

Perfiles de Certificados de la Entidad de Certificación

Agencia Notarial de Certificación

Información general

Control documental

Proyecto:	Perfiles de Certificados de la Entidad de Certificación
Entidad de destino:	Agencia Notarial de Certificación, S.L.U.
Versión:	3.9
Estado:	Aprobado
Confidencialidad:	Público
Fecha de la edición:	06/02/2023
Fecha de aprobación:	20/04/2023
Fecha de publicación:	24/04/2023
Archivo:	Perfiles_Certificados_ANCERT_2023.docx
Formato:	Word 2019

Control de versiones

Versión	Partes que cambian	Descripción	Fecha cambio	Fecha publicación
2.0	Todo	Original	27/03/2010	
2.1	Todo	Revisión	26/04/2010	
2.2	Todo	Revisión	28/04/2010	
2.3	Certificado notarial de Servidor Seguro	Eliminación declaración como SSL EV	10/05/2010	
2.4	Certificado notarial Corporativo de Representación	Añadidos los atributos DateOfBirth y CountryOfCitizenship	11/05/2010	
2.5	Issuer de todos los perfiles	Corregido el Issuer para que incluya el campo L	27/05/2010	
2.6	Logo ANCERT	Nuevo logo de ANCERT	30/11/2010	01/01/2011
3.0	Certificados CGN de Cargo. Certificado de firma de código. Certificado corporativo de servidor seguro Restricciones de los certificados	Nueva clase de certificados. Añadido nuevo EKU. Nueva clase de certificados. Nota sobre el uso de sha2rsa como algoritmo de firma	30/01/2011	01/03/2011
3.1	Todos los perfiles Certificados de	Cambio del algoritmo de firma a sha256rsa. Añadida a la extensión AuthorityInformationAccess la URL de acceso al certificado de la CA emisora. Nombre del servidor obligatoriamente como dnsName en la extensión	16/03/2015	17/06/2015

	Servidor Seguro	SubjectAlternativeNames.		
3.2	Certificado Corporativo de Representación AGE	Nuevo perfil de certificado	04/05/2017	15/05/2017
3.3	Certificado FEREN de firma centralizada Certificado de servidor seguro Certificado de sellado de tiempo cualificado Certificado de OCSP Certificado personal corporativo y de corporaciones de derecho público	Nuevo perfil de certificado Periodo de validez de 825 días Nuevo perfil de certificado Nuevo perfil de certificado Certificados no cualificados	10/04/2018	25/05/2018
3.4	Certificado Notarial Corporativo de Representación AGE Certificado Notarial Corporativo de Sello Electrónico Certificado FEREN de firma centralizada Certificados para empleados Todos	Se elimina la extensión QCStatements del certificado de autenticación Nuevo perfil de certificado (con / sin QSCD). Nuevo perfil de certificado de firma centralizada (sin rQSCD) Nuevos perfiles de firma en software y de firma centralizada (con / sin rQSCD) Se elimina la secciones de cambios sobre el perfil V1.	22/01/2019	03/05/2019
3.5	Certificado Notarial Corporativo de Sello Electrónico Certificados FEREN de firma centraliza sin rQSCD Certificados para empleados software Certificados para empleados de firma centraliza sin rQSCD	Eliminación del keyUsage de "Data Encipherment" y añadido el de "Key Agreement"	14/06/2019	30/06/2019
3.6	Certificado de responder OCSP Certificado de Autoridad de Sellado de Tiempo Cualificada.		16/12/2019	06/04/2020
3.7	Certificado para empleados software Todos los perfiles	Revisión de campos opcionales en el SubjectDN. Revisión de longitud de nombres	14/12/2020	08/04/2021

		Actualización de referencias		
3.8	Certificado de servidor seguro	Periodo de validez de 397 días	24/02/2022	
	Todos los perfiles	Actualización de referencias		
3.9	Certificado de servidor seguro	Componentes en el SubjectDN de acuerdo con los requisitos CA/Browser Forum BR v1.8.4 Nuevos perfiles de certificados de firma electrónica para ciudadanos en la Sede Electrónica Notarial	06/02/2023	

Referencias

- Especificaciones técnicas relacionadas con la O.M. HAC/1181/2003.
- ETSI EN 319 412-1 v1.4.4 Certificate Profiles Part 1: Overview and common data structures
- ETSI EN 319 412-2 v2.2.1 Certificate Profiles Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 v1.2.1 Certificate Profiles Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-4 v1.2.1 Certificate Profiles Part 4: Certificate profile for web site certificates issued to organisations
- ETSI EN 319 412-5 v2.3.1 Certificate Profiles Part 5: QCStatements
- IETF RFC 6960. X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.
- IETF RFC 5280. Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 3739. Internet X.509 Public Key Infrastructure. Qualified Certificates Profile.
- ISO 3166-1, alpha-2 country codes.
- ISO/IEC 9594-8/ITU-T X.509.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Orden HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria. (B.O.E. 15-05-2003).
- CA/Browser Forum. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.8.1.
- Política de certificación del Consejo General del Notariado de España.

Índice

Perfiles de Certificados de la Entidad de Certificación.....	1
Agencia Notarial de Certificación.....	1
Información general	2
Control documental.....	2
Control de versiones	2
Referencias.....	5
Índice	6
1. Introducción.....	10
1.1. Convenciones.....	12
2. Certificados notariales	14
2.1. Certificado notarial personal (con garantía de dispositivo seguro)	14
2.1.1 Certificado de firma electrónica.....	14
2.1.2 Certificado de autenticación	17
2.1.3 Certificado de cifrado	20
2.2. Certificado notarial personal de representación personal (con garantía de dispositivo seguro).....	23
2.2.1 Certificado de firma.....	23
2.2.2 Certificado de autenticación	27
2.2.3 Certificado de cifrado	31
2.4. Certificado persona física Sede Electrónica Notarial	34
2.4.1 Perfil propuesto	34
2.5. Certificado notarial de servidor seguro (con garantía de dispositivo seguro).....	37
2.5.1 Perfil propuesto	37
2.6. Certificado notarial de servidor seguro (sin garantía de dispositivo seguro)	40
2.6.1 Perfil propuesto	40
2.7. Certificado notarial de autoridad de sellado de tiempo (con garantía de dispositivo seguro).....	43
2.7.1 Perfil propuesto	43
2.8. Certificado notarial de autoridad de sellado de tiempo (sin garantía de dispositivo seguro)	46

2.8.1 Perfil propuesto	46
2.9. Certificado notarial de firma de código (con garantía de dispositivo seguro)	49
2.9.1 Perfil propuesto	49
2.10. Certificado notarial de firma de código (sin garantía de dispositivo seguro)	52
2.10.1 Perfil propuesto	52
2.11. Certificado notarial de aplicación segura (con garantía de dispositivo seguro)	55
2.11.1 Perfil propuesto	55
2.12. Certificado notarial de aplicación segura (sin garantía de dispositivo seguro)	58
2.12.1 Perfil propuesto	58
2.13. Certificado notarial de OCSP Trusted Responder (sin garantía de dispositivo seguro) ...	61
2.13.1 Perfil propuesto	61
2.14. Certificado notarial corporativo (con garantía de dispositivo seguro)	64
2.14.1 Certificado de firma	64
2.14.2 Certificado de autenticación	68
2.14.3 Certificado de cifrado.....	72
2.15. Certificado notarial corporativo de representación (con garantía de dispositivo seguro)	75
2.15.1 Certificado de firma	75
2.15.2 Certificado de autenticación	79
2.15.3 Certificado de cifrado.....	83
2.16. Certificado notarial corporativo de representación AGE (con garantía de dispositivo seguro).....	86
2.16.1 Certificado de firma	86
2.16.2 Certificado de autenticación	89
2.16.3 Codificación de campos.....	91
2.17. Certificado notarial de facturación electrónica (sin garantía de dispositivo seguro).....	93
2.17.1 Perfil propuesto	93
2.18. Certificado de sello electrónico (con garantía de dispositivo seguro)	96
2.18.1 Perfil propuesto	96
2.19. Certificado de sello electrónico (sin garantía de dispositivo seguro)	99
2.19.1 Perfil propuesto	99
2.20. Certificado de representante Sede Electrónica Notarial.....	102

2.20.1 Perfil propuesto	102
3. Certificados corporativos	105
3.1. Certificado corporativo personal (con garantía de dispositivo seguro)	105
3.1.1 Certificado de firma.....	105
3.1.2 Certificado de autenticación	108
3.1.3 Certificado de cifrado	111
3.2. Certificado corporativo personal (sin garantía de dispositivo seguro).....	114
3.2.1 Perfil propuesto	114
3.3. Certificado corporativo de aplicación segura (sin garantía de dispositivo seguro).....	117
3.3.1 Perfil propuesto	117
3.4. Certificado corporativo de servidor seguro (sin garantía de dispositivo seguro)	120
3.4.1 Perfil propuesto	120
4. Certificados de Corporaciones de Derecho Público.....	123
4.1. Certificado personal de Corporación de Derecho Público (con garantía de dispositivo seguro).....	123
4.1.1 Certificado de firma.....	123
4.1.2 Certificado de autenticación	126
4.1.3 Certificado de cifrado	129
4.2. Certificado de aplicación segura de Corporación de Derecho Público (sin garantía de dispositivo seguro)	132
4.2.1 Perfil propuesto	132
5. Certificados del Consejo General del Notariado.....	135
5.1. Certificado FERN	135
5.1.1 Certificado de firma.....	135
5.1.2 Certificado de autenticación.....	138
5.1.3 Certificado de cifrado.....	141
5.1.4 Certificado de firma remota cualificada.....	144
5.1.5 Certificado de firma remota.....	147
5.2. Certificado de cargo	150
5.2.1 Certificado de firma.....	150
5.2.2 Certificado de autenticación	153
5.2.3 Certificado de cifrado	156

5.2.4 Unidades organizativas y cargos.....	158
5.3. Certificado de empleado/a.....	159
5.3.1 Certificado de firma.....	159
5.3.2 Certificado de autenticación.....	162
5.3.3 Certificado de cifrado	165
5.3.4 Certificado de firma (sin garantía de dispositivo seguro)	168
5.3.5 Certificado de firma remota cualificada.....	172
5.3.6 Certificado de firma remota.....	175
6. Atributos propios de ANCERT	179
6.1. Atributo "Nivel de apoderamiento": ANCERT.10.1.1	179
6.2. Atributo "Documento de representación": ANCERT.10.1.3	180
6.3. Atributo "Otras circunstancias personales": ANCERT.10.1.4	180
6.4. Atributo "Límite de uso por razón de la materia": ANCERT.10.1.5.....	180
6.5. Atributo "Datos registrales de la representación": ANCERT.10.1.6.....	180
6.6. Atributo "Persona representada": ANCERT.10.1.7	180
7. Certificados de infraestructura	183
7.1. Certificado de OCSP responder	183
7.1.1 Perfil propuesto	183
7.2. Certificado de Autoridad de Sellado de tiempo Cualificada	185
7.2.1 Perfil propuesto	185
8. Restricciones de los certificados.....	188
8.1. Componentes de los nombres de emisor y suscriptor.....	188
8.2. Extensión de políticas de certificados	188
8.3. Reglas de nomenclatura	188
8.4. Uso de SHA2RSA como algoritmo de firma	189

1. Introducción

Este documento recoge los perfiles de certificados que expedirá ANCERT, en cumplimiento de la Política de Certificación del Consejo General del Notariado de España.

El OID de ANCERT es 1.3.6.1.4.1.18920

Los perfiles de certificados descritos en este documento son los siguientes¹:

Certificados notariales

Certificado notarial personal (firma)	ANCERT.1.1.1.2.1
Certificado notarial personal (autenticación)	ANCERT.1.1.1.2.2
Certificado notarial personal (cifrado)	ANCERT.1.1.1.2.3
Certificado notarial personal de representación personal (firma)	ANCERT.1.1.2.2.1
Certificado notarial personal de representación personal (autenticación)	ANCERT.1.1.2.2.2
Certificado notarial personal de representación personal (cifrado)	ANCERT.1.1.2.2.3
Certificado persona física Sede Electrónica Notarial	ANCERT.1.1.3.1.2
Certificado notarial de servidor seguro (con dispositivo seguro)	ANCERT.1.2.1.2.1
Certificado notarial de servidor seguro (sin dispositivo seguro)	ANCERT.1.2.1.2.2
Certificado notarial de autoridad de sellado de tiempo (con dispositivo seguro)	ANCERT.1.2.3.2.1
Certificado notarial de autoridad de sellado de tiempo (sin dispositivo seguro)	ANCERT.1.2.3.2.2
Certificado notarial de firma de código (con dispositivo seguro)	ANCERT.1.2.5.2.1
Certificado notarial de firma de código (sin dispositivo seguro)	ANCERT.1.2.5.2.2
Certificado notarial de aplicación segura (con dispositivo seguro)	ANCERT.1.2.6.1.1
Certificado notarial de aplicación segura (sin dispositivo seguro)	ANCERT.1.2.6.1.2

¹ Se ha optado por emplear el último arco del OID de cada política para señalar la versión de la política, que siempre se trata de la versión 2, excepto para las políticas nuevas, que son, lógicamente, versión 1. Por su parte, para diferenciar los usos de claves en los certificados de la misma política con diferentes perfiles se ha añadido un arco adicional.

Certificado notarial de OCSP (sin dispositivo seguro)	ANCERT.1.2.7.1.2
Certificado notarial corporativo (firma)	ANCERT.1.3.1.2.1
Certificado notarial corporativo (autenticación)	ANCERT.1.3.1.2.2
Certificado notarial corporativo (cifrado)	ANCERT.1.3.1.2.3
Certificado notarial corporativo de representación (firma)	ANCERT.1.3.2.2.1
Certificado notarial corporativo de representación (autenticación)	ANCERT.1.3.2.2.2
Certificado notarial corporativo de representación (cifrado)	ANCERT.1.3.2.2.3
Certificado notarial corporativo de representación AGE (firma)	ANCERT.1.3.2.3.1
Certificado notarial corporativo de representación AGE (autenticación)	ANCERT.1.3.2.3.2
Certificado notarial de facturación electrónica (sin dispositivo seguro)	ANCERT.1.3.3.1.2
Certificado notarial de sello electrónico (con dispositivo seguro)	ANCERT.1.3.4.1.1
Certificado notarial de sello electrónico (sin dispositivo seguro)	ANCERT.1.3.4.1.2
Certificado de representante Sede Electrónica Notarial	ANCERT.1.3.5.1.2
Certificados corporativos personales (con dispositivo seguro - firma)	ANCERT.2.1.1.2.1
Certificados corporativos personales (con dispositivo seguro - autenticación)	ANCERT.2.1.1.2.2
Certificados corporativos personales (con dispositivo seguro - cifrado)	ANCERT.2.1.1.2.3
Certificados corporativos personales (sin dispositivo seguro)	ANCERT.2.1.1.2.4
Certificados corporativos de aplicación segura (sin dispositivo seguro)	ANCERT.2.2.1.1.2
Certificados corporativos de servidor seguro (sin dispositivo seguro)	ANCERT.2.2.2.1.2
Certificados de Corporaciones de Derecho Público	
Certificados personales de Corporaciones de Derecho Público (firma)	ANCERT.3.1.1.2.1
Certificados personales de Corporaciones de Derecho Público (autenticación)	ANCERT.3.1.1.2.2
Certificados personales de Corporaciones de Derecho Público (cifrado)	ANCERT.3.1.1.2.3

Certificados de aplicación segura de Corporaciones de Derecho Público (sin dispositivo seguro) ANCERT.3.2.1.1.2

Certificados Consejo General del Notariado

Certificado FERN - Firma electrónica reconocida notarial (firma) ANCERT.4.1.1.2.1

Certificado FERN - Firma electrónica reconocida notarial (autenticación) ANCERT.4.1.1.2.2

Certificado FERN - Firma electrónica reconocida notarial (cifrado) ANCERT.4.1.1.2.3

Certificado FERN - Firma electrónica remota cualificada ANCERT.4.1.1.3.1

Certificado FERN - Firma electrónica remota ANCERT.4.1.1.3.2

Certificado de cargo (firma) ANCERT.4.1.2.2.1

Certificado de cargo (autenticación) ANCERT.4.1.2.2.2

Certificado de cargo (cifrado) ANCERT.4.1.2.2.3

Certificado de empleado/a (firma) ANCERT.4.2.1.2.1

Certificado de empleado/a (autenticación) ANCERT.4.2.1.2.2

Certificado de empleado/a (cifrado) ANCERT.4.2.1.2.3

Certificado de empleado/a de firma (sin dispositivo seguro) ANCERT.4.2.1.2.4

Certificado de empleado/a de firma remota cualificada ANCERT.4.2.1.3.1

Certificado de empleado/a de firma remota ANCERT.4.2.1.3.2

Certificados de Servicios de firma electrónica

Certificado de OCSP

Certificado de TSA cualificada ANCERT.5.1.1.1

1.1. Convenciones

El presente documento utiliza una estructura de tabla para detallar la descripción de cada uno de los perfiles propuestos.

