán indicadas en Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX 	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Documento identificativo de la organización y organización	√	-	OID 2.5.4.3 (DOCUMENTO IDENTIFICATIVO ORGANIZACIÓN) ORGANIZACIÓN DOCUMENTO IDENTIFICATIVO SUScriptor NOMBRE APELLIDOS
4.3 Serial Number (SERIALNUMBER)	Documento identificativo del responsable, según la norma técnica ETSI EN 319 412-1 (IDCES + NIF del responsable)	√	-	OID 2.5.4.5
4.4 Organization Identifier (2.5.4.97)	Identificador de la organización distinto del nombre, según la norma técnica ETSI EN 319 412-1 (VATES + CIF de la entidad)	√		OID 2.5.4.97
4.5 Email Address (E)	Dirección de correo electrónico de la organización	√	-	Dirección de correo electrónico de la organización

4.6 Locality (L)	Distrito de la organización	√	-	OID 2.5.4.7 Distrito de la organización
4.7 Country (C)	País de la organización	√	-	OID 2.5.4.6 País de la organización. Código de país codificado de acuerdo al ISO 3166-1 alpha-2
4.8 StateOrProvinceName (S)	Provincia de la organización	√	-	OID 2.5.4.8 Provincia de la organización
4.9 Organization (O)	Nombre de la organización	√	-	OID 2.5.4.10 Nombre de la organización
4.10 Given Name (G)	Nombre responsable	√	-	OID 2.5.4.42 NOMBRE
4.11 Surname (SN)	Apellidos responsable	√	-	OID 2.5.4.4 APELLIDOS
4.12 Title (T)	Cargo o función del responsable en la organización	√	-	OID 2.5.4.12 Cargo o función del responsable en la organización
4.13 Organizational Unit (OU)	Área o dependencia del responsable en la organización	√	-	OID 2.5.4.11 Área o dependencia del responsable en la organización
4.14 Subject Public Key Info	RSAEncryption Clave pública de 4096 bits (RFC3279)	√	X	OID 1.2.840.113549.1.1.1 RSAEncryption Clave pública de 4096 bits (RFC3279)
4.15 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	

5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.3.X.Y	√	-	1.3.6.1.4.1.49959.1.1.3.1.1 Persona Natural Representante Legal Software 1.3.6.1.4.1.49959.1.1.3.2.1 Persona Natural Representante Legal Hardware 1.3.6.1.4.1.49959.1.1.3.3.1 Persona Natural Representante Legal Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.3.3.2 Persona Natural Representante Legal Centralizado UP

				1.3.6.1.4.1.49959.1. 1.3.3.3 Persona Natural Representante Legal Centralizado Huella dactilar
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	
5.1.4.3 Policy Identifier [2]	0.4.0.194112.1.X	√	-	0.4.0.194112.1.0 (qcp-natural) Persona Natural Representante Legal Software 0.4.0.194112.1.2 (qcp-natural-qscd) Persona Natural Representante Legal Hardware 0.4.0.194112.1.2 (qcp-natural-qscd) Persona Natural Representante Legal Lleida.net Wallet 0.4.0.194112.1.2 (qcp-natural-qscd) Persona Natural Representante Legal Centralizado UP 0.4.0.194112.1.2 (qcp-natural-qscd) Persona Natural Representante Legal Centralizado Huella dactilar
5.1.4.4 Policy Identifier [3]	2.16.724.1.3.5.8	√	-	OID de persona física representante de persona jurídica

				según Secretaría SGIADSC
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	OID 2.5.29.37
5.1.11.1 serverAuth	0	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	1	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	0	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	1	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	0	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	0	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	1	-	-	OID 1.3.6.1.4.1.311.20.2.2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	OID 1.3.6.1.4.1.311.2.1.22
5.1.11.9 Microsoft Encrypting	1	-	-	OID 1.3.6.1.4.1.311.10.3.4