La tabla de descripción de perfil tiene las siguiente estructura:

Campo	Contenido	O	C
-------	-----------	---	---

La primera columna, denominada “Campo” se corresponde con el nombre del elemento del certificado descrito (campo básico, extensión, o subcomponente de los mismos). Para los nombres de los campos se ha optado por no traducir los nombres originales en inglés que aparecen en los estándares de referencia.

La columna “Contenido” detalla el valor que debe tomar cada campo. Para el caso de campos que solo pueden tomar dos valores, se utiliza la nomenclatura “Seleccionado. “1”” / “No Seleccionado. “0””. Para el caso de campos que pueden aparecer o ser opcionales, pero que no pueden tomar un valor, la columna “Contenido” contiene el literal “Presente” y completa su significado con la columna “O”.

La columna “O” indica si el campo es obligatorio (Sí) u opcional (No). Finalmente, la columna “C” es utilizada para indicar las extensiones que deben ser marcadas en el certificado como críticas.

2. Certificados notariales

2.1. Certificado notarial personal (con garantía de dispositivo seguro)

2.1.1 Certificado de firma electrónica

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²	Sí	
1.2. Serial Number	Establecido automáticamente ³	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁴	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁵		Sí	
1.6.1. Country (C)	País ⁶	Sí	
1.6.2. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.3. Organizational Unit (OU)	"Certificado Notarial Personal (Firma)"	Sí	
1.6.4. Surname	Apellidos	Sí	
1.6.5. Given Name	Nombre	Sí	
1.6.6. Serial Number	NIF ⁷	Sí	

² El literal "2" corresponde a la versión 3.

³ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁴ Debe ser el país de establecimiento del prestador del servicio de certificación.

⁵ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

⁶ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.7. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.1.1.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNPFirma "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNPFirma "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. dateOfBirth	Fecha de nacimiento	Sí	

⁷ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6.2. CountryOfCitizenship	Nacionalidad del suscriptor	Sí	
2.6.3. ANCERT.10.1.4	Circunstancias adicionales de la persona física	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCP_V2crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTTCP_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTTCP_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTTCP_V2.crt"		
2.10. Qualified Certificate Statements		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

2.1.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ⁸	Sí	
1.2. Serial Number	Establecido automáticamente ⁹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁰	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹¹		Sí	
1.6.1. Country (C)	País ¹²	Sí	
1.6.2. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.3. Organizational Unit (OU)	"Certificado Notarial Personal (Autentica)"	Sí	
1.6.4. Surname	Apellidos	Sí	
1.6.5. Given Name	Nombre	Sí	
1.6.6. Serial Number	NIF ¹³	Sí	
1.6.7. Common Name (CN)	Nombre y apellidos	Sí	

⁸ El literal "2" corresponde a la versión 3.

⁹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁰ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹¹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹² El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

¹³ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.1.1.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNPAuth"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNPAuth"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. dateOfBirth	Fecha de nacimiento	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del suscriptor	Sí	
2.6.3. ANCERT.10.1.4	Circunstancias adicionales de la persona física	No	
2.7. Basic Constraints		Sí	Sí

Campo	Contenido	O	C
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente		
2.8.2. clientAuth	Presente		
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERT CP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCER TCP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCER TCP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/cert s/ANCERTCP_V2.crt"		
2.11. Qualified Certificate Statements		Sí	
2.11.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.11.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	

2.1.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁴	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁷		Sí	
1.6.1. Country (C)	País ¹⁸	Sí	
1.6.2. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.3. Organizational Unit (OU)	"Certificado Notarial Personal (Cifrado)"	Sí	
1.6.4. Surname	Apellidos	Sí	
1.6.5. Given Name	Nombre	Sí	
1.6.6. Serial Number	NIF ¹⁹	Sí	
1.6.7. Common Name (CN)	Nombre y apellidos	Sí	

¹⁴ El literal "2" corresponde a la versión 3.

¹⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

¹⁹ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.1.1.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNPCifra "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNPCifra "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. dateOfBirth	Fecha de nacimiento	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del suscriptor	Sí	
2.6.3. ANCERT.10.1.4	Circunstancias adicionales de la persona física	No	
2.7. Basic Constraints		Sí	Sí

Campo	Contenido	O	C
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente		
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERT CP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCER TCP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCER TCP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.1)	"http://www.ancert.com/pki/v2/cert s/ANCERTCP_V2.crt"		

2.2. Certificado notarial personal de representación personal (con garantía de dispositivo seguro)

2.2.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁰	Sí	
1.2. Serial Number	Establecido automáticamente ²¹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²²	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²³		Sí	
1.6.1. Country (C)	País ²⁴	Sí	
1.6.2. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.3. Organizational Unit (OU)	"Certificado Notarial de Representación Personal (Firma)"	Sí	
1.6.4. Title	Rol o función en conexión con la representación	No	
1.6.5. Surname	Apellidos representante	Sí	
1.6.6. Given Name	Nombre representante	Sí	

²⁰ El literal "2" corresponde a la versión 3.

²¹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²² Debe ser el país de establecimiento del prestador del servicio de certificación.

²³ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.7. Serial Number	NIF ²⁵ representante	Sí	
1.6.8. Common Name (CN)	Nombre y apellidos representante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente		
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.1.2.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNPRPFirma"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNPRPFirma"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	

²⁵ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6.1. dateOfBirth	Fecha de nacimiento del suscriptor (representante)	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del suscriptor (representante)	Sí	
2.6.3. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.4. ANCERT.10.1.3	Documento de representación	Sí	
2.6.5. ANCERT.10.1.4	Atributos adicionales de la persona física	No	
2.6.6. ANCERT.10.1.5	Límite de uso	No ²⁶	
2.6.7. ANCERT.10.1.6	Datos registrales de la representación	No ²⁷	
2.6.8. ANCERT.10.1.7	Persona representada (física)	Sí	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCP_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTTCP_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTTCP_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTTCP_V2.crt"		
1.1. Qualified Certificate Statements ²⁸		Sí	
1.1.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
1.1.2. QcEuLimitValue (OID 0.4.0.1862.1.2)		No ²⁹	

²⁶ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

²⁷ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

²⁸ No existe en el perfil actual, pero se propone incorporarlo.

²⁹ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

Campo	Contenido	O	C
1.1.2.1. Currency	Moneda, de acuerdo con la norma ISO 4217		
1.1.2.2. Amount	Cantidad		
1.1.2.3. Exponent	Exponente		
1.1.3. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
1.1.4. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

2.2.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³⁰	Sí	
1.2. Serial Number	Establecido automáticamente ³¹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³²	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ³³		Sí	
1.6.1. Country (C)	País ³⁴	Sí	
1.6.2. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.3. Organizational Unit (OU)	"Certificado Notarial de Representación Personal (Autentica)"	Sí	
1.6.4. Title	Rol o función en conexión con la representación	No	
1.6.5. Surname	Apellidos representante	Sí	

³⁰ El literal "2" corresponde a la versión 3.

³¹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³² Debe ser el país de establecimiento del prestador del servicio de certificación.

³³ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.6. Given Name	Nombre representante	Sí	
1.6.7. Serial Number	NIF ³⁵ representante	Sí	
1.6.8. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.1.2.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNPRPAuth "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNPRPAuth "		
2.5. Subject Alternative Names		Sí	

³⁵ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. dateOfBirth	Fecha de nacimiento (representante)	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del suscriptor (representante)	Sí	
2.6.3. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.4. ANCERT.10.1.3	Documento de representación	Sí	
2.6.5. ANCERT.10.1.4	Atributos adicionales de la persona física	No	
2.6.6. ANCERT.10.1.5	Límite de uso	No ³⁶	
2.6.7. ANCERT.10.1.6	Datos registrales de la representación	No ³⁷	
2.6.8. ANCERT.10.1.7	Persona representada (física)	Sí	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente		
2.8.2. clientAuth	Presente		
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCP_V2.crt"		
2.11. Qualified Certificate Statements ³⁸		Sí	

³⁶ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

³⁷ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

³⁸ No existe en el perfil actual, pero se propone incorporarlo.

Campo	Contenido	O	C
2.11.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.11.2. QcEuLimitValue (OID 0.4.0.1862.1.2)		No ³⁹	
2.11.2.1. Currency	Moneda, de acuerdo con la norma ISO 4217		
2.11.2.2. Amount	Cantidad		
2.11.2.3. Exponent	Exponente		
2.11.3. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	

³⁹ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

2.2.3 Certificado de cifrado

Campo	Contenido	Obligatorio	Crítico
1. Basic structure			
1.1. Version	"2" ⁴⁰	Sí	
1.2. Serial Number	Establecido automáticamente ⁴¹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁴²	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁴³		Sí	
1.6.1. Country (C)	País ⁴⁴	Sí	
1.6.2. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.3. Organizational Unit (OU)	"Certificado Notarial de Representación Personal (Cifrado)"	Sí	
1.6.4. Title	Rol o función en conexión con la representación	No	
1.6.5. Surname	Apellidos representante	Sí	
1.6.6. Given Name	Nombre representante	Sí	
1.6.7. Serial Number	NIF ⁴⁵ representante	Sí	

⁴⁰ El literal "2" corresponde a la versión 3.

⁴¹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁴² Debe ser el país de establecimiento del prestador del servicio de certificación.

⁴³ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

⁴⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	Obligatorio	Crítico
1.6.8. Common Name (CN)	Nombre y apellidos representante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.1.2.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNPRPCifra "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNPRPCifra "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	

⁴⁵ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.6.1. dateOfBirth	Fecha de nacimiento (representante)	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del suscriptor (representante)	Sí	
2.6.3. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.4. ANCERT.10.1.3	Documento de representación	Sí	
2.6.5. ANCERT.10.1.4	Atributos adicionales de la persona física	No	
2.6.6. ANCERT.10.1.5	Límite de uso	No ⁴⁶	
2.6.7. ANCERT.10.1.6	Datos registrales de la representación	No ⁴⁷	
2.6.8. ANCERT.10.1.7	Persona representada (física)	Sí	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente		
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCP_V2.crt"		

⁴⁶ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

⁴⁷ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

2.4. Certificado persona física Sede Electrónica Notarial

2.4.1 Perfil propuesto

Campo	Contenido	O	C
2. Basic structure			
2.12. Version	"2" ⁴⁸	Sí	
2.13. Serial Number	Establecido automáticamente ⁴⁹	Sí	
2.14. Signature Algorithm	SHA-256 with RSA Signature	Sí	
2.15. Issuer Distinguished Name		Sí	
2.15.1. Country (C)	"ES" ⁵⁰	Sí	
2.15.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
2.15.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
2.15.4. Common Name (CN)	"ANCERT Certificados Notariales Personales V2"	Sí	
2.16. Validity	2 años	Sí	
2.16.1. Not Before	Fecha de inicio de validez		
2.16.2. Not After	Fecha de expiración		
2.17. Subject		Sí	
2.17.1. Country (C)	País ⁵¹	Sí	
2.17.2. Organizational Unit (OU)	"Certificado persona física Sede Electrónica Notarial"	Sí	
2.17.3. Surname	Apellido(s)	Sí	
2.17.4. Given Name	Nombre	Sí	
2.17.5. Serial Number	NIF/NIE ⁵²	Sí	
2.17.6. Common Name (CN)	Nombre y apellido(s)	Sí	

⁴⁸ El literal "2" corresponde a la versión 3.

⁴⁹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁵⁰ Debe ser el país de establecimiento del prestador del servicio de certificación.

⁵¹ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

⁵² Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
2.18. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
3. Extensions			
3.1. Authority Key Identifier	Presente	Sí	
3.1.1. Key Identifier	Presente	Sí	
3.2. Subject Key Identifier	Presente	Sí	
3.3. Key Usage		Sí	Sí
3.3.1. Digital Signature	Seleccionado. "0"		
3.3.2. Content Commitment	No seleccionado. "1"		
3.3.3. Key Encipherment	No seleccionado. "0"		
3.3.4. Data Encipherment	No seleccionado. "0"		
3.3.5. Key Agreement	No seleccionado. "0"		
3.3.6. Key Certificate Signature	No seleccionado. "0"		
3.3.7. CRL Signature	No seleccionado. "0"		
3.3.8. EncipherOnly	No seleccionado. "0"		
3.3.9. DecipherOnly	No seleccionado. "0"		
3.4. Certificate Policies		Sí	
3.4.1. Policy Identifier	ANCERT. 1.1.3.1.2		
3.4.2. Policy Qualifier ID			
3.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CPSEN"		
3.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CPSEN"		
3.4.2.3. Policy Identifier	0.4.0.194112.1.0	Sí	
3.5. Subject Alternative Names		Sí	
3.5.1. rfc822Name	Correo electrónico		
3.6. Basic Constraints		Sí	Sí
3.6.1. CA	Falso		
3.7. CRL Distribution Points		Sí	
3.7.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCP_V2.crl"		

Campo	Contenido	O	C
3.7.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCP_V2.crl"		
3.8. Authority Information Access		Sí	
3.8.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
3.8.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCP_V2.crt"		
3.9. Qualified Certificate Statements ⁵³		Sí	
3.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
3.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (13 años)	Sí	
3.9.3. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
3.9.4. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
3.9.5. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId-Natural (OID 0.4.0.194121.1.1)	Sí	

⁵³ No existe en el perfil actual, pero se propone incorporarlo.

2.5. Certificado notarial de servidor seguro (con garantía de dispositivo seguro)

2.5.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ⁵⁴	Sí	
1.2. Serial Number	Establecido automáticamente ⁵⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁵⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	397 días	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁵⁷		Sí	
1.6.1. Country (C)	País ⁵⁸	Sí	
1.6.2. StateOrProvince (ST)	Provincia	Sí	
1.6.3. Locality (L)	Localidad	Sí	
1.6.4. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No ⁵⁹	
1.6.5. Surname	Apellidos de la persona física, cuando sea suscriptora del certificado	No	

⁵⁴ El literal "2" corresponde a la versión 3.

⁵⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁵⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

⁵⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

⁵⁸ El campo "país" será el de nacionalidad del suscriptor del certificado, indicándose el código de dos letras especificado en la norma ISO 3166.

⁵⁹ El campo Organization (O) es obligatorio para las personas jurídicas mientras que los campos Surname y Given Name lo son para las personas físicas.

Campo	Contenido	O	C
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Dominio ⁶⁰	No	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.1.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNSSHard"		
2.4.2.2. User Notice ⁶¹	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNSSHard"		
2.5. Subject Alternative Names		Sí	

⁶⁰ Si está presente, debe contener uno de los valores presentes en la extensión Subject Alternative Names.

⁶¹ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
2.5.1. rfc822Name	Correo electrónico	No	
2.5.2. dnsName	Nombre del servidor y dominio	Sí	
2.5.3. ipAddress	Dirección IP del servidor	No	
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. ServerAuth	Presente	Sí	
2.7.2. ClientAuth	Presente	No	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		

2.6. Certificado notarial de servidor seguro (sin garantía de dispositivo seguro)

2.6.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ⁶²	Sí	
1.2. Serial Number	Establecido automáticamente ⁶³	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁶⁴	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	397 días	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁶⁵		Sí	
1.6.1. Country (C)	País ⁶⁶	Sí	
1.6.2. StateOrProvince (ST)	Provincia	Sí	
1.6.3. Locality (L)	Localidad	Sí	
1.6.4. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No ⁶⁷	
1.6.5. Surname	Apellidos de la persona física, cuando sea suscriptora del certificado	No	

⁶² El literal "2" corresponde a la versión 3.

⁶³ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁶⁴ Debe ser el país de establecimiento del prestador del servicio de certificación.

⁶⁵ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

⁶⁶ El campo "país" será el de nacionalidad del suscriptor del certificado, indicándose el código de dos letras especificado en la norma ISO 3166.

⁶⁷ El campo Organization (O) es obligatorio para las personas jurídicas mientras que los campos Surname y Given Name lo son para las personas físicas.

Campo	Contenido	O	C
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Dominio ⁶⁸	No	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.1.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNSSSoft"		
2.4.2.2. User Notice ⁶⁹	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNSSSoft"		
2.5. Subject Alternative Names		Sí	

⁶⁸ Si está presente, debe contener uno de los valores presentes en la extensión Subject Alternative Names.

⁶⁹ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
2.5.1. rfc822Name	Correo electrónico	No	
2.5.2. dnsName	Nombre del servidor y dominio	Sí	
2.5.3. ipAddress	Dirección IP del servidor	No	
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. ServerAuth	Presente	Sí	
2.7.2. ClientAuth	Presente	No	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		

2.7. Certificado notarial de autoridad de sellado de tiempo (con garantía de dispositivo seguro)

2.7.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ⁷⁰	Sí	
1.2. Serial Number	Establecido automáticamente ⁷¹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁷²	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	6 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁷³		Sí	
1.6.1. Country (C)	País ⁷⁴	Sí	
1.6.2. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No ⁷⁵	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial de Sellado de Tiempo"	Sí	
1.6.5. Surname	Apellidos de la persona física, cuando	No	

⁷⁰ El literal "2" corresponde a la versión 3.

⁷¹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁷² Debe ser el país de establecimiento del prestador del servicio de certificación.

⁷³ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

⁷⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

⁷⁵ El campo Organization (O) es obligatorio para las personas jurídicas mientras que los campos Surname y Given Name lo son para las personas físicas.

Campo	Contenido	O	C
	sea suscriptora del certificado		
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Nombre de la autoridad y unidad de sellado de tiempo	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.3.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNSTHard"		
2.4.2.2. User Notice ⁷⁶	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNSTHard"		
2.5. Subject Alternative Names		Sí	

⁷⁶ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		No	
2.6.1. ANCERT.10.1.5	Límite de uso	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	Sí ⁷⁷
2.8.1. timeStamping	Presente		
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		
2.11. Subject Information Access ⁷⁸		No	
2.11.1. Access Method	OID para TimeStamping		
2.11.2. Access Location	Dirección HTTP/FTP de prestación del servicio de fecha de tiempo		

⁷⁷ Impuesto por IETF RFC 3161.

⁷⁸ Tantos como métodos de acceso se emplean para los protocolos de la TSA.

2.8. Certificado notarial de autoridad de sellado de tiempo (sin garantía de dispositivo seguro)

2.8.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ⁷⁹	Sí	
1.2. Serial Number	Establecido automáticamente ⁸⁰	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁸¹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	6 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁸²		Sí	
1.6.1. Country (C)	País ⁸³	Sí	
1.6.2. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No ⁸⁴	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial de Sellado de	Sí	

⁷⁹ El literal "2" corresponde a la versión 3.

⁸⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁸¹ Debe ser el país de establecimiento del prestador del servicio de certificación.

⁸² Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

⁸³ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

⁸⁴ El campo Organization (O) es obligatorio para las personas jurídicas mientras que los campos Surname y Given Name lo son para las personas físicas.

Campo	Contenido	O	C
	Tiempo"		
1.6.5. Surname	Apellidos de la persona física, cuando sea suscriptora del certificado	No	
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Nombre de la autoridad de sellado de tiempo	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.3.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNSTSoft"		
2.4.2.2. User Notice ⁸⁵	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones"		

⁸⁵ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
	/CNSTSoft"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		No	
2.6.1. ANCERT.10.1.5	Límite de uso	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	Sí ⁸⁶
2.8.1. timeStamping	Presente		
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		
2.11. Subject Information Access ⁸⁷		No	
2.11.1. Access Method	OID para TimeStamping		
2.11.2. Access Location	Dirección HTTP/FTP de prestación del servicio de fecha de tiempo		

⁸⁶ Impuesto por IETF RFC 3161.

⁸⁷ Tantos como métodos de acceso se emplean para los protocolos de la TSA.

2.9. Certificado notarial de firma de código (con garantía de dispositivo seguro)

2.9.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ⁸⁸	Sí	
1.2. Serial Number	Establecido automáticamente ⁸⁹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁹⁰	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁹¹		Sí	
1.6.1. Country (C)	País ⁹²	Sí	
1.6.2. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No ⁹³	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial de Firma de	Sí	

⁸⁸ El literal "2" corresponde a la versión 3.

⁸⁹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁹⁰ Debe ser el país de establecimiento del prestador del servicio de certificación.

⁹¹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

⁹² El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

⁹³ El campo Organization (O) es obligatorio para las personas jurídicas mientras que los campos Surname y Given Name lo son para las personas físicas.

Campo	Contenido	O	C
	Código"		
1.6.5. Surname	Apellidos de la persona física, cuando sea suscriptora del certificado	No	
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Nombre del editor de código	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.5.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNSFCHard"		
2.4.2.2. User Notice ⁹⁴	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNSFCHard"		

⁹⁴ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	Sí
2.7.1. CodeSigning	Presente		
2.7.2. Lifetime signing ⁹⁵	Presente		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		

⁹⁵ OID: 1.3.6.1.4.1.311.10.3.13

2.10. Certificado notarial de firma de código (sin garantía de dispositivo seguro)

2.10.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ⁹⁶	Sí	
1.2. Serial Number	Establecido automáticamente ⁹⁷	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ⁹⁸	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ⁹⁹		Sí	
1.6.1. Country (C)	País ¹⁰⁰	Sí	
1.6.2. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial de Firma de Código"	Sí	
1.6.5. Surname	Apellidos de la persona física, cuando sea suscriptora del certificado	No	

⁹⁶ El literal "2" corresponde a la versión 3.

⁹⁷ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁹⁸ Debe ser el país de establecimiento del prestador del servicio de certificación.

⁹⁹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁰⁰ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Nombre del editor de código	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.5.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNSFCSof "		
2.4.2.2. User Notice ¹⁰¹	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNSFCSof "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		

¹⁰¹ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	Sí ¹⁰²
2.7.1. CodeSigning	Presente		
2.7.2. Lifetime Signing ¹⁰³	Presente		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		

¹⁰² Impuesto por IETF RFC 3161.

¹⁰³ OID: 1.3.6.1.4.1.311.10.3.13

2.11. Certificado notarial de aplicación segura (con garantía de dispositivo seguro)

2.11.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁰⁴	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁰⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁰⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁰⁷		Sí	
1.6.1. Country (C)	País ¹⁰⁸	Sí	
1.6.2. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No ¹⁰⁹	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial de Aplicación	Sí	

¹⁰⁴ El literal "2" corresponde a la versión 3.

¹⁰⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁰⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁰⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁰⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

¹⁰⁹ El campo Organization (O) es obligatorio para las personas jurídicas mientras que los campos Surname y Given Name lo son para las personas físicas.

Campo	Contenido	O	C
	Segura"		
1.6.5. Surname	Apellidos de la persona física, cuando sea suscriptora del certificado	No	
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Identificación de la aplicación segura	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.6.1.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNASHard"		
2.4.2.2. User Notice ¹¹⁰	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNASHard"		

¹¹⁰ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		No	
2.6.1. ANCERT.10.1.5	Límite de uso	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		

2.12. Certificado notarial de aplicación segura (sin garantía de dispositivo seguro)

2.12.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹¹¹	Sí	
1.2. Serial Number	Establecido automáticamente ¹¹²	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹¹³	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹¹⁴		Sí	
1.6.1. Country (C)	País ¹¹⁵	Sí	
1.6.2. Organization (O)	Nombre de la entidad, cuando sea suscriptora del certificado	No ¹¹⁶	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial de Aplicación Segura"	Sí	
1.6.5. Surname	Apellidos de la persona física, cuando	No	

¹¹¹ El literal "2" corresponde a la versión 3.

¹¹² No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹¹³ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹¹⁴ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹¹⁵ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

¹¹⁶ El campo Organization (O) es obligatorio para las personas jurídicas mientras que los campos Surname y Given Name lo son para las personas físicas.

Campo	Contenido	O	C
	sea suscriptora del certificado		
1.6.6. Given Name	Nombre de la persona física, cuando sea suscriptora del certificado	No	
1.6.7. Serial Number	CIF o NIF de la persona física o entidad suscriptora del certificado.	Sí	
1.6.8. Common Name (CN)	Identificación de la aplicación segura	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.2.6.1.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNASSoft "		
2.4.2.2. User Notice ¹¹⁷	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNASSoft "		
2.5. Subject Alternative Names		Sí	

¹¹⁷ Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		No	
2.6.1. ANCERT.10.1.5	Límite de uso	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		

2.13. Certificado notarial de OCSP Trusted Responder (sin garantía de dispositivo seguro)

2.13.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹¹⁸	Sí	
1.2. Serial Number	Establecido automáticamente ¹¹⁹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹²⁰	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject		Sí	
1.6.1. Country (C)	País ¹²¹	Sí	
1.6.2. Organization (O)	Nombre de la entidad prestadora del servicio OCSP	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organization Unit (OU)	"Certificado Notarial de TR OCSP"	Sí	
1.6.5. Serial Number	CIF de la entidad de prestadora del servicio OCSP	Sí	
1.6.6. Common Name (CN)	"OCSP de " + nombre de la Entidad prestadora del servicio OCSP	Sí	

¹¹⁸ El literal "2" corresponde a la versión 3.

¹¹⁹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹²⁰ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹²¹ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
1. Extensions			
1.1. Authority Key Identifier	Presente	Sí	
1.1.1. Key Identifier	Presente	Sí	
1.2. Subject Key Identifier	Presente	Sí	
1.3. Key Usage		Sí	Sí
1.3.1. Digital Signature	Seleccionado. "1"		
1.3.2. Content Commitment	No seleccionado. "0"		
1.3.3. Key Encipherment	No seleccionado. "0"		
1.3.4. Data Encipherment	No seleccionado. "0"		
1.3.5. Key Agreement	No seleccionado. "0"		
1.3.6. Key Certificate Signature	No seleccionado. "0"		
1.3.7. CRL Signature	No seleccionado. "0"		
1.3.8. EncipherOnly	No seleccionado. "0"		
1.3.9. DecipherOnly	No seleccionado. "0"		
1.4. Certificate Policies		Sí	
1.4.1. Policy Identifier	ANCERT.1.2.7.1.2		
1.4.2. Policy Qualifier ID			
1.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNSOCSP "		
1.4.2.2. User Notice ¹²²	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNSOCSP "		
1.5. Subject Alternative Names		Sí	
1.5.1. rfc822Name	Correo electrónico		
1.6. Basic Constraints		Sí	Sí
1.6.1. CA	Falso		
1.7. Extended Key Usage		Sí	Sí
1.7.1. OCSPSigning	Presente		

¹²² Se modifica el texto para no indicar que se trata de un certificado reconocido.

Campo	Contenido	O	C
1.8. OID: 1.3.6.1.5.5.7.48.1.5 ¹²³	NULL	Sí	

¹²³ Indica que el estado de revocación del certificado de OCSP no se verifica.

2.14. Certificado notarial corporativo (con garantía de dispositivo seguro)

2.14.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹²⁴	Sí	
1.2. Serial Number	Establecido automáticamente ¹²⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹²⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹²⁷		Sí	
1.6.1. Country (C)	País ¹²⁸	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo (Firma)"	Sí	
1.6.5. Title	Rol o función del custodio	No	
1.6.6. Surname	Apellidos del custodio	Sí	

¹²⁴ El literal "2" corresponde a la versión 3.

¹²⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹²⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹²⁷ Se propone modificar la estructura del campo Subject, en concordancia con los restantes perfiles de certificados, que siguen la alternativa 2 de las especificaciones de la AEAT, y para evitar superar las longitudes de los componentes del nombre, siguiendo las recomendaciones establecidas en la serie de Recomendaciones ITU-T X.500. Asimismo, se elimina el componente EA, dado que debe aparecer en el campo Subject Alternative Name.

¹²⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.7. Given Name	Nombre del custodio	Sí	
1.6.8. OID "1.3.6.1.4.1.18838.1.1"	NIF ¹²⁹ del custodio	Sí	
1.6.9. Serial Number	NIF de la entidad suscriptora	Sí	
1.6.10. Common Name (CN)	Nombre de la entidad suscriptora	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.1.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNCFirma "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCFirma "		
2.5. Subject Alternative Names		Sí	

¹²⁹ El campo "1.3.6.1.4.1.18838.1.1" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.2. ANCERT.10.1.3	Documento de representación	Sí	
2.6.3. ANCERT.10.1.5	Límite de uso	No	
2.6.4. ANCERT.10.1.6	Datos registrales de la representación	No ¹³⁰	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		
2.10. Qualified Certificate Statements ¹³¹		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuLimitValue (OID 0.4.0.1862.1.2)		No ¹³²	
2.10.2.1. Currency	Moneda, de acuerdo con la norma ISO 4217		
2.10.2.2. Amount	Cantidad		
2.10.2.3. Exponent	Exponente		
2.10.3. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	

¹³⁰ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

¹³¹ No existe en el perfil actual, pero se propone incorporarlo.

¹³² Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

Campo	Contenido	O	C
2.10.4. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

2.14.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹³³	Sí	
1.2. Serial Number	Establecido automáticamente ¹³⁴	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹³⁵	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹³⁶		Sí	
1.6.1. Country (C)	País ¹³⁷	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo (Autentica)"	Sí	
1.6.5. Title	Rol o función del custodio	No	
1.6.6. Surname	Apellidos del custodio	Sí	
1.6.7. Given Name	Nombre del custodio	Sí	

¹³³ El literal "2" corresponde a la versión 3.

¹³⁴ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹³⁵ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹³⁶ Se propone modificar la estructura del campo Subject, en concordancia con los restantes perfiles de certificados, que siguen la alternativa 2 de las especificaciones de la AEAT, y para evitar superar las longitudes de los componentes del nombre, siguiendo las recomendaciones establecidas en la serie de Recomendaciones ITU-T X.500. Asimismo, se elimina el componente EA, dado que debe aparecer en el campo Subject Alternative Name.