File System 1.3.6.2.1.31136.10.3.4				
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl1.esigna.es/sub/indenova_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl.esigna.es/sub/indenova_pki_003.crl	√	-	
5.1.13 qcStatements		√	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	1	√	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	0	-	-	
5.1.13.3 id-etsi-qcs-QcRetentionPeriod	15	-	-	
5.1.13.4 id-etsi-qcs-QcSSCD	1	-	-	Únicamente aplica a los siguientes perfiles: 1.3.6.1.4.1.49959.1.1.1.2.1 Persona Natural Representante Legal Hardware 1.3.6.1.4.1.49959.1.1.1.3.1 Persona Natural Representante Legal Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.1.3.2 Persona Natural Representante Legal Centralizado UP 1.3.6.1.4.1.49959.1.1.1.3.3 Persona Natural Representante Legal Centralizado Huella dactilar
5.1.13.5 id-etsi-qcs-QcPDS	[[https://pki.esigna.es/pds/EN_v1.0.pdf, en]]	√	-	

5.1.13.6 id-etsi-qcs-QcType	[0.4.0.1862.1.6.1]	√	-	id-etsi-qct-esign
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	√	-	
5.2.1.2 accessLocation	URI:http://ocsp2.esigna.es	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	
5.2.2.2 accessLocation	URL=http://certs.esigna.es/ca/indenova_pki_003.crt	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint		√	X	Establecido por la plataforma PKI al momento de generar el certificado

6.4 SELLO ELECTRÓNICO

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	RFC 5280
1.2 Serial number		√	X	Establecido por la plataforma PKI al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	OID 2.5.4.13
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	OID 2.5.4.3
2.3 Organization (O)	inDenova SL	√	-	OID 2.5.4.10
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	OID 2.5.4.97
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	OID 2.5.4.5
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	OID 2.5.4.11
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	OID 2.5.4.12
2.8 Locality (L)	VALENCIA	√	X	OID 2.5.4.7
2.9 Country (C)	ES	√	-	OID 2.5.4.6
3 Validity				
3.1 notBefore		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
3.2 notAfter		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
4 Subject				

4.1 Description (Description)	Certificado de Sello Electrónico - Emitido por inDenova SUB CA 003	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Documento identificativo de la organización y organización	√	-	OID 2.5.4.3 (DOCUMENTO IDENTIFICATIVO ORGANIZACIÓN) ORGANIZACIÓN
4.3 Serial Number (SERIALNUMBER)	Documento identificativo del responsable, según la norma técnica ETSI EN 319 412-1 (IDCES + NIF del responsable)	√	-	OID 2.5.4.5
4.4 Organization Identifier (2.5.4.97)	Identificador de la organización distinto del nombre, según la norma técnica ETSI EN 319 412-1 (VATES + CIF de la entidad)	√		OID 2.5.4.97
4.5 Email Address (E)	Dirección de correo electrónico de la organización	√	-	Dirección de correo electrónico de la organización
4.6 Locality (L)	Distrito de la organización	√	-	OID 2.5.4.7 Distrito de la organización
4.7 Country (C)	País de la organización	√	-	OID 2.5.4.6 País de la organización. Código de país codificado de acuerdo al ISO 3166-1 alpha-2
4.8 StateOrProvinceName (S)	Provincia de la organización	√	-	OID 2.5.4.8 Provincia de la organización
4.9 Organization (O)	Nombre de la organización	√	-	OID 2.5.4.10 Nombre de la organización
4.10 Given Name (G)	Nombre responsable	√	-	OID 2.5.4.42 NOMBRE
4.11 Surname (SN)	Apellidos responsable	√	-	OID 2.5.4.4 APELLIDOS
4.12 Title (T)	Cargo o función del responsable en la organización	√	-	OID 2.5.4.12 Cargo o función del responsable en la organización
4.13 Organizational Unit (OU)	SELLO ELECTRÓNICO	√	-	Indica la naturaleza del certificado
4.14 Subject Public Key Info	RSAEncryption Clave pública de 4096 bits (RFC3279)	√	X	OID 1.2.840.113549.1.1.1 RSAEncryption Clave pública de 4096 bits (RFC3279)
4.15 Public key parameters	05 00	√	X	

5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerial Number		X	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	1	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.3.X.Y	√	-	1.3.6.1.4.1.49959.1.1.3.4.1 Certificado de Sello Electrónico Software 1.3.6.1.4.1.49959.1.1.3.4.2 Certificado Sello Electrónico Hardware 1.3.6.1.4.1.49959.1.1.3.4.3 Certificado Sello