¹³⁷ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.8. OID "1.3.6.1.4.1.18838.1.1"	NIF ¹³⁸ del custodio	Sí	
1.6.9. Serial Number	NIF de la entidad suscriptora	Sí	
1.6.10. Common Name (CN)	Nombre de la entidad suscriptora	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.1.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNCAuth "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCAuth "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		

¹³⁸ El campo "1.3.6.1.4.1.18838.1.1" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.2. ANCERT.10.1.3	Documento de representación	Sí	
2.6.3. ANCERT.10.1.5	Límite de uso	No	
2.6.4. ANCERT.10.1.6	Datos registrales de la representación	No ¹³⁹	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCNC_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		
2.11. Qualified Certificate Statements ¹⁴⁰		Sí	
2.11.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.11.2. QcEuLimitValue (OID 0.4.0.1862.1.2)		No ¹⁴¹	
2.11.2.1. Currency	Moneda, de acuerdo con la norma ISO 4217		
2.11.2.2. Amount	Cantidad		

¹³⁹ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

¹⁴⁰ No existe en el perfil actual, pero se propone incorporarlo.

¹⁴¹ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

Campo	Contenido	O	C
2.11.2.3. Exponent	Exponente		
2.11.3. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	

2.14.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁴²	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁴³	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁴⁴	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁴⁵		Sí	
1.6.1. Country (C)	País ¹⁴⁶	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo (Cifrado)"	Sí	
1.6.5. Title	Rol o función del custodio	No	
1.6.6. Surname	Apellidos del custodio	Sí	
1.6.7. Given Name	Nombre del custodio	Sí	

¹⁴² El literal "2" corresponde a la versión 3.

¹⁴³ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁴⁴ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁴⁵ Se propone modificar la estructura del campo Subject, en concordancia con los restantes perfiles de certificados, que siguen la alternativa 2 de las especificaciones de la AEAT, y para evitar superar las longitudes de los componentes del nombre, siguiendo las recomendaciones establecidas en la serie de Recomendaciones ITU-T X.500. Asimismo, se elimina el componente EA, dado que debe aparecer en el campo Subject Alternative Name.

¹⁴⁶ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.8. OID "1.3.6.1.4.1.18838.1.1"	NIF ¹⁴⁷ del custodio	Sí	
1.6.9. Serial Number	NIF de la entidad suscriptora	Sí	
1.6.10. Common Name (CN)	Nombre de la entidad suscriptora	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.1.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNCCifra "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCCifra "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		

¹⁴⁷ El campo "1.3.6.1.4.1.18838.1.1" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.2. ANCERT.10.1.3	Documento de representación	Sí	
2.6.3. ANCERT.10.1.5	Límite de uso	No	
2.6.4. ANCERT.10.1.6	Datos registrales de la representación	No ¹⁴⁸	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCNC_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		

¹⁴⁸ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

2.15. Certificado notarial corporativo de representación (con garantía de dispositivo seguro)

2.15.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁴⁹	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁵⁰	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁵¹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁵²		Sí	
1.6.1. Country (C)	País ¹⁵³	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo de Representación (Firma)"	Sí	
1.6.5. Title	Rol o función conectado con la representación	No	
1.6.6. Surname	Apellidos de la persona física	Sí	

¹⁴⁹ El literal "2" corresponde a la versión 3.

¹⁵⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁵¹ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁵² Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁵³ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
	representante		
1.6.7. Given Name	Nombre de la persona física representante	Sí	
1.6.8. Serial Number	NIF ¹⁵⁴ de la persona física representante	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos del representante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.2.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNCRFirma"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCRFirma"		

¹⁵⁴ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. dateOfBirth	Fecha de nacimiento del representante	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del representante	Sí	
2.6.3. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.4. ANCERT.10.1.3	Documento de representación	Sí	
2.6.5. ANCERT.10.1.4	Circunstancias adicionales de la persona física	No	
2.6.6. ANCERT.10.1.5	Límite de uso	No ¹⁵⁵	
2.6.7. ANCERT.10.1.6	Datos registrales de la representación	No ¹⁵⁶	
2.6.8. ANCERT.10.1.7	Persona representada (jurídica)	Sí	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		
2.10. Qualified Certificate Statements ¹⁵⁷		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuLimitValue (OID 0.4.0.1862.1.2)		No ¹⁵⁸	

¹⁵⁵ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

¹⁵⁶ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

¹⁵⁷ No existe en el perfil actual, pero se propone incorporarlo.

Campo	Contenido	O	C
2.10.2.1. Currency	Moneda, de acuerdo con la norma ISO 4217		
2.10.2.2. Amount	Cantidad		
2.10.2.3. Exponent	Exponente		
2.10.3. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.4. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

¹⁵⁸ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

2.15.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁵⁹	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁶⁰	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁶¹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁶²		Sí	
1.6.1. Country (C)	País ¹⁶³	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo de Representación (Autentica)"	Sí	
1.6.5. Title	Rol o función conectado con la representación	No	
1.6.6. Surname	Apellidos de la persona física representante	Sí	
1.6.7. Given Name	Nombre de la persona física representante	Sí	

¹⁵⁹ El literal "2" corresponde a la versión 3.

¹⁶⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁶¹ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁶² Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁶³ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.8. Serial Number	NIF ¹⁶⁴ de la persona física representante	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos del representante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.2.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNCRAuth"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCRAuth"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		

¹⁶⁴ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6. Subject Directory Attributes		Sí	
2.6.1. dateOfBirth	Fecha de nacimiento del representante	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del representante	Sí	
2.6.3. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.4. ANCERT.10.1.3	Documento de representación	Sí	
2.6.5. ANCERT.10.1.4	Circunstancias adicionales de la persona física	No	
2.6.6. ANCERT.10.1.5	Límite de uso	No ¹⁶⁵	
2.6.7. ANCERT.10.1.6	Datos registrales de la representación	No ¹⁶⁶	
2.6.8. ANCERT.10.1.7	Persona representada (jurídica)	Sí	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCNC_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		
2.11. Qualified Certificate Statements ¹⁶⁷		Sí	
2.11.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	

¹⁶⁵ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

¹⁶⁶ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

¹⁶⁷ No existe en el perfil actual, pero se propone incorporarlo.

Campo	Contenido	O	C
2.11.2. QcEuLimitValue (OID 0.4.0.1862.1.2)		No ¹⁶⁸	
2.11.2.1. Currency	Moneda, de acuerdo con la norma ISO 4217		
2.11.2.2. Amount	Cantidad		
2.11.2.3. Exponent	Exponente		
2.11.3. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	

¹⁶⁸ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

2.15.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁶⁹	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁷⁰	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁷¹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁷²		Sí	
1.6.1. Country (C)	País ¹⁷³	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo de Representación (Cifrado)"	Sí	
1.6.5. Title	Rol o función conectado con la representación	Sí	
1.6.6. Surname	Apellidos de la persona física representante	Sí	
1.6.7. Given Name	Nombre de la persona física representante	Sí	

¹⁶⁹ El literal "2" corresponde a la versión 3.

¹⁷⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁷¹ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁷² Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁷³ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.8. Serial Number	NIF ¹⁷⁴ de la persona física representante	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos del representante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.2.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNRCifra"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNRCifra"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		

¹⁷⁴ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6. Subject Directory Attributes		Sí	
2.6.1. dateOfBirth	Fecha de nacimiento del representante	Sí	
2.6.2. CountryOfCitizenship	Nacionalidad del representante	Sí	
2.6.3. ANCERT.10.1.1	Nivel de apoderamiento	Sí	
2.6.4. ANCERT.10.1.3	Documento de representación	Sí	
2.6.5. ANCERT.10.1.4	Circunstancias adicionales de la persona física	No	
2.6.6. ANCERT.10.1.5	Límite de uso	No ¹⁷⁵	
2.6.7. ANCERT.10.1.6	Datos registrales de la representación	No ¹⁷⁶	
2.6.8. ANCERT.10.1.7	Persona representada (jurídica)	Sí	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCNC_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		

¹⁷⁵ Resulta obligatorio cuando el contenido del atributo ANCERT.10.1.1 contiene "Poderes limitados".

¹⁷⁶ Es obligatorio cuando la representación se encuentra sujeta a inscripción obligatoria.

2.16. Certificado notarial corporativo de representación AGE (con garantía de dispositivo seguro)

2.16.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁷⁷	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁷⁸	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁷⁹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁸⁰		Sí	
1.6.1. Description (2.5.4.13)	Documento público que acredita las facultades del representante o los datos registrales. (Ver sección 2.16.3)	Sí	
1.6.2. Country (C)	País ¹⁸¹	Sí	
1.6.3. Organization (O)	Razón Social (entidad subscriptora), tal como figura en los registros oficiales.	Sí	
1.6.4. Organization Identifier (2.5.4.97)	NIF de la entidad subscriptora ¹⁸²		

¹⁷⁷ El literal "2" corresponde a la versión 3.

¹⁷⁸ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁷⁹ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁸⁰ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁸¹ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

¹⁸² Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
1.6.5. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.6. Organizational Unit (OU)	"Certificado Notarial Corporativo de Representación"	Sí	
1.6.7. Surname	Apellidos de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.8. Given Name	Nombre de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.9. Serial Number	DNI/NIE ¹⁸³ del representante	Sí	
1.6.10. Common Name (CN)	Codificación detallada en la sección 2.16.3	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.2.3.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condicione		

¹⁸³ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
	s/CNCRFirma”		
2.4.2.2. User Notice	“Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCRFirma ”		
2.4.3. Policy Identifier	0.4.0.194112.1.2	Sí	
2.4.4. Policy Identifier	2.16.724.1.3.5.8	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. CRL Distribution Points		Sí	
2.7.1. distributionPoint	“ http://www.ancert.com/crl/ANCERTCNC_V2.crl ”		
2.7.2. distributionPoint	“ http://www2.ancert.com/crl/ANCERTCNC_V2.crl ”		
2.8. Authority Information Access		Sí	
2.8.1. Access Method (1.3.6.1.5.5.7.48.1)	“ http://ocsp.ac.ancert.com/ocsp.xuda ”		
2.8.2. Access Method (1.3.6.1.5.5.7.48.2)	“ http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt ”		
2.9. Qualified Certificate Statements		Sí	
2.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.9.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	
2.9.4. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
2.9.5. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
2.9.6. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (OID 0.4.0.194121.1.1)	Sí	

2.16.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁸⁴	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁸⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁸⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁸⁷		Sí	
1.6.1. Description (2.5.4.13)	Documento público que acredita las facultades del representante o los datos registrales. (Ver sección 2.16.3)	Sí	
1.6.2. Country (C)	País ¹⁸⁸	Sí	
1.6.3. Organization (O)	Razón Social (entidad subscriptora), tal como figura en los registros oficiales.	Sí	
1.6.4. Organization Identifier (2.5.4.97)	NIF de la entidad subscriptora ¹⁸⁹		
1.6.5. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	

¹⁸⁴ El literal "2" corresponde a la versión 3.

¹⁸⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁸⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁸⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁸⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

¹⁸⁹ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
1.6.6. Organizational Unit (OU)	"Certificado Notarial Corporativo de Representación"	Sí	
1.6.7. Surname	Apellidos de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.8. Given Name	Nombre de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.9. Serial Number	DNI/NIE ¹⁹⁰ del representante	Sí	
1.6.10. Common Name (CN)	Codificación detallada en la sección 2.16.3	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.2.3.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNCRAuth"		
2.4.2.2. User Notice	"Este certificado se expide como"		

¹⁹⁰ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
	Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCRAuth		
2.4.3. Policy Identifier	0.4.0.194112.1.0	Sí	
2.4.4. Policy Identifier	2.16.724.1.3.5.8	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	" http://www.ancert.com/crl/ANCERTCNC_V2.crl "		
2.8.2. distributionPoint	" http://www2.ancert.com/crl/ANCERTCNC_V2.crl "		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	" http://ocsp.ac.ancert.com/ocsp.xuda "		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	" http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt "		

2.16.3 Codificación de campos

La clase de certificados Certificado Notarial Corporativo de Representación AGE, es un subtipo de la Clase Certificado Notarial Corporativo de Representación que se ajusta a los perfiles de certificados propuestos en el Anexo I del documento "Perfiles de certificados electrónicos" de abril de 2016 publicado por el Ministerio de Hacienda y Administraciones Públicas del Gobierno de España. Este documento define el perfil básico de interoperabilidad para los certificados de representante de persona jurídica usados en las relaciones con la Administración General del Estado (AGE).

Common Name

Campo	Contenido	Longitud¹⁹¹
NIF	Número DNI/NIE del representate	10
Nombre	Nombre del representate tal y como figura en el DNI / NIE	4
Apellido 1	Primer apellido del representate tal y como figura en el DNI / NIE	9
Literal	(R:	2
NIF	NIF del representado, tal como figura en los registros oficiales	9
Literal)	2
Literal (opcional)	ATENTIC, FIRMA	8

Description

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.

- 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

¹⁹¹ Contando espacio blanco posterior

2.17. Certificado notarial de facturación electrónica (sin garantía de dispositivo seguro)

2.17.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁹²	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁹³	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ¹⁹⁴	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ¹⁹⁵		Sí	
1.6.1. Country (C)	País ¹⁹⁶	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora del certificado	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial de Facturación	Sí	

¹⁹² El literal "2" corresponde a la versión 3.

¹⁹³ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁹⁴ Debe ser el país de establecimiento del prestador del servicio de certificación.

¹⁹⁵ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

¹⁹⁶ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
	Electrónica"		
1.6.5. Pseudonym	"Seudónimo: Custodio de certificado de facturación"	Sí	
1.6.6. Serial Number	NIF de la entidad suscriptora del certificado.	Sí	
1.6.7. Common Name (CN)	Nombre de la entidad suscriptora del certificado	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.3.1.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNFESoft"		

Campo	Contenido	O	C
2.4.2.2. User Notice ¹⁹⁷	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNFESoft "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		No	
2.6.1. ANCERT.10.1.5	Límite de uso	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	" http://www.ancert.com/crl/ANCERTCNC_V2.crl "		
2.8.2. distributionPoint	" http://www2.ancert.com/crl/ANCERTCNC_V2.crl "		
2.8.3. distributionPoint	" http://www3.ancert.com/crl/ANCERTCNC_V2.crl "		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	" http://ocsp.ac.ancert.com/ocsp.xuda "		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	" http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt "		

¹⁹⁷ Se modifica el texto para no indicar que se trata de un certificado reconocido.

2.18. Certificado de sello electrónico (con garantía de dispositivo seguro)

2.18.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ¹⁹⁸	Sí	
1.2. Serial Number	Establecido automáticamente ¹⁹⁹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁰⁰	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁰¹		Sí	
1.6.1. Country (C)	País ²⁰²	Sí	
1.6.2. Organization (O)	Razón Social (entidad subscriptora), tal como figura en los registros oficiales.	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo de Sello Electrónico"	Sí	
1.6.5. Organization Identifier (2.5.4.97)	CIF de la entidad subscriptora ²⁰³	Sí	

¹⁹⁸ El literal "2" corresponde a la versión 3.

¹⁹⁹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁰⁰ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁰¹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁰² El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²⁰³ Utilizando la semántica propuesta por la norma ETSI EN319 412-1 sección 5.1.4.

Campo	Contenido	O	C
1.6.6. Common Name (CN)	Nombre utilizado para referirse a la entidad subscriptora (puede no coincidir exactamente con la razón social)	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	Seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT. 1.3.4.1.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNCsello "		
2.4.2.2. User Notice	"Este certificado se expide como Sello Electronico Cualificado de acuerdo con la legislacion vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCsello "		
2.4.3. Policy Identifier	0.4.0.194112.1.3	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		

Campo	Contenido	O	C
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		
2.10. Qualified Certificate Statements		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	
2.10.4. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
2.10.5. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-eseal (OID 0.4.0.1862.1.6.2)	Sí	
2.10.6. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (OID 0.4.0.194121.1.2)	Sí	

2.19. Certificado de sello electrónico (sin garantía de dispositivo seguro)

2.19.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁰⁴	Sí	
1.2. Serial Number	Establecido automáticamente ²⁰⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁰⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁰⁷		Sí	
1.6.1. Country (C)	País ²⁰⁸	Sí	
1.6.2. Organization (O)	Razón Social (entidad subscriptora), tal como figura en los registros oficiales.	Sí	
1.6.3. Organizational Unit (OU)	"Autorizado ante Notario " + identificación de Notario	Sí	
1.6.4. Organizational Unit (OU)	"Certificado Notarial Corporativo de Sello Electrónico"	Sí	
1.6.5. Organization Identifier (2.5.4.97)	CIF de la entidad subscriptora ²⁰⁹	Sí	

²⁰⁴ El literal "2" corresponde a la versión 3.

²⁰⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁰⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁰⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁰⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²⁰⁹ Utilizando la semántica propuesta por la norma ETSI EN319 412-1 sección 5.1.4.

Campo	Contenido	O	C
1.6.6. Common Name (CN)	Nombre utilizado para referirse a la entidad subscriptora (puede no coincidir exactamente con la razón social)	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	Seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.1.3.4.1.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CNCsello "		
2.4.2.2. User Notice	"Este certificado se expide como Sello Electronico Cualificado de acuerdo con la legislacion vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCsello "		
2.4.3. Policy Identifier	0.4.0.194112.1.1	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		

Campo	Contenido	O	C
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCNC_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCNC_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt"		
2.10. Qualified Certificate Statements		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.3. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
2.10.4. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-eseal (OID 0.4.0.1862.1.6.2)	Sí	
2.10.5. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (OID 0.4.0.194121.1.2)	Sí	

2.20. Certificado de representante Sede Electrónica Notarial

2.20.1 Perfil propuesto

Campo	Contenido	O	C
2. Basic structure			
2.10. Version	"2" ²¹⁰	Sí	
2.11. Serial Number	Establecido automáticamente ²¹¹	Sí	
2.12. Signature Algorithm	SHA-256 with RSA Signature	Sí	
2.13. Issuer Distinguished Name		Sí	
2.13.1. Country (C)	"ES" ²¹²	Sí	
2.13.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
2.13.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
2.13.4. Common Name (CN)	"ANCERT Certificados Notariales Corporativos V2"	Sí	
2.14. Validity	2 años	Sí	
2.14.1. Not Before	Fecha de inicio de validez		
2.14.2. Not After	Fecha de expiración		
2.15. Subject ²¹³		Sí	
2.15.1. Description (2.5.4.13)	Documento público que acredita las facultades del representante o los datos registrales. (ver sección 2.16.3)	Sí	
2.15.2. Country (C)	País ²¹⁴	Sí	
2.15.3. Organization (O)	Razón Social (entidad subscriptora), tal como figura en los registros oficiales.	Sí	
2.15.4. Organization Identifier (2.5.4.97)	NIF de la entidad subscriptora ²¹⁵		

²¹⁰ El literal "2" corresponde a la versión 3.

²¹¹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²¹² Debe ser el país de establecimiento del prestador del servicio de certificación.

²¹³ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²¹⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²¹⁵ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
2.15.5. Organizational Unit (OU)	"Certificado de representante Sede Electrónica Notarial"	Sí	
2.15.6. Surname	Apellido(s) de la persona física representante (como consta en el DNI/NIE)	Sí	
2.15.7. Given Name	Nombre de la persona física representante (como consta en el DNI/NIE)	Sí	
2.15.8. Serial Number	DNI/NIE ²¹⁶ del representante	Sí	
2.15.9. Common Name (CN)	Codificación detallada en la sección 2.16.3	Sí	
2.16. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
3. Extensions			
3.1. Authority Key Identifier	Presente	Sí	
3.1.1. Key Identifier	Presente	Sí	
3.2. Subject Key Identifier	Presente	Sí	
3.3. Key Usage		Sí	Sí
3.3.1. Digital Signature	No seleccionado. "0"		
3.3.2. Content Commitment	Seleccionado. "1"		
3.3.3. Key Encipherment	No seleccionado. "0"		
3.3.4. Data Encipherment	No seleccionado. "0"		
3.3.5. Key Agreement	No seleccionado. "0"		
3.3.6. Key Certificate Signature	No seleccionado. "0"		
3.3.7. CRL Signature	No seleccionado. "0"		
3.3.8. EncipherOnly	No seleccionado. "0"		
3.3.9. DecipherOnly	No seleccionado. "0"		
3.4. Certificate Policies		Sí	
3.4.1. Policy Identifier	ANCERT. 1.3.5.1.2		
3.4.2. Policy Qualifier ID			
3.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CRSEN"		

²¹⁶ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
3.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CRSEN "		
3.4.3. Policy Identifier	0.4.0.194112.1.0	Sí	
3.4.4. Policy Identifier	2.16.724.1.3.5.8	Sí	
3.5. Subject Alternative Names		Sí	
3.5.1. rfc822Name	Correo electrónico		
3.6. Basic Constraints		Sí	Sí
3.6.1. CA	Falso		
3.7. CRL Distribution Points		Sí	
3.7.1. distributionPoint	" http://www.ancert.com/crl/ANCERTCNC_V2.crl "		
3.7.2. distributionPoint	" http://www2.ancert.com/crl/ANCERTCNC_V2.crl "		
3.8. Authority Information Access		Sí	
3.8.1. Access Method (1.3.6.1.5.5.7.48.1)	" http://ocsp.ac.ancert.com/ocsp.xuda "		
3.8.2. Access Method (1.3.6.1.5.5.7.48.2)	" http://www.ancert.com/pki/v2/certs/ANCERTCNC_V2.crt "		
3.9. Qualified Certificate Statements		Sí	
3.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
3.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (13 años)	Sí	
3.9.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	
3.9.4. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
3.9.5. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
3.9.6. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId-Natural (OID 0.4.0.194121.1.1)	Sí	

3. Certificados corporativos

3.1. Certificado corporativo personal (con garantía de dispositivo seguro)

3.1.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²¹⁷	Sí	
1.2. Serial Number	Establecido automáticamente ²¹⁸	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²¹⁹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporativos Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²²⁰		Sí	
1.6.1. Country (C)	País ²²¹	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	Campo libre ²²²	No	
1.6.4. Organizational Unit (OU)	"Certificado Corporativo Personal (Firma)"	Sí	
1.6.5. Title	Rol o función del poseedor de claves	No	
1.6.6. Surname	Apellidos del poseedor de claves	Sí	

²¹⁷ El literal "2" corresponde a la versión 3.

²¹⁸ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²¹⁹ Debe ser el país de establecimiento del prestador del servicio de certificación.

²²⁰ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²²¹ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²²² Sólo puede emplearse para indicar una división departamental de la entidad.

Campo	Contenido	O	C
1.6.7. Given Name	Nombre del poseedor de claves	Sí	
1.6.8. Serial Number	NIF ²²³ del poseedor de claves	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos del poseedor de claves	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.2.1.1.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCPFirma"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	"Sin garantía de poderes"	Sí	

²²³ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6.2. ANCERT.10.1.4	Atributos adicionales del poseedor de claves	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCCP_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCCP_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCCP_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCCP_V2.crt"		

3.1.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²²⁴	Sí	
1.2. Serial Number	Establecido automáticamente ²²⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²²⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporativos Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²²⁷		Sí	
1.6.1. Country (C)	País ²²⁸	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	Campo libre ²²⁹	No	
1.6.4. Organizational Unit (OU)	"Certificado Corporativo Personal (Auténtica)"	Sí	
1.6.5. Title	Rol o función del poseedor de claves	No	
1.6.6. Surname	Apellidos del poseedor de claves	Sí	
1.6.7. Given Name	Nombre del poseedor de claves	Sí	
1.6.8. Serial Number	NIF ²³⁰ del poseedor de claves	Sí	

²²⁴ El literal "2" corresponde a la versión 3.

²²⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²²⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

²²⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²²⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²²⁹ Sólo puede emplearse para indicar una división departamental de la entidad.

²³⁰ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
1.6.9. Common Name (CN)	Nombre y apellidos del poseedor de claves	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.2.1.1.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCPAAuth"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	"Sin garantía de poderes"	Sí	
2.6.2. ANCERT.10.1.4	Atributos adicionales del poseedor de claves	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	

Campo	Contenido	O	C
2.8.2. clientAuth	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCCP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCCP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCCP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCCP_V2.crt"		

3.1.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²³¹	Sí	
1.2. Serial Number	Establecido automáticamente ²³²	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²³³	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporativos Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²³⁴		Sí	
1.6.1. Country (C)	País ²³⁵	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	Campo libre ²³⁶	No	
1.6.4. Organizational Unit (OU)	"Certificado Corporativo Personal (Cifrado)"	Sí	
1.6.5. Title	Rol o función del poseedor de claves	No	
1.6.6. Surname	Apellidos del poseedor de claves	Sí	
1.6.7. Given Name	Nombre del poseedor de claves	Sí	
1.6.8. Serial Number	NIF ²³⁷ del poseedor de claves	Sí	

²³¹ El literal "2" corresponde a la versión 3.

²³² No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²³³ Debe ser el país de establecimiento del prestador del servicio de certificación.

²³⁴ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²³⁵ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²³⁶ Sólo puede emplearse para indicar una división departamental de la entidad.

²³⁷ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
1.6.9. Common Name (CN)	Nombre y apellidos del poseedor de claves	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.2.1.1.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CCPCifra "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	"Sin garantía de poderes"	Sí	
2.6.2. ANCERT.10.1.4	Atributos adicionales del poseedor de claves	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	

Campo	Contenido	O	C
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCCP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCCP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCCP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCCP_V2.crt"		

3.2. Certificado corporativo personal (sin garantía de dispositivo seguro)

3.2.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic estructura			
1.1. Version	"2" ²³⁸	Sí	
1.2. Serial Number	Establecido automáticamente ²³⁹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁴⁰	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporativos Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁴¹		Sí	
1.6.1. Country (C)	País ²⁴²	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	Campo libre ²⁴³	No	
1.6.4. Organizational Unit (OU)	"Certificado Corporativo Personal"	Sí	
1.6.5. Title	Rol o función del poseedor de claves en la entidad suscriptora	No	
1.6.6. Surname	Apellidos del poseedor de claves	Sí	
1.6.7. Given Name	Nombre del poseedor de claves	Sí	
1.6.8. Serial Number	NIF ²⁴⁴ del poseedor de claves	Sí	

²³⁸ El literal "2" corresponde a la versión 3.

²³⁹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁴⁰ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁴¹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁴² El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²⁴³ Sólo puede emplearse para indicar una división departamental de la entidad.

Campo	Contenido	O	C
1.6.9. Common Name (CN)	Nombre y apellidos del poseedor de claves	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.2.1.1.2.4		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCPSoft"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	"Sin garantía de poderes"	Sí	
2.6.2. ANCERT.10.1.4	Atributos adicionales del poseedor de claves	No	
2.7. Basic Constraints		Sí	Sí

²⁴⁴ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCCP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCCP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCCP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCCP_V2.crt"		

3.3. Certificado corporativo de aplicación segura (sin garantía de dispositivo seguro)

3.3.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁴⁵	Sí	
1.2. Serial Number	Establecido automáticamente ²⁴⁶	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁴⁷	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporativos de Sistemas V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject		Sí	
1.6.1. Country (C)	País ²⁴⁸	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Certificado Corporativo de Aplicación Segura"	Sí	
1.6.4. Serial Number	NIF de la entidad suscriptora	Sí	
1.6.5. Common Name (CN)	Identificador de la aplicación segura	Sí	

²⁴⁵ El literal "2" corresponde a la versión 3.

²⁴⁶ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁴⁷ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁴⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.2.2.1.1.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCASSoft"		
2.4.2.2. User Notice	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CCASSoft"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	

Campo	Contenido	O	C
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERT CCS_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ ANCERTCCS_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ ANCERTCCS_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/cert s/ANCERTCCS_V2.crt"		

3.4. Certificado corporativo de servidor seguro (sin garantía de dispositivo seguro)

3.4.1 Perfil propuesto

Campo	Contenido	O	C
2. Basic structure			
2.10. Version	"2" ²⁴⁹	Sí	
2.11. Serial Number	Establecido automáticamente ²⁵⁰	Sí	
2.12. Signature Algorithm	SHA-256 with RSA Signature	Sí	
2.13. Issuer Distinguished Name		Sí	
2.13.1. Country (C)	"ES" ²⁵¹	Sí	
2.13.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
2.13.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
2.13.4. Common Name (CN)	"ANCERT Corporativos de Sistemas V2"	Sí	
2.14. Validity	3 años	Sí	
2.14.1. Not Before	Fecha de inicio de validez		
2.14.2. Not After	Fecha de expiración		
2.15. Subject		Sí	
2.15.1. Country (C)	País ²⁵²	Sí	
2.15.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
2.15.3. Organizational Unit (OU)	"Certificado Corporativo de Servidor Seguro"	Sí	
2.15.4. Serial Number	NIF de la entidad suscriptora	Sí	
2.15.5. Common Name (CN)	Nombre del servidor y dominio	No	

²⁴⁹ El literal "2" corresponde a la versión 3.

²⁵⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁵¹ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁵² El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
2.16. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
3. Extensions			
3.1. Authority Key Identifier	Presente	Sí	
3.1.1. Key Identifier	Presente	Sí	
3.2. Subject Key Identifier	Presente	Sí	
3.3. Key Usage		Sí	Sí
3.3.1. Digital Signature	Seleccionado. "1"		
3.3.2. Content Commitment	No seleccionado. "0"		
3.3.3. Key Encipherment	Seleccionado. "1"		
3.3.4. Data Encipherment	Seleccionado. "1"		
3.3.5. Key Agreement	No seleccionado. "0"		
3.3.6. Key Certificate Signature	No seleccionado. "0"		
3.3.7. CRL Signature	No seleccionado. "0"		
3.3.8. EncipherOnly	No seleccionado. "0"		
3.3.9. DecipherOnly	No seleccionado. "0"		
3.4. Certificate Policies		Sí	
3.4.1. Policy Identifier	ANCERT.2.2.2.1.2		
3.4.2. Policy Qualifier ID			
3.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCSSSoft"		
3.4.2.2. User Notice	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CCSSSoft"		
3.5. Subject Alternative Names		Sí	
3.5.1. rfc822Name	Correo electrónico	No	
3.5.2. dnsName	Nombre del servidor y dominio	Sí	
3.5.3. ipAddress	Dirección IP del servidor	No	
3.6. Basic Constraints		Sí	Sí

Campo	Contenido	O	C
3.6.1. CA	Falso		
3.7. Extended Key Usage		Sí	
3.7.1. serverAuth	Presente	Sí	
3.7.2. clientAuth	Presente	No	
3.8. CRL Distribution Points		Sí	
3.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERT CCS_V2.crl"		
3.8.2. distributionPoint	"http://www2.ancert.com/crl/ ANCERTCCS_V2.crl"		
3.8.3. distributionPoint	"http://www3.ancert.com/crl/ ANCERTCCS_V2.crl"		
3.9. Authority Information Access		Sí	
3.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
3.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/cert s/ANCERTCCS_V2.crt"		

4. Certificados de Corporaciones de Derecho Público

4.1. Certificado personal de Corporación de Derecho Público (con garantía de dispositivo seguro)

4.1.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁵³	Sí	
1.2. Serial Number	Establecido automáticamente ²⁵⁴	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁵⁵	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporaciones de Derecho Publico Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁵⁶		Sí	
1.6.1. Country (C)	País ²⁵⁷	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	Campo libre ²⁵⁸	No	
1.6.4. Organizational Unit (OU)	"Cert. Personal de Corporación de Derecho Público (Firma)"	Sí	
1.6.5. Title	Rol o función del poseedor de claves	No	

²⁵³ El literal "2" corresponde a la versión 3.

²⁵⁴ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁵⁵ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁵⁶ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁵⁷ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²⁵⁸ Sólo puede emplearse para indicar una división departamental de la entidad.