				Electrónico Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.3.4.4 Certificado Sello Electrónico Centralizado UP
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	- Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio/alto. Consulte las condiciones de uso en http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	- Nivel medio: Software - Nivel alto: Hardware, centralizado, Lleida.net Wallet
5.1.4.3 Policy Identifier [2]	0.4.0.194112.1.X	√	-	0.4.0.194112.1.1 (qcp-legal) Certificado de Sello Electrónico Software 0.4.0.194112.1.3
5.1.4.4 Policy Identifier [3]	0.4.0.194112.1.X	√	-	OID 2.16.724.1.3.5.6.1 (OID de la política de certificado de sello de nivel alto) --> en los que no son de tipo software OID 0.4.0.194112.1.3 Certificado Sello Electrónico Hardware OID 0.4.0.194112.1.3 Certificado Sello Electrónico Lleida.net Wallet OID 0.4.0.194112.1.3 Certificado Sello Electrónico Centralizado UP
5.1.5 Subject Alternative Name	Nombre RFC822=(correo electrónico) Dirección del directorio: OID.2.16.724.1.3.5.6.1.9= (Opcional. Correo electrónico)	√	-	

	OID.2.16.724.1.3.5.6.1.8=Apellido2 (Opcional) OID.2.16.724.1.3.5.6.1.7=Apellido1 (Opcional) OID.2.16.724.1.3.5.6.1.6=Nombre (Opcional) OID.2.16.724.1.3.5.6.1.5= (Opcional. Breve descripción de la componente que posee el certificado de sello) OID.2.16.724.1.3.5.6.1.4=99999999R (Opcional. DNI o NIE del responsable) OID.2.16.724.1.3.5.6.1.3=A99999999 (Número único de identificación de la entidad) OID.2.16.724.1.3.5.6.1.2=Nombre de la Administración OID.2.16.724.1.3.5.6.1.1="SELLO ELECTRONICO"			
5.1.6 Issuer Alternative Name	No está presente	X	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	OID 2.5.29.37
5.1.11.1 serverAuth	0	-	-	OID 1.3.6.1.5.5.7.3.1

5.1.11.2 clientAuth	1	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	0	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	1	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	0	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	0	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	1	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3. 4	1	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.esigna.es/sub/inden ova_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl.esigna.es/sub/inden ova_pki_003.crl	√	-	
5.1.13 qcStatements		-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id- etsi-qcs- QcCompliance	1	√	-	
5.1.13.2 id- etsi-qcs- QcLimitValue	0	-	-	
5.1.13.3 id- etsi-qcs- QcRetentionPeriod	15	-	-	
5.1.13.4 id- etsi-qcs-QcSSCD	0	-	-	

5.1.13.5 id-etsi-qcs-QcPDS	[[https://pki.esigna.es/pds/EN_v1.0.pdf,en]]	√	-	
5.1.13.6 id-etsi-qcs-QcType	[0.4.0.1862.1.6.2]	√	-	id-etsi-qct-eseal
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	√	-	
5.2.1.2 accessLocation	URI:http://ocsp2.esigna.es	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	
5.2.2.2 accessLocation	URL=http://certs.esigna.es/ca/indena_ova_pki_003.crt	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint		√	X	Establecido por la plataforma PKI al momento de generar el certificado

6.5 EMPLEADO PÚBLICO

Campo	Contenido	Obligato rio	Críti co	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	RFC 5280
1.2 Serial number		√	X	Establecido por la plataforma PKI al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	OID 2.5.4.13
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	OID 2.5.4.3
2.3 Organization (O)	inDenova SL	√	-	OID 2.5.4.10
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	OID 2.5.4.97
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	OID 2.5.4.5
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	OID 2.5.4.11
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	OID 2.5.4.12
2.8 Locality (L)	VALENCIA	√	X	OID 2.5.4.7
2.9 Country (C)	ES	√	-	OID 2.5.4.6
3 Validity				
3.1 notBefore		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
3.2 notAfter		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)