Campo	Contenido	O	C
1.6.6. Surname	Apellidos del poseedor de claves	Sí	
1.6.7. Given Name	Nombre del poseedor de claves	Sí	
1.6.8. Serial Number	NIF ²⁵⁹ del poseedor de claves	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos del poseedor de claves	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.3.1.1.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCDPPFirma"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	"Sin garantía de poderes"	Sí	

²⁵⁹ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6.2. ANCERT.10.1.4	Atributos adicionales del poseedor de claves	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCDPP_V2.crt"		

4.1.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic estructura			
1.1. Version	"2" ²⁶⁰	Sí	
1.2. Serial Number	Establecido automáticamente ²⁶¹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁶²	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporaciones de Derecho Publico Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁶³		Sí	
1.6.1. Country (C)	País ²⁶⁴	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	Campo libre ²⁶⁵	No	
1.6.4. Organizational Unit (OU)	"Cert. Personal de Corporación de Derecho Público (Autentica)"	Sí	
1.6.5. Title	Rol o función del poseedor de claves	No	
1.6.6. Surname	Apellidos del poseedor de claves	Sí	
1.6.7. Given Name	Nombre del poseedor de claves	Sí	
1.6.8. Serial Number	NIF ²⁶⁶ del poseedor de claves	Sí	

²⁶⁰ El literal "2" corresponde a la versión 3.

²⁶¹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁶² Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁶³ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁶⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²⁶⁵ Sólo puede emplearse para indicar una división departamental de la entidad.

²⁶⁶ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
1.6.9. Common Name (CN)	Nombre y apellidos del poseedor de claves	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.3.1.1.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCDPPAuth"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	"Sin garantía de poderes"	Sí	
2.6.2. ANCERT.10.1.4	Atributos adicionales del poseedor de claves	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	

Campo	Contenido	O	C
2.8.2. clientAuth	Presente	Sí	
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCDPP_V2.crt"		

4.1.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁶⁷	Sí	
1.2. Serial Number	Establecido automáticamente ²⁶⁸	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁶⁹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporaciones de Derecho Publico Personales V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁷⁰		Sí	
1.6.1. Country (C)	País ²⁷¹	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	Campo libre ²⁷²	No	
1.6.4. Organizational Unit (OU)	"Cert. Personal de Corporación de Derecho Público (Cifrado)"	Sí	
1.6.5. Title	Rol o función del poseedor de claves	No	
1.6.6. Surname	Apellidos del poseedor de claves	Sí	
1.6.7. Given Name	Nombre del poseedor de claves	Sí	
1.6.8. Serial Number	NIF ²⁷³ del poseedor de claves	Sí	

²⁶⁷ El literal "2" corresponde a la versión 3.

²⁶⁸ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁶⁹ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁷⁰ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁷¹ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

²⁷² Sólo puede emplearse para indicar una división departamental de la entidad.

²⁷³ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
1.6.9. Common Name (CN)	Nombre y apellidos del poseedor de claves	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.3.1.1.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCDPPCifra"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Subject Directory Attributes		Sí	
2.6.1. ANCERT.10.1.1	"Sin garantía de poderes"	Sí	
2.6.2. ANCERT.10.1.4	Atributos adicionales del poseedor de claves	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. CA	Falso		
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	

Campo	Contenido	O	C
2.9. CRL Distribution Points		Sí	
2.9.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.9.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.9.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCDPP_V2.crl"		
2.10. Authority Information Access		Sí	
2.10.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.10.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCDPP_V2.crt"		

4.2. Certificado de aplicación segura de Corporación de Derecho Público (sin garantía de dispositivo seguro)

4.2.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁷⁴	Sí	
1.2. Serial Number	Establecido automáticamente ²⁷⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁷⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificación S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporaciones de Derecho Público de Sistemas V2"	Sí	
1.5. Validity	3 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁷⁷		Sí	
1.6.1. Country (C)	País ²⁷⁸	Sí	
1.6.2. Organization (O)	Nombre de la entidad suscriptora	Sí	
1.6.3. Organizational Unit (OU)	"Cert. Aplicación Segura de Corporación de Derecho Público"	Sí	
1.6.4. Client Serial Number	CIF entidad	Sí	
1.6.5. Common Name (CN)	Id aplicación segura	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	

²⁷⁴ El literal "2" corresponde a la versión 3.

²⁷⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁷⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁷⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁷⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.3.2.1.1.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CCDPASSoft "		
2.4.2.2. User Notice	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CCDPASSoft "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	" http://www.ancert.com/crl/ANCERTCDPS_V2.crl "		

Campo	Contenido	O	C
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCDPS_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCDPS_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCDPS_V2.crt"		

5. Certificados del Consejo General del Notariado

5.1. Certificado FERN

5.1.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁷⁹	Sí	
1.2. Serial Number	Establecido automáticamente ²⁸⁰	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁸¹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.4.5. Validity	3 o 5 años	Sí	
1.4.6. Not Before	Fecha de inicio de validez		
1.4.7. Not After	Fecha de expiración		
1.5. Subject ²⁸²		Sí	
1.5.1. Country (C)	País ²⁸³	Sí	
1.5.2. State or Province (ST)	Provincia	Sí	
1.5.3. Locality (L)	Localidad	Sí	
1.5.4. Organization (O)	"Consejo General del Notariado"	Sí	
1.5.5. Organizational Unit (OU)	Entidad integrante de la organización colegial notarial	Sí	
1.5.6. Organizational Unit (OU)	Código de notaría	Sí	
1.5.7. Title	"Notario (Firma)"	Sí	

²⁷⁹ El literal "2" corresponde a la versión 3.

²⁸⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁸¹ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁸² Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁸³ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.5.8. Surname	Apellidos	Sí	
1.5.9. Given Name	Nombre	Sí	
1.5.10. Serial Number	NIF ²⁸⁴	Sí	
1.5.11. Common Name (CN)	Nombre y apellidos	Sí	
1.6. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.1.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CCGNFERNFirma "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNFERNFirma "		
2.5. Subject Alternative Names		Sí	

²⁸⁴ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. CRL Distribution Points		Sí	
2.7.1. distributionPoint	"http://www.ancert.com/crl/ANCERTFERN_V2.crl"		
2.7.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.7.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8. Authority Information Access		Sí	
2.8.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.8.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		
2.9. Qualified Certificate Statements ²⁸⁵		Sí	
2.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.9.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

²⁸⁵ No existe en el perfil actual, pero se propone incorporarlo.

5.1.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁸⁶	Sí	
1.2. Serial Number	Establecido automáticamente ²⁸⁷	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁸⁸	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.5. Validity	3 o 5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁸⁹		Sí	
1.6.1. Country (C)	País ²⁹⁰	Sí	
1.6.2. State or Province (ST)	Provincia	Sí	
1.6.3. Locality (L)	Localidad	Sí	
1.6.4. Organization (O)	"Consejo General del Notariado"	Sí	
1.6.5. Organizational Unit (OU)	Entidad integrante de la organización colegial notarial	Sí	
1.6.6. Organizational Unit (OU)	Código de notaría	Sí	
1.6.7. Title	"Notario (Autentica)"	Sí	
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	
1.6.10. Serial Number	NIF ²⁹¹	Sí	

²⁸⁶ El literal "2" corresponde a la versión 3.

²⁸⁷ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁸⁸ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁸⁹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁹⁰ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.11. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.1.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNFERNAuth"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNFERNAuth"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		

²⁹¹ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTFERN_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		
2.10. Qualified Certificate Statements ²⁹²		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

²⁹² No existe en el perfil actual, pero se propone incorporarlo.

5.1.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ²⁹³	Sí	
1.2. Serial Number	Establecido automáticamente ²⁹⁴	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ²⁹⁵	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.5. Validity	3 o 5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ²⁹⁶		Sí	
1.6.1. Country (C)	País ²⁹⁷	Sí	
1.6.2. State or Province (ST)	Provincia	Sí	
1.6.3. Locality (L)	Localidad	Sí	
1.6.4. Organization (O)	"Consejo General del Notariado"	Sí	
1.6.5. Organizational Unit (OU)	Entidad integrante de la organización colegial notarial	Sí	
1.6.6. Organizational Unit (OU)	Código de notaría	Sí	
1.6.7. Title	"Notario (Cifrado)"	Sí	
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	

²⁹³ El literal "2" corresponde a la versión 3.

²⁹⁴ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁹⁵ Debe ser el país de establecimiento del prestador del servicio de certificación.

²⁹⁶ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

²⁹⁷ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.10. Serial Number	NIF ²⁹⁸	Sí	
1.6.11. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.1.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNFERNCifra"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNFERNCifra"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí

²⁹⁸ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	O	C
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTFERN_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		

5.1.4 Certificado de firma remota cualificada

Campo	Contenido	O	C
1. Basic estructura			
1.1. Version	"2" ²⁹⁹	Sí	
1.2. Serial Number	Establecido automáticamente ³⁰⁰	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³⁰¹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.4.5. Validity	3 años	Sí	
1.4.6. Not Before	Fecha de inicio de validez		
1.4.7. Not After	Fecha de expiración		
1.5. Subject ³⁰²		Sí	
1.5.1. Country (C)	País ³⁰³	Sí	
1.5.2. State or Province (ST)	Provincia	Sí	
1.5.3. Locality (L)	Localidad	Sí	
1.5.4. Organization (O)	"Consejo General del Notariado"	Sí	
1.5.5. Organizational Unit (OU)	Entidad integrante de la organización colegial notarial	Sí	
1.5.6. Organizational Unit (OU)	Código de notaría	Sí	
1.5.7. Title	"Notario"	Sí	
1.5.8. Surname	Apellidos	Sí	
1.5.9. Given Name	Nombre	Sí	
1.5.10. Serial Number	IDCES-NIF ³⁰⁴	Sí	

²⁹⁹ El literal "2" corresponde a la versión 3.

³⁰⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁰¹ Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁰² Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³⁰³ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.5.11. Common Name (CN)	Nombre y primer apellido + “ (rQSCD)”	Sí	
1.6. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. “0”		
2.3.2. Content Commitment	Seleccionado. “1”		
2.3.3. Key Encipherment	No seleccionado. “0”		
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.3.8. EncipherOnly	No seleccionado. “0”		
2.3.9. DecipherOnly	No seleccionado. “0”		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.1.3.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	“ https://www.ancert.com/condiciones/CCGNFERNFirmaCentralizada ”		
2.4.2.2. User Notice	“Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNFERNFirmaCentralizada ”		
2.4.3. Policy Identifier	0.4.0.194112.1.2	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí

³⁰⁴ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
2.6.1. CA	Falso		
2.7. CRL Distribution Points		Sí	
2.7.1. distributionPoint	"http://www.ancert.com/crl/ANCERT_FERN_V2.crl"		
2.7.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8. Authority Information Access		Sí	
2.8.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.8.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		
2.9. Qualified Certificate Statements ³⁰⁵		Sí	
2.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.9.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	
2.9.4. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
2.9.5. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
2.9.6. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId-Natural (OID 0.4.0.194121.1.1)	Sí	

³⁰⁵ No existe en el perfil actual, pero se propone incorporarlo.

5.1.5 Certificado de firma remota

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³⁰⁶	Sí	
1.2. Serial Number	Establecido automáticamente ³⁰⁷	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³⁰⁸	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.4.5. Validity	3 años	Sí	
1.4.6. Not Before	Fecha de inicio de validez		
1.4.7. Not After	Fecha de expiración		
1.5. Subject ³⁰⁹		Sí	
1.5.1. Country (C)	País ³¹⁰	Sí	
1.5.2. State or Province (ST)	Provincia	Sí	
1.5.3. Locality (L)	Localidad	Sí	
1.5.4. Organization (O)	"Consejo General del Notariado"	Sí	
1.5.5. Organizational Unit (OU)	Entidad integrante de la organización colegial notarial	Sí	
1.5.6. Organizational Unit (OU)	Código de notaría	Sí	
1.5.7. Title	"Notario"	Sí	
1.5.8. Surname	Apellidos	Sí	
1.5.9. Given Name	Nombre	Sí	
1.5.10. Serial Number	IDCES-NIF ³¹¹	Sí	

³⁰⁶ El literal "2" corresponde a la versión 3.

³⁰⁷ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁰⁸ Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁰⁹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³¹⁰ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.5.11. Common Name (CN)	Nombre y primer apellido + “ (rSCD)”	Sí	
1.6. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”		
2.3.2. Content Commitment	Seleccionado. “1”		
2.3.3. Key Encipherment	Seleccionado. “1”		
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	Seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.3.8. EncipherOnly	No seleccionado. “0”		
2.3.9. DecipherOnly	No seleccionado. “0”		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.1.3.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	“ https://www.ancert.com/condiciones/CCGNFERNFirmaCentralizada ”		
2.4.2.2. User Notice	“Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNFERNFirmaCentralizada ”		
2.4.3. Policy Identifier	0.4.0.194112.1.0	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí

³¹¹ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

Campo	Contenido	O	C
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		
2.10. Qualified Certificate Statements ³¹²		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.3. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
2.10.4. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
2.10.5. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId-Natural (OID 0.4.0.194121.1.1)	Sí	

³¹² No existe en el perfil actual, pero se propone incorporarlo.

5.2. Certificado de cargo

5.2.1 Certificado de firma

Campo	Contenido	O	C
1. Basic estructura			
1.1. Version	"2" ³¹³	Sí	
1.2. Serial Number	Establecido automáticamente ³¹⁴	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³¹⁵	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.5. Validity	4 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject		Sí	
1.6.1. Country (C)	País	Sí	
1.6.2. Organization (O)	"Consejo General del Notariado"	Sí	
1.6.3. Organizational Unit (OU)	Entidad integrante de la organización notarial	No	
1.6.4. Organizational Unit (OU)	Entidad integrante de la organización notarial	No	
1.6.5. Organizational Unit (OU)	IDCN ³¹⁶	Sí	
1.6.6. Title	Cargo del poseedor de claves + " (Firma)"	Sí	
1.6.7. Surname	Apellidos	Sí	
1.6.8. Given Name	Nombre	Sí	

³¹³ El literal "2" corresponde a la versión 3.

³¹⁴ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³¹⁵ Debe ser el país de establecimiento del prestador del servicio de certificación.

³¹⁶ Identificador de cargo notarial

Campo	Contenido	O	C
1.6.9. Serial Number	NIF	Sí	
1.6.10. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.2.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNCargoFirma"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNCargoFirma"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. CRL Distribution Points		Sí	

Campo	Contenido	O	C
2.7.1. distributionPoint	"http://www.ancert.com/crl/ANCERTFERN_V2.crl"		
2.7.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.7.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8. Authority Information Access		Sí	
2.8.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.8.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		
2.9. Qualified Certificate Statements		Sí	
2.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.9.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

5.2.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³¹⁷	Sí	
1.2. Serial Number	Establecido automáticamente ³¹⁸	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³¹⁹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.5. Validity	4 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject		Sí	
1.6.1. Country (C)	País	Sí	
1.6.2. Organization (O)	"Consejo General del Notariado"	Sí	
1.6.3. Organizational Unit (OU)	Entidad integrante de la organización notarial	No	
1.6.4. Organizational Unit (OU)	Entidad integrante de la organización notarial	No	
1.6.5. Organizational Unit (OU)	IDCN ³²⁰	Sí	
1.6.6. Title	Cargo del poseedor de claves + "(Autentica)"	Sí	
1.6.7. Surname	Apellidos	Sí	
1.6.8. Given Name	Nombre	Sí	
1.6.9. Serial Number	NIF	Sí	
1.6.10. Common Name (CN)	Nombre y apellidos	Sí	

³¹⁷ El literal "2" corresponde a la versión 3.

³¹⁸ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³¹⁹ Debe ser el país de establecimiento del prestador del servicio de certificación.

³²⁰ Identificador de cargo notarial

Campo	Contenido	O	C
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.2.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNCargoAuth"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNCargoAuth"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico	Sí	
2.5.2. UPN	usuario@dominio ³²¹	No	
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		

³²¹ Nombre de usuario en un dominio Windows para aplicaciones de SmartCard Logon.

Campo	Contenido	O	C
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.7.3. smartCardLogon ³²²	Presente	No	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTFERN_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		
2.10. Qualified Certificate Statements		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.11. Certificate Template	SmartcardUser	No	

³²² OID: 1.3.6.1.4.1.311.20.2.2

5.2.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³²³	Sí	
1.2. Serial Number	Establecido automáticamente ³²⁴	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados FERN V2"	Sí	
1.5. Validity	4 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject		Sí	
1.6.1. Country (C)	País	Sí	
1.6.2. Organization (O)	"Consejo General del Notariado"	Sí	
1.6.3. Organizational Unit (OU)	Entidad integrante de la organización notarial	No	
1.6.4. Organizational Unit (OU)	Entidad integrante de la organización notarial	No	
1.6.5. Organizational Unit (OU)	IDCN ³²⁵	Sí	
1.6.6. Title	Cargo del poseedor de claves + " (Cifrado)"	Sí	
1.6.7. Surname	Apellidos	Sí	
1.6.8. Given Name	Nombre	Sí	
1.6.9. Serial Number	NIF	Sí	
1.6.10. Common Name (CN)	Nombre y apellidos	Sí	

³²³ El literal "2" corresponde a la versión 3.

³²⁴ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³²⁵ Identificador de cargo notarial

Campo	Contenido	O	C
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.1.2.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	" https://www.ancert.com/condiciones/CCGNCargoCifra "		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNCargoCifra "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.8. CRL Distribution Points		Sí	

Campo	Contenido	O	C
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTFERN_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTFERN_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTFERN_V2.crt"		

5.2.4 Unidades organizativas y cargos

- Cargos del Consejo General del Notariado³²⁶:
 - o No se utilizan los atributos OU1 y OU2
- Junta directiva de Colegio Notarial:
 - o OU1=Colegio Notarial de <>
 - o OU2=Junta Directiva de Colegio
- Otros cargos dentro del Colegio Notarial:
 - o OU1=Colegio Notarial de <>
 - o No se utiliza el atributo OU2
- Cargos de distrito:
 - o OU1=Colegio Notarial de <>
 - o OU2=Distrito de <>

³²⁶ Esta categoría incluye los certificados de los miembros de la Junta del Consejo, e.g. Presidente, Vicepresidente, Secretario, etc.

5.3. Certificado de empleado/a

5.3.1 Certificado de firma

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³²⁷	Sí	
1.2. Serial Number	Establecido automáticamente ³²⁸	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³²⁹	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados para empleados V2"	Sí	
1.5. Validity	3 o 5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ³³⁰		Sí	
1.6.1. Country (C)	País ³³¹	Sí	
1.6.2. State or Province (ST)	Provincia	Sí	
1.6.3. Locality (L)	Localidad	Sí	
1.6.4. Organization (O)	Notaria o Entidad integrante de la organización colegial notarial	Sí	
1.6.5. Organizational Unit (OU)	Código de notaría o de Entidad integrante de la organización colegial notarial	Sí	
1.6.6. Organizational Unit (OU)	Departamento, cuando resulte procedente	No	

³²⁷ El literal "2" corresponde a la versión 3.

³²⁸ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³²⁹ Debe ser el país de establecimiento del prestador del servicio de certificación.

³³⁰ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³³¹ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.7. Title	Rol o función (cargo) del poseedor de claves + " (Firma)"	Sí	
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	
1.6.10. Serial Number	NIF ³³²	Sí	
1.6.11. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage ³³³		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.2.1.2.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNEFirma"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con		

³³² El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

³³³ Se propone el alineamiento de los bits del campo Key Usage, por consistencia con la política del certificado. De acuerdo con la política, se trata de un certificado de firma reconocida, y el perfil en cambio corresponde a un certificado de autenticación web, lo cual no es consistente.

Campo	Contenido	O	C
	la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNEFirma		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. CRL Distribution Points		Sí	
2.7.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCE_V2.crl"		
2.7.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCE_V2.crl"		
2.7.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCE_V2.crl"		
2.8. Authority Information Access		Sí	
2.8.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.8.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCE_V2.crt"		
2.9. Qualified Certificate Statements ³³⁴		Sí	
2.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.9.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	

³³⁴ No existe en el perfil actual, pero se propone incorporarlo.

5.3.2 Certificado de autenticación

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³³⁵	Sí	
1.2. Serial Number	Establecido automáticamente ³³⁶	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³³⁷	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados para empleados V2"	Sí	
1.5. Validity	3 o 5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ³³⁸		Sí	
1.6.1. Country (C)	País ³³⁹	Sí	
1.6.2. State or Province (ST)	Provincia	Sí	
1.6.3. Locality (L)	Localidad	Sí	
1.6.4. Organization (O)	Notaria o Entidad integrante de la organización colegial notarial	Sí	
1.6.5. Organizational Unit (OU)	Código de notaría o de Entidad integrante de la organización colegial notarial	Sí	
1.6.6. Organizational Unit (OU)	Departamento, cuando resulte procedente	No	
1.6.7. Title	Rol o función (cargo) del poseedor de	Sí	

³³⁵ El literal "2" corresponde a la versión 3.

³³⁶ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³³⁷ Debe ser el país de establecimiento del prestador del servicio de certificación.

³³⁸ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³³⁹ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
	claves + " (Autentica)"		
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	
1.6.10. Serial Number	NIF ³⁴⁰	Sí	
1.6.11. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage ³⁴¹		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.2.1.2.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNEAuth"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en		

³⁴⁰ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

³⁴¹ Se propone el alineamiento de los bits del campo Key Usage, por consistencia con la política del certificado. De acuerdo con la política, se trata de un certificado de firma reconocida, y el perfil en cambio corresponde a un certificado de autenticación web, lo cual no es consistente.

Campo	Contenido	O	C
	https://www.ancert.com/condiciones/CCGNEAuth"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection ³⁴²	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCE_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCE_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCE_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCE_V2.crt"		
2.10. Qualified Certificate Statements ³⁴³		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	

³⁴² No existe en el perfil actual, pero se propone incorporarlo.

³⁴³ No existe en el perfil actual, pero se propone incorporarlo.

5.3.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³⁴⁴	Sí	
1.2. Serial Number	Establecido automáticamente ³⁴⁵	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³⁴⁶	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados para empleados V2"	Sí	
1.5. Validity	3 o 5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ³⁴⁷		Sí	
1.6.1. Country (C)	País ³⁴⁸	Sí	
1.6.2. State or Province (ST)	Provincia	Sí	
1.6.3. Locality (L)	Localidad	Sí	
1.6.4. Organization (O)	Notaria o Entidad integrante de la organización colegial notarial	Sí	
1.6.5. Organizational Unit (OU)	Código de notaría o de Entidad integrante de la organización colegial notarial	Sí	
1.6.6. Organizational Unit (OU)	Departamento, cuando resulte procedente	No	

³⁴⁴ El literal "2" corresponde a la versión 3.

³⁴⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁴⁶ Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁴⁷ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³⁴⁸ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.7. Title	Rol o función (cargo) del poseedor de claves + " (Cifrado)"	Sí	
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	
1.6.10. Serial Number	NIF ³⁴⁹	Sí	
1.6.11. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage ³⁵⁰		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	Seleccionado. "1"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.2.1.2.3		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNECifra"		

³⁴⁹ El campo "número de serie" debe incluir el NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

³⁵⁰ Se propone el alineamiento de los bits del campo Key Usage, por consistencia con la política del certificado. De acuerdo con la política, se trata de un certificado de firma reconocida, y el perfil en cambio corresponde a un certificado de autenticación web, lo cual no es consistente.

Campo	Contenido	O	C
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNECifra "		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection ³⁵¹	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	" http://www.ancert.com/crl/ANCERTCE_V2.crl "		
2.8.2. distributionPoint	" http://www2.ancert.com/crl/ANCERTCE_V2.crl "		
2.8.3. distributionPoint	" http://www3.ancert.com/crl/ANCERTCE_V2.crl "		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	" http://ocsp.ac.ancert.com/ocsp.xuda "		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	" http://www.ancert.com/pki/v2/certs/ANCERTCE_V2.crt "		

³⁵¹ No existe en el perfil actual, pero se propone incorporarlo.

5.3.4 Certificado de firma (sin garantía de dispositivo seguro)

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³⁵²	Sí	
1.2. Serial Number	Establecido automáticamente ³⁵³	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³⁵⁴	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados para empleados V2"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ³⁵⁵		Sí	
1.6.1. Country (C)	País ³⁵⁶	Sí	
1.6.2. State or Province (ST)	Provincia	No	
1.6.3. Locality (L)	Localidad	No	
1.6.4. Organization (O)	Notaria o Entidad integrante de la organización colegial notarial ³⁵⁷	Sí	
1.6.5. Organizational Unit (OU)	Código de notaría o de Entidad integrante de la organización colegial notarial ³⁵⁸	Sí	

³⁵² El literal "2" corresponde a la versión 3.

³⁵³ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁵⁴ Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁵⁵ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³⁵⁶ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

³⁵⁷ Para los certificados de empleados de notaría que no lleven información de la notaría el campo Organización contendrá el literal "Consejo General del Notariado".

³⁵⁸ Para los certificados de empleados de notaría que no lleven información de la notaría el campo Unidad Organizativa contendrá el literal "Personal de Notaría".

Campo	Contenido	O	C
1.6.6. Organizational Unit (OU)	Departamento, cuando resulte procedente	No	
1.6.7. Title	Rol o función (cargo) del poseedor de claves	No	
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	
1.6.10. Serial Number	IDCES-NIF ³⁵⁹	Sí	
1.6.11. Common Name (CN)	Nombre y primer apellido Nombre y primer apellido + “ (código notaria)”	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage ³⁶⁰		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”		
2.3.2. Content Commitment	Seleccionado. “1”		
2.3.3. Key Encipherment	Seleccionado. “1”		
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	Seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.3.8. EncipherOnly	No seleccionado. “0”		
2.3.9. DecipherOnly	No seleccionado. “0”		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.2.1.2.4		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	“https://www.ancert.com/condicione		

³⁵⁹ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

³⁶⁰ Se propone el alineamiento de los bits del campo Key Usage, por consistencia con la política del certificado. De acuerdo con la política, se trata de un certificado de firma reconocida, y el perfil en cambio corresponde a un certificado de autenticación web, lo cual no es consistente.

Campo	Contenido	O	C
	s/CCGNESoft"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en https://www.ancert.com/condiciones / CCGNESoft "		
2.4.3. Policy Identifier	0.4.0.194112.1.0	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	" http://www.ancert.com/crl/ANCERTCE_V2.crl "		
2.8.2. distributionPoint	" http://www2.ancert.com/crl/ANCERTCE_V2.crl "		
2.8.3. distributionPoint	" http://www3.ancert.com/crl/ANCERTCE_V2.crl "		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	" http://ocsp.ac.ancert.com/ocsp.xuda "		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	" http://www.ancert.com/pki/v2/certs/ANCERTCE_V2.crt "		
2.10. Qualified Certificate Statements ³⁶¹		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.3. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	

³⁶¹ No existe en el perfil actual, pero se propone incorporarlo.

Campo	Contenido	O	C
2.10.4. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
2.10.5. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId-Natural (OID 0.4.0.194121.1.1)	Sí	

5.3.5 Certificado de firma remota cualificada

Campo	Contenido	O	C
1. Basic structure			
1.1. Version	"2" ³⁶²	Sí	
1.2. Serial Number	Establecido automáticamente ³⁶³	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³⁶⁴	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados para empleados V2"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ³⁶⁵		Sí	
1.6.1. Country (C)	País ³⁶⁶	Sí	
1.6.2. State or Province (ST)	Provincia	No	
1.6.3. Locality (L)	Localidad	No	
1.6.4. Organization (O)	Notaria o Entidad integrante de la organización colegial notarial	Sí	
1.6.5. Organizational Unit (OU)	Código de notaría o de Entidad integrante de la organización colegial notarial	No	
1.6.6. Organizational Unit (OU)	Departamento, cuando resulte procedente	No	
1.6.7. Title	Rol o función (cargo) del poseedor de claves	Sí	

³⁶² El literal "2" corresponde a la versión 3.

³⁶³ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁶⁴ Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁶⁵ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³⁶⁶ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	
1.6.10. Serial Number	IDCES-NIF ³⁶⁷	Sí	
1.6.11. Common Name (CN)	Nombre y primer apellido + "(rQSCD)" Nombre y primer apellido + " (código notaría)" + "(rQSCD)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage ³⁶⁸		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.2.1.3.1		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNEFirmaCentralizada"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en		

³⁶⁷ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

³⁶⁸ Se propone el alineamiento de los bits del campo Key Usage, por consistencia con la política del certificado. De acuerdo con la política, se trata de un certificado de firma reconocida, y el perfil en cambio corresponde a un certificado de autenticación web, lo cual no es consistente.

Campo	Contenido	O	C
	https://www.ancert.com/condiciones/CCGNEFirmaCentralizada		
2.4.3. Policy Identifier	0.4.0.194112.1.2	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. CRL Distribution Points		Sí	
2.7.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCE_V2.crl"		
2.7.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCE_V2.crl"		
2.7.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCE_V2.crl"		
2.8. Authority Information Access		Sí	
2.8.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.8.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCE_V2.crt"		
2.9. Qualified Certificate Statements ³⁶⁹		Sí	
2.9.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.9.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.9.3. QcSSCD (OID 0.4.0.1862.1.4)	Presente	Sí	
2.9.4. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
2.9.5. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
2.9.6. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (OID 0.4.0.194121.1.1)	Sí	

³⁶⁹ No existe en el perfil actual, pero se propone incorporarlo.

5.3.6 Certificado de firma remota

Campo	Contenido	O	C
1. Basic estructura			
1.1. Version	"2" ³⁷⁰	Sí	
1.2. Serial Number	Establecido automáticamente ³⁷¹	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES" ³⁷²	Sí	
1.4.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.4.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Certificados para empleados V2"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez		
1.5.2. Not After	Fecha de expiración		
1.6. Subject ³⁷³		Sí	
1.6.1. Country (C)	País ³⁷⁴	Sí	
1.6.2. State or Province (ST)	Provincia	No	
1.6.3. Locality (L)	Localidad	No	
1.6.4. Organization (O)	Notaria o Entidad integrante de la organización colegial notarial	Sí	
1.6.5. Organizational Unit (OU)	Código de notaría o de Entidad integrante de la organización colegial notarial	No	
1.6.6. Organizational Unit (OU)	Departamento, cuando resulte procedente	No	
1.6.7. Title	Rol o función (cargo) del poseedor de claves	Sí	

³⁷⁰ El literal "2" corresponde a la versión 3.

³⁷¹ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁷² Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁷³ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

³⁷⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
1.6.8. Surname	Apellidos	Sí	
1.6.9. Given Name	Nombre	Sí	
1.6.10. Serial Number	IDCES-NIF ³⁷⁵	Sí	
1.6.11. Common Name (CN)	Nombre y primer apellido + "(rSCD)" Nombre y primer apellido + " (código notaría)" + "(rSCD)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage ³⁷⁶		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	Seleccionado. "1"		
2.3.3. Key Encipherment	Seleccionado. "1"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	Seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	ANCERT.4.2.1.3.2		
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNEFirmaCentralizada"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislación vigente. Condiciones de uso en		

³⁷⁵ Utilizando la semántica propuesta por la norma ETSI EN319 412-1.

³⁷⁶ Se propone el alineamiento de los bits del campo Key Usage, por consistencia con la política del certificado. De acuerdo con la política, se trata de un certificado de firma reconocida, y el perfil en cambio corresponde a un certificado de autenticación web, lo cual no es consistente.

Campo	Contenido	O	C
	https://www.ancert.com/condiciones/CCGNEFirmaCentralizada		
2.4.3. Policy Identifier	0.4.0.194112.1.0	Sí	
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		
2.6. Basic Constraints		Sí	Sí
2.6.1. CA	Falso		
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. CRL Distribution Points		Sí	
2.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCE_V2.crl"		
2.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCE_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCE_V2.crl"		
2.9. Authority Information Access		Sí	
2.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
2.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCE_V2.crt"		
2.10. Qualified Certificate Statements ³⁷⁷		Sí	
2.10.1. QcCompliance (OID 0.4.0.1862.1.1)	Presente	Sí	
2.10.2. QcEuRetentionPeriod (OID 0.4.0.1862.1.3)	Periodo de conservación de informaciones (12 años)	Sí	
2.10.3. QcPDS (OID 0.4.0.1862.1.5)	http://www.ancert.com/cps (EN)	Sí	
2.10.4. QcType (OID 0.4.0.1862.1.6)	id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)	Sí	
2.10.5. QcSyntaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId-Natural (OID 0.4.0.194121.1.1)	Sí	

³⁷⁷ No existe en el perfil actual, pero se propone incorporarlo.

6. Atributos propios de ANCERT

Los siguientes atributos son empleados en los certificados de ANCERT, en la extensión Subject Directory Attributes.

6.1. Atributo "Nivel de apoderamiento": ANCERT.10.1.1

Corresponde al nivel de garantía en relación con el apoderamiento, indicando también la ausencia de garantía con respecto a los poderes de una persona física. Sustituye a la extensión ANCERT.10.1.1 anterior.

El atributo contiene un OBJECT STRING, que deberá ser codificado en UTF8String. Contiene una cadena de texto tasado, con las siguientes posibilidades:

- "Sin garantía de poderes", que se emplea para indicar que el certificado se emite sin haber comprobado si la persona tiene algún poder de actuación.
- "Poderes limitados", que se emplea para indicar que el certificado se emite habiendo comprobado que la persona tiene algún poder de actuación. En este caso, debe acudir al atributo ANCERT.10.1.5 sobre límite de uso, que incorpora por referencia los poderes.
- "Poderes generales", que se emplea para indicar que el certificado se emite habiendo comprobado que la persona tiene todos los poderes generales de actuación, bien por ser un representante legal u orgánico, o por ser un representante voluntario con poderes generales de actuación.

Este atributo se complementa con el atributo Title, en el que se puede incluir la posición o cargo de la persona dentro de la organización (por ejemplo, "Director general"), debiendo ser ambos atributos consistentes.

Estas opciones sustituyen las actualmente empleadas, que hasta la fecha son:

- "Apoderado general", en todos los certificados de representación.
- "Apoderado mercantil", en todos los certificados de representación.
- "Cargo fundacional", en certificados notariales corporativos de representación³⁷⁸.
- "Gran empresa"³⁷⁹, en certificados notariales corporativos y corporativos de representación.

Entendemos que el lugar apropiado para indicar estas opciones (con excepción de "Gran empresa", que no indica una clase de apoderamiento, sino más bien una clase registrada de

³⁷⁸ Así se indica en la página web de ANCERT, pero no aparece mencionado ni en las políticas ni en la Declaración de Prácticas de Certificación.

³⁷⁹ No se ha encontrado ningún modelo de poderes de grandes empresas en la web de ANCERT, a pesar de que la política lo establece como necesario.

semántica para el procesamiento de las informaciones contenidas en el certificado), y otras similares, como "Representante" o "Tutor" es el atributo Title.

6.2. Atributo "Documento de representación": ANCERT.10.1.3

Corresponde al nombre y apellidos del Notario autorizante del documento de representación, así como número y año del protocolo correspondiente, en caso de poder notarial; o a la Entidad u Órgano otorgante, en caso de que la representación no derive de un poder notarial.

El atributo contiene un OBJECT STRING, que deberá ser codificado en UTF8String. Contiene una cadena de texto libre, con las anteriores informaciones.

6.3. Atributo "Otras circunstancias personales": ANCERT.10.1.4

Corresponde a los atributos específicos de los suscriptores de los certificados, diferentes de los atributos ya definidos, como Title.

El atributo contiene una secuencia de OBJECT STRING, que deberá ser codificado en UTF8String. Cada OBJECT STRING contiene una cadena de texto libre, con un atributo adicional del suscriptor.

6.4. Atributo "Límite de uso por razón de la materia": ANCERT.10.1.5

Este atributo debe emplearse cuando en el atributo ANCERT.10.1.1 se contiene la clase de apoderamiento "Poderes limitados".

Corresponde a cualquier límite de uso del certificado (se entiende que diferente del límite de cuantía), expresado como una URL que contiene la lista de los poderes / facultades de que dispone el representante.

6.5. Atributo "Datos registrales de la representación": ANCERT.10.1.6

Corresponde a los datos referentes a la inscripción de la escritura pública o actuación judicial del nombramiento del representante, inscrita en el registro jurídico o administrativo correspondiente a la persona física o jurídica, cuando la misma sea obligatoria.

El atributo contiene un OBJECT STRING, que deberá ser codificado en UTF8String. Contiene una cadena de texto libre, con las anteriores informaciones.

6.6. Atributo "Persona representada": ANCERT.10.1.7

Corresponde a los datos referentes a la persona representada, en certificados personales o corporativos de representación. Se ha optado por establecer estos datos en un atributo propio tanto para personas físicas como jurídicas para simplificar la semántica del Subject Name, que actualmente resulta demasiado compleja.

En el caso de los certificados corporativos de representación, existe un cierto solapamiento de informaciones, dado que parte de los datos de la persona jurídica ya forman parte del Subject Name. Aunque esto es cierto, se ha optado por unificar en esta extensión la semántica completa de la persona representada por diversos motivos:

- Disponer de toda la información en un atributo facilita el procesamiento por los destinatarios.
- La semántica se puede definir con independencia de las restricciones legales impuestas para el campo Subject Name por la AEAT, algo que resulta interesante con respecto a la indicación, por ejemplo, del país.
- Pueden existir casos en que interese que una persona que dispone de un certificado emitido al suscriptor corporativo A pueda incluir su representación de una persona jurídica B que no es suscriptora del certificado (por ejemplo, dentro de grupos de sociedades). Actualmente la política indica que en certificados notariales corporativos de representación la persona jurídica representada sea obligatoriamente la suscriptora del certificado, pero no resulta imprescindible que sea de esta forma, si existen determinados controles adicionales.
- Finalmente, este atributo permitiría la creación, caso que se estime oportuno, de un certificado notarial personal de representación corporativa, donde el suscriptor sería la persona física, que en este caso alegraría sencillamente la representación, incluso sin conocimiento de la persona jurídica representada³⁸⁰.

No se considera apropiada la inclusión de este atributo en los certificados notariales corporativos, dado que en términos legales no son certificados de representación.

El atributo contiene una secuencia de uno o más atributos "representado", permitiendo que un único certificado manifieste más de una representación - la persona jurídica actúa como firmante, en términos de la exposición de motivos de la Ley 59/2003.

El atributo "Persona representada", con OID ANCERT.10.7 contiene un Name formado por una combinación de los siguientes componentes.

Cuando el representado es una persona física:

- Country (PrintableString)
- Surname (UTF8String)
- Given Name (UTF8String)
- Serial Number (PrintableString)

³⁸⁰ Esta opción resulta muy similar a la que actualmente tiene vigente ANCERT para los certificados notariales corporativos de representación, en cuanto al procedimiento. La diferencia entre ambos certificados es la actuación y responsabilidad de la persona jurídica: en el caso del certificado notarial corporativo de representación, la garantía de validez de la representación es ofrecida de forma continuada durante toda la vida del certificado, mientras que en el caso de un hipotético certificado notarial personal de representación corporativa, la garantía queda limitada a la veracidad de la información en el momento de la expedición del certificado, dado que el suscriptor no tiene por qué conocer acerca de la existencia del certificado.

Cuando el representado es una persona jurídica:

- Country (PrintableString)
- Organization (UTF8String)
- Serial Number (PrintableString)

7. Certificados de infraestructura

7.1. Certificado de OCSP responder

7.1.1 Perfil propuesto

Campo	Contenido	O	C
2. Basic estructura			
1.8. Version	"2" ³⁸¹	Sí	
1.9. Serial Number	Establecido automáticamente ³⁸²	Sí	
1.10. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.11. Issuer Distinguished Name		Sí	
1.11.1. Country (C)	"ES" ³⁸³	Sí	
1.11.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
1.11.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
1.11.4. Common Name (CN)	Common Name de la CA emisora	Sí	
1.12. Validity	14 meses	Sí	
1.12.1. Not Before	Fecha de inicio de validez		
1.12.2. Not After	Fecha de expiración		
1.13. Subject		Sí	
1.13.1. Country (C)	País ³⁸⁴	Sí	
1.13.2. Organization (O)	Agencia Notarial de Certificación S.L. Unipersonal	Sí	
1.13.3. Organizational Unit (OU)	OCSP	Sí	
1.13.4. Organizatin Identifier	VATES-B83395988	Sí	
1.13.5. Common Name (CN)	Common Name de la CA emisora	Sí	
1.14. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			

³⁸¹ El literal "2" corresponde a la versión 3.

³⁸² No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁸³ Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁸⁴ El campo "país" será el de nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166.

Campo	Contenido	O	C
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier	Presente	Sí	
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"		
2.3.2. Content Commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. EncipherOnly	No seleccionado. "0"		
2.3.9. DecipherOnly	No seleccionado. "0"		
2.4. Basic Constraints		Sí	Sí
2.4.1. CA	Falso		
2.5. Extended Key Usage		Sí	Sí
2.5.1. OCSPSigning	Presente		
2.6. OID: 1.3.6.1.5.5.7.48.1.5 ³⁸⁵	NULL	Sí	
2.7. Private Key Usage Period		No	
2.7.1. Not Before			
2.7.2. Not After			

³⁸⁵ Indica que el estado de revocación del certificado de OCSP no se verifica.

7.2. Certificado de Autoridad de Sellado de tiempo Cualificada

7.2.1 Perfil propuesto

Campo	Contenido	O	C
2. Basic structure			
2.12. Version	"2" ³⁸⁶	Sí	
2.13. Serial Number	Establecido automáticamente ³⁸⁷	Sí	
2.14. Signature Algorithm	SHA-256 with RSA Signature	Sí	
2.15. Issuer Distinguished Name		Sí	
2.15.1. Country (C)	"ES" ³⁸⁸	Sí	
2.15.2. Locality (L)	"Paseo del General Martinez Campos 46 6a planta 28010 Madrid"	Sí	
2.15.3. Organization (O)	"Agencia Notarial de Certificacion S.L.U. - CIF B83395988"	Sí	
2.15.4. Common Name (CN)	"ANCERT Certificados Notariales de Sistemas V2"	Sí	
2.16. Validity	6 años	Sí	
2.16.1. Not Before	Fecha de inicio de validez		
2.16.2. Not After	Fecha de expiración		
2.17. Subject ³⁸⁹		Sí	
2.17.1. Country (C)	ES	Sí	
2.17.2. Organization (O)	"Agencia Notarial de Certificación S.L. Unipersonal"	Sí	
2.17.3. Organization Identifier	VATES-B83395988	Sí	
2.17.4. Common Name (CN)	Nombre de la autoridad de sellado de tiempo	Sí	
2.18. Subject Public Key Info	3072-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
3. Extensions			
3.1. Authority Key Identifier	Presente	Sí	
3.1.1. Key Identifier	Presente	Sí	

³⁸⁶ El literal "2" corresponde a la versión 3.

³⁸⁷ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁸⁸ Debe ser el país de establecimiento del prestador del servicio de certificación.

³⁸⁹ Se elimina el componente EA del subject name, dado que debe aparecer en el campo Subject Alternative Name.

Campo	Contenido	O	C
3.2. Subject Key Identifier	Presente	Sí	
3.3. Key Usage		Sí	Sí
3.3.1. Digital Signature	Seleccionado. "1"		
3.3.2. Content Commitment	No seleccionado. "0"		
3.3.3. Key Encipherment	No seleccionado. "0"		
3.3.4. Data Encipherment	No seleccionado. "0"		
3.3.5. Key Agreement	No seleccionado. "0"		
3.3.6. Key Certificate Signature	No seleccionado. "0"		
3.3.7. CRL Signature	No seleccionado. "0"		
3.3.8. EncipherOnly	No seleccionado. "0"		
3.3.9. DecipherOnly	No seleccionado. "0"		
3.4. Certificate Policies		Sí	
3.4.1. Policy Identifier	ANCERT.1.2.3.3.1		
3.5. Subject Alternative Names		Sí	
3.5.1. rfc822Name	Correo electrónico		
3.6. Basic Constraints		Sí	Sí
3.6.1. CA	Falso		
3.7. Extended Key Usage		Sí	Sí ³⁹⁰
3.7.1. timeStamping	Presente		
3.8. CRL Distribution Points		Sí	
3.8.1. distributionPoint	"http://www.ancert.com/crl/ANCERTCS_V2.crl"		
3.8.2. distributionPoint	"http://www2.ancert.com/crl/ANCERTCS_V2.crl"		
3.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCS_V2.crl"		
3.9. Authority Information Access		Sí	
3.9.1. Access Method (1.3.6.1.5.5.7.48.1)	"http://ocsp.ac.ancert.com/ocsp.xuda"		
3.9.2. Access Method (1.3.6.1.5.5.7.48.2)	"http://www.ancert.com/pki/v2/certs/ANCERTCS_V2.crt"		

³⁹⁰ Impuesto por IETF RFC 3161.

Campo	Contenido	O	C
3.10. Subject Information Access ³⁹¹		No	
3.10.1. Access Method	OID para TimeStamping		
3.10.2. Access Location	Dirección HTTP/FTP de prestación del servicio de fecha de tiempo		
3.11. Private Key Usage Period	Periodo máximo de uso de la clave.	No	
3.11.1. Not Before	Fecha de inicio de validez		
3.11.2. Not After	Fecha de fin de validez (5 años)		

³⁹¹ Tantos como métodos de acceso se emplean para los protocolos de la TSA.

8. Restricciones de los certificados

8.1. Componentes de los nombres de emisor y suscriptor

De acuerdo con el Anexo C de la Recomendación ITU-T X.520, la Recomendación ITU-T X.509 y el RFC 5280, aplicable a los componentes que forman los nombres diferenciados en directorios y, por tanto, en certificados X.509, se recomienda no superar las siguientes longitudes:

Componente	ITU-T X.520	ITU-T X.509	RFC 5280
Common Name	64	64	64
Country Name	2	2	2
Locality Name	64	128	128
Given Name	64	64	16
Surname	64	64	40
Organization Name	64	64	64
Organizational Unit Name	64	32	32
Serial Number	64	64	64
StateOrProvince Name	64	128	128
Description	1024	N/D	N/D

Para los Certificados Notariales de Sistemas las longitudes no deberán superar las recomendaciones definidas en el RFC 5280.

Para el resto de perfiles se recomienda no superar las longitudes definidas en la Recomendación ITU-T X.509 o en caso de no estar establecido un límite las de ITU-T X.520 para evitar problemas de interoperabilidad.

En perfiles específicos se permite superar estas longitudes en determinados componentes para que los nombres puedan coincidir con los que constan en documentos identificativos oficiales.

8.2. Extensión de políticas de certificados

El componente User Notice debe tener un tamaño máximo de 200 caracteres.

8.3. Reglas de nomenclatura

Para todos los perfiles de entidad final se seguirá la siguiente regla de nomenclatura:

- Información fija (es decir, literales prefijados o datos no introducidos directamente en los formularios de emisión o recuperados de la BBDD corporativa): caracteres en minúsculas capitalizadas y con signos de puntuación (acentos, diéresis, etc..)³⁹²
- Información variable: caracteres