4 Subject				
4.1 Description (Description)	Empleado Público - Emitido por inDenova SUB CA 003	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Documento identificativo, nombre y apellidos del suscriptor y documento identificativo de la organización	√	-	OID 2.5.4.3 (DOCUMENTO IDENTIFICATIVO SUScriptor) NOMBRE APELLIDOS (DOCUMENTO IDENTIFICATIVO ORGANIZACIÓN)
4.3 Serial Number (SERIALNUMBER)	Documento identificativo del responsable, según la norma técnica ETSI EN 319 412-1 (IDCES + NIF del responsable)	√	-	OID 2.5.4.5
4.4 Organization Identifier (2.5.4.97)	Identificador de la organización distinto del nombre, según la norma técnica ETSI EN 319 412-1 (VATES + CIF de la entidad)	√	-	OID 2.5.4.97
4.5 Email Address (E)	Dirección de correo electrónico del suscriptor	√	-	Dirección de correo electrónico del suscriptor
4.6 Locality (L)	Distrito de la organización	√	-	OID 2.5.4.7 Distrito de la organización
4.7 Country (C)	País de la organización	√	-	OID 2.5.4.6 País de la organización. Código de país codificado de acuerdo al ISO 3166-1 alpha-2
4.8 StateOrProvinceName (S)	Provincia de la organización	√	-	OID 2.5.4.8 Provincia de la organización
4.9 Organization (O)	Nombre de la organización	√	-	OID 2.5.4.10 Nombre de la organización
4.10 Given Name (G)	Nombre suscriptor	√	-	OID 2.5.4.42 NOMBRE
4.11 Surname (SN)	Apellidos suscriptor	√	-	OID 2.5.4.4 APELLIDOS
4.12 Title (T)	Cargo o función del suscriptor en la organización	√	-	OID 2.5.4.12 Cargo o función del suscriptor en la organización

4.13 Organizational Unit (OU)	Área o dependencia de la organización	√	-	OID 2.5.4.11 Área o dependencia de la organización
4.14 Subject Public Key Info	RSAEncryption Clave pública de 4096 bits (RFC3279)	√	X	OID 1.2.840.113549.1.1.1 RSAEncryption Clave pública de 4096 bits (RFC3279)
4.15 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32

5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.2.X.Y	√	-	1.3.6.1.4.1.49959.1.1.3.5.1 Empleado Público Software 1.3.6.1.4.1.49959.1.1.3.5.2 Empleado Público Hardware 1.3.6.1.4.1.49959.1.1.3.5.3 Empleado Público Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.3.5.4 Empleado Público Centralizado UP 1.3.6.1.4.1.49959.1.1.3.5.5 Empleado Público Centralizado Huella dactilar
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	
5.1.4.3 Policy Identifier [2]	0.4.0.194112.1.X	√	-	0.4.0.194112.1.0 Empleado Público Software 0.4.0.194112.1.2 Empleado Público Hardware 0.4.0.194112.1.2 Empleado Público Lleida.net Wallet 0.4.0.194112.1.2 Empleado Público Centralizado UP 0.4.0.194112.1.2 Empleado Público Centralizado Huella dactilar

5.1.4.4 Policy Identifier [3]	2.16.724.1.3.5.7.X	√	-	2.16.724.1.3.5.7.2 Empleado Público Software 2.16.724.1.3.5.7.1 Empleado Público Hardware 2.16.724.1.3.5.7.1 Empleado Público Lleida.net Wallet 2.16.724.1.3.5.7.1 Empleado Público Centralizado UP 2.16.724.1.3.5.7.1 Empleado Público Centralizado Huella dactilar
5.1.5 Subject Alternative Name	Nombre RFC822= (correo electrónico del titular) Dirección del directorio: OID.2.16.724.1.3.5.7.1.11=CARGO (Opcional) OID.2.16.724.1.3.5.7.1.10=DEPARTAMENTO (Opcional) OID.2.16.724.1.3.5.7.1.9= (Correo electrónico del firmante - opcional) OID.2.16.724.1.3.5.7.1.8=APELLIDO2 OID.2.16.724.1.3.5.7.1.7=APELLIDO1 OID.2.16.724.1.3.5.7.1.6=NOMBRE OID.2.16.724.1.3.5.7.1.5=11111111 (corresponde con el NRP o NIP - Opcional) OID.2.16.724.1.3.5.7.1.4=99999999R (DNI o NIE del responsable)	√	-	

	OID.2.16.724.1.3.5.7.1.3=A99999999 (Número único de identificación de la entidad) OID.2.16.724.1.3.5.7.1.2=NOMBRE DE LA ORGANIZACIÓN OID.2.16.724.1.3.5.7.1.1="CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO"			
5.1.6 Issuer Alternative Name	No está presente	X	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	OID 2.5.29.37
5.1.11.1 serverAuth	0	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	1	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	0	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	1	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	0	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	0	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	1	-	-	OID 1.3.6.1.4.1.311.20.2.2
5.1.11.8 Microsoft Commercial Code	0	-	-	OID 1.3.6.1.4.1.311.2.1.22

Signing 1.3.6.2.1.311.2.1.22				
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	1	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl1.esigna.es/sub/indenova_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl.esigna.es/sub/indenova_pki_003.crl	√	-	
5.1.13 qcStatements		-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	1	√	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	0	-	-	
5.1.13.3 id-etsi-qcs-QcRetentionPeriod	15	-	-	
5.1.13.4 id-etsi-qcs-QcSSCD	1	-	-	Únicamente aplica a los siguientes perfiles: 1.3.6.1.4.1.49959.1.1.3.5.2 Empleado Público Hardware 1.3.6.1.4.1.49959.1.1.3.5.3 Empleado Público Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.3.5.4 Empleado Público Centralizado UP 1.3.6.1.4.1.49959.1.1.3.5.5 Empleado Público Centralizado Huella dactilar
5.1.13.5 id-etsi-qcs-QcPDS	[[https://pki.esigna.es/pds/EN_v1.0.pdf, en]]	√	-	
5.1.13.6 id-etsi-qcs-QcType	[0.4.0.1862.1.6.1]	√	-	id-etsi-qct-esign
5.1.14 Netscape Cert Type	No está presente	√	-	

5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	√	-	
5.2.1.2 accessLocation	URI:http://ocsp2.esigna.es	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	
5.2.2.2 accessLocation	URL=http://certs.esigna.es/ca/indenova_pki_003.crt	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint		√	X	Establecido por la plataforma PKI al momento de generar el certificado

6.6 REPRESENTANTE LEGAL SIN PERSONALIDAD JURÍDICA

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	RFC 5280
1.2 Serial number		√	X	Establecido por la plataforma PKI al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	OID 2.5.4.13
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	OID 2.5.4.3
2.3 Organization (O)	inDenova SL	√	-	OID 2.5.4.10
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	OID 2.5.4.97
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	OID 2.5.4.5
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	OID 2.5.4.11
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	OID 2.5.4.12
2.8 Locality (L)	VALENCIA	√	X	OID 2.5.4.7
2.9 Country (C)	ES	√	-	OID 2.5.4.6
3 Validity				
3.1 notBefore		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
3.2 notAfter		√	X	Establecido por la plataforma PKI al momento de

				generar el certificado (UTC-5)
4 Subject				
4.1 Description (Description)	<p>Codificación del documento público que acredita las facultades del firmante o los datos registrales. Se presentan varias opciones, según si se ha consultado el Registro Mercantil o un Poder Notarial, u otro tipo de registro o documento oficial.</p> <ul style="list-style-type: none"> • En el Registro Mercantil: Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX • Poder Notarial: Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa • En el caso de que las facultades vengan indicadas en Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX 	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Documento identificativo de la organización y organización	√	-	OID 2.5.4.3 (DOCUMENTO IDENTIFICATIVO ORGANIZACIÓN) ORGANIZACIÓN DOCUMENTO IDENTIFICATIVO SUScriptor NOMBRE APELLIDOS
4.3 Serial Number (SERIALNUMBER)	Documento identificativo del responsable, según la norma técnica ETSI EN 319 412-1 (IDCES + NIF del responsable)	√	-	OID 2.5.4.5
4.4 Organization Identifier (2.5.4.97)	Identificador de la organización distinto del nombre, según la norma técnica ETSI EN 319 412-1 (VATES + CIF de la entidad)	√		OID 2.5.4.97

4.5 Email Address (E)	Dirección de correo electrónico de la organización	√	-	Dirección de correo electrónico de la organización
4.6 Locality (L)	Distrito de la organización	√	-	OID 2.5.4.7 Distrito de la organización
4.7 Country (C)	País de la organización	√	-	OID 2.5.4.6 País de la organización. Código de país codificado de acuerdo al ISO 3166-1 alpha-2
4.8 StateOrProvinceName (S)	Provincia de la organización	√	-	OID 2.5.4.8 Provincia de la organización
4.9 Organization (O)	Nombre de la organización	√	-	OID 2.5.4.10 Nombre de la organización
4.10 Given Name (G)	Nombre responsable	√	-	OID 2.5.4.42 NOMBRE
4.11 Surname (SN)	Apellidos responsable	√	-	OID 2.5.4.4 APELLIDOS
4.12 Title (T)	Cargo o función del responsable en la organización	√	-	OID 2.5.4.12 Cargo o función del responsable en la organización
4.13 Organizational Unit (OU)	Área o dependencia del responsable en la organización	√	-	OID 2.5.4.11 Área o dependencia del responsable en la organización
4.14 Subject Public Key Info	RSAEncryption Clave pública de 4096 bits (RFC3279)	√	X	OID 1.2.840.113549.1.1.1 RSAEncryption Clave pública de 4096 bits (RFC3279)
4.15 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6b29806c46	√	-	
5.1.1.2 authorityCertIssuer		X	-	

5.1.1.3 authorityCertSerialNumber		X	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.3.X.Y	√	-	1.3.6.1.4.1.49959.1.1.3.6.1 Representante Legal Sin Personalidad Jurídica Software 1.3.6.1.4.1.49959.1.1.3.6.2 Representante Legal Sin Personalidad Jurídica Hardware 1.3.6.1.4.1.49959.1.1.3.6.3 Representante Legal Sin Personalidad Jurídica Lleida.net Wallet

				1.3.6.1.4.1.49959.1. 1.3.6.4 Representante Legal Sin Personalidad Jurídica Centralizado UP 1.3.6.1.4.1.49959.1. 1.3.6.5 Representante Legal Sin Personalidad Jurídica Centralizado Huella dactilar
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	
5.1.4.3 Policy Identifier [2]	0.4.0.194112.1.X	√	-	0.4.0.194112.1.0 Representante Legal Sin Personalidad Jurídica Software 0.4.0.194112.1.2 Representante Legal Sin Personalidad Jurídica Hardware 0.4.0.194112.1.2 Representante Legal Sin Personalidad Jurídica Lleida.net Wallet 0.4.0.194112.1.2 Representante Legal Sin Personalidad Jurídica Centralizado UP 0.4.0.194112.1.2

				Representante Legal Sin Personalidad Jurídica Centralizado Huella dactilar
5.1.4.4 Policy Identifier [3]	2.16.724.1.3.5.9	√	-	OID de persona física representante de entidad sin personalidad jurídica según Secretaría SGIADSC
5.1.5 Subject Alternative Name	No está presente	X	X	
5.1.6 Issuer Alternative Name	No está presente	X	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	OID 2.5.29.37
5.1.11.1 serverAuth	0	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	1	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	0	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	1	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	0	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	0	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card	1	-	-	OID 1.3.6.1.4.1.311.20.2.2

Logon for Windows 1.3.6.2.1.311.20.2.2				
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	1	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl1.esigna.es/sub/indenov a_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl.esigna.es/sub/indenova_ pki_003.crl	√	-	
5.1.13 qcStatements		√	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi- qcs-QcCompliance	1	√	-	
5.1.13.2 id-etsi- qcs-QcLimitValue	0	-	-	
5.1.13.3 id-etsi- qcs- QcRetentionPeriod	15	-	-	
5.1.13.4 id-etsi- qcs-QcSSCD	1	-	-	Únicamente aplica a los siguientes perfiles: 1.3.6.1.4.1.49959.1. 1.3.2.1 Representante Legal Sin Personalidad Jurídica Hardware 1.3.6.1.4.1.49959.1. 1.3.3.1 Representante Legal Sin Personalidad Jurídica Lleida.net Wallet 1.3.6.1.4.1.49959.1. 1.3.3.2 Representante Legal Sin

				Personalidad Jurídica Centralizado UP 1.3.6.1.4.1.49959.1.1.3.3.3 Representante Legal Sin Personalidad Jurídica Centralizado Huella dactilar
5.1.13.5 id-etsi-qcs-QcPDS	[[https://pki.esigna.es/pds/EN_v1.0.pdf, en]]	√	-	
5.1.13.6 id-etsi-qcs-QcType	[0.4.0.1862.1.6.1]	√	-	id-etsi-qct-esign
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	√	-	
5.2.1.2 accessLocation	URI:http://ocsp2.esigna.es	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	
5.2.2.2 accessLocation	URL=http://certs.esigna.es/ca/indenova_pki_003.crt	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	

7.2 Thumbprint		√	X	Establecido por la plataforma PKI al momento de generar el certificado
-----------------------	--	---	---	--

6.7 EMPLEADO PÚBLICO CON SEUDÓNIMO

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	RFC 5280
1.2 Serial number		√	X	Establecido por la plataforma PKI al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Description (Description)	inDenova Subordinate CA 003	√	X	OID 2.5.4.13
2.2 Common Name (CN)	inDenova SUB CA 003	√	-	OID 2.5.4.3
2.3 Organization (O)	inDenova SL	√	-	OID 2.5.4.10
2.4 Organization Identifier (2.5.4.97)	VATES-B97458996	√	-	OID 2.5.4.97
2.5 Serial Number (SERIALNUMBER)	B97458996	√	-	OID 2.5.4.5
2.6 Organizational Unit (OU)	Certification Authority inDenova SL	√	-	OID 2.5.4.11
2.7 Title (T)	Subordinate Certificate Authority inDenova SL	√	-	OID 2.5.4.12
2.8 Locality (L)	VALENCIA	√	X	OID 2.5.4.7
2.9 Country (C)	ES	√	-	OID 2.5.4.6
3 Validity				
3.1 notBefore		√	X	Establecido por la plataforma PKI al momento de generar el certificado (UTC-5)
3.2 notAfter		√	X	Establecido por la plataforma PKI al momento de

				generar el certificado (UTC-5)
4 Subject				
4.1 Description (Description)	Empleado Público con Seudónimo - Emitido por inDenova SUB CA 003	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Puesto o Cargo o literal 'SEUDONIMO' - Seudónimo (Numero identificación personal distinto al DNI) - Nombre oficial de la organización	√	-	OID 2.5.4.3
4.3 Organization Identifier (2.5.4.97)	Identificador de la organización distinto del nombre, según la norma técnica ETSI EN 319 412-1 (VATES + CIF de la entidad)	√		OID 2.5.4.97
4.4 Email Address (E)	Dirección de correo electrónico del suscriptor	√	-	Dirección de correo electrónico del suscriptor
4.5 Country (C)	País de la organización	√	-	OID 2.5.4.6 País de la organización. Código de país codificado de acuerdo al ISO 3166-1 alpha-2
4.6 Organization (O)	Nombre de la organización	√	-	OID 2.5.4.10 Nombre de la organización
4.7 Title (T)	Cargo o función del suscriptor en la organización	√	-	OID 2.5.4.12 Cargo o función del suscriptor en la organización
4.8 Organizational Unit (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO	√	-	OID 2.5.4.11
4.9 Organizational Unit (OU)	Área o dependencia de la organización	√	-	OID 2.5.4.11 Área o dependencia de la organización
4.10 Pseudonym	Seudónimo (Número de Identificación Personal distinto al DNI)	√	-	OID 2.5.4.65
4.11 Subject Public Key Info	RSAEncryption Clave pública de 4096 bits (RFC3279)	√	X	OID 1.2.840.113549.1.1.1

				RSAEncryption Clave pública de 4096 bits (RFC3279)
4.12 Public key parameters	05 00	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier	c39c745dd022a8edf2ee50beafad7b6 b29806c46	√	-	
5.1.1.2 authorityCertIssuer		X	-	
5.1.1.3 authorityCertSerial Number		X	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	1	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	1	X	-	
5.1.3.3 keyEncipherment	0	X	-	
5.1.3.4 dataEncipherment	0	X	-	
5.1.3.5 keyAgreement	0	X	-	
5.1.3.6 keyCertSign	0	√	-	
5.1.3.7 cRLSign	0	√	-	
5.1.3.8 encipherOnly	0	X	-	
5.1.3.9 decipherOnly	0	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32

5.1.4.1 Policy Identifier	1.3.6.1.4.1.49959.1.1.3.7.X	√	-	1.3.6.1.4.1.49959.1.1.3.7.1 Empleado Público con Seudónimo Software 1.3.6.1.4.1.49959.1.1.3.7.2 Empleado Público con Seudónimo Hardware 1.3.6.1.4.1.49959.1.1.3.7.3 Empleado Público con Seudónimo Lleida.net Wallet 1.3.6.1.4.1.49959.1.1.3.7.4 Empleado Público con Seudónimo Centralizado UP 1.3.6.1.4.1.49959.1.1.3.7.5 Empleado Público con Seudónimo Centralizado Huella dactilar
5.1.4.2 Policy Qualifier ID	CPS	√	-	
5.1.4.2.1 CPS Pointer	http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS http://cps.esigna.es/sub/cps_sub003_ca.pdf	√	-	
5.1.4.3 Policy Identifier [2]	0.4.0.194112.1.X	√	-	0.4.0.194112.1.0 Empleado Público con Seudónimo Software 0.4.0.194112.1.2 Empleado Público con Seudónimo Hardware 0.4.0.194112.1.2 Empleado Público con Seudónimo Lleida.net Wallet 0.4.0.194112.1.2

				Empleado Público con Seudónimo Centralizado UP 0.4.0.194112.1.2 Empleado Público con Seudónimo Centralizado Huella dactilar
5.1.4.4 Policy Identifier [3]	2.16.724.1.3.5.4.X	√	-	2.16.724.1.3.5.4.2 Empleado Público con Seudónimo Software 2.16.724.1.3.5.4.1 Empleado Público con Seudónimo Hardware 2.16.724.1.3.5.4.1 Empleado Público con Seudónimo Lleida.net Wallet 2.16.724.1.3.5.4.1 Empleado Público con Seudónimo Centralizado UP 2.16.724.1.3.5.4.1 Empleado Público con Seudónimo Centralizado Huella dactilar
5.1.5 Subject Alternative Name	<p>Nombre RFC822= (correo electrónico del titular)</p> <p>Dirección del directorio:</p> <p>OID.2.16.724.1.3.5.4.2.12 --> Obligatorio: Seudónimo (NIP)</p> <p>OID.2.16.724.1.3.5.3.2.11 --> Opcional: Puesto o cargo</p> <p>OID.2.16.724.1.3.5.3.2.10 --> Opcional: Unidad organizativa</p> <p>OID.2.16.724.1.3.5.3.2.9 --> Opcional: Correo electrónico de contacto</p>	√	√	

	<p>OID.2.16.724.1.3.5.3.2.3 --> Obligatorio: NIF entidad suscriptora</p> <p>OID.2.16.724.1.3.5.3.2.2 --> Obligatorio: Nombre de la entidad suscriptora</p> <p>OID.2.16.724.1.3.5.4.2.1=CERTIFICAD O ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO --> Obligatorio: Tipo de certificado</p>			
5.1.6 Issuer Alternative Name	No está presente	X	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	Ninguno	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage		X	X	OID 2.5.29.37
5.1.11.1 serverAuth	0	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	1	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	0	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	1	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	0	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	0	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	1	-	-	OID 1.3.6.1.4.1.311.20.2.2

5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	0	-	-	OID 1.3.6.1.4.1.311.2.1 .22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3. 4	1	-	-	OID 1.3.6.1.4.1.311.10. 3.4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl1.esigna.es/sub/indeno va_pki_003.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl.esigna.es/sub/indeno va_pki_003.crl	√	-	
5.1.13 qcStatements		-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id- etsi-qcs- QcCompliance	1	√	-	
5.1.13.2 id- etsi-qcs- QcLimitValue	0	-	-	
5.1.13.3 id- etsi-qcs- QcRetentionPeriod	15	-	-	
5.1.13.4 id- etsi-qcs-QcSSCD	1	-	-	Únicamente aplica a los siguientes perfiles: 1.3.6.1.4.1.49959. 1.1.3.7.2 Empleado Público con Seudónimo Hardware 1.3.6.1.4.1.49959. 1.1.3.7.3 Empleado Público con Seudónimo Lleida.net Wallet 1.3.6.1.4.1.49959. 1.1.3.7.4 Empleado Público con Seudónimo

				Centralizado UP 1.3.6.1.4.1.49959. 1.1.3.7.5 Empleado Público con Seudónimo Centralizado Huella dactilar
5.1.13.5 id-etsi-qcs-QcPDS	[[https://pki.esigna.es/pds/EN_v1.0.pdf,en]]	√	-	
5.1.13.6 id-etsi-qcs-QcType	[0.4.0.1862.1.6.1]	√	-	id-etsi-qct-esign
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	√	-	
5.2.1.2 accessLocation	URI:http://ocsp2.esigna.es	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	
5.2.2.2 accessLocation	URL=http://certs.esigna.es/ca/indenova_pki_003.crt	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	

7.2 Thumbprint		√	X	Establecido por la plataforma PKI al momento de generar el certificado
---------------------------	--	---	---	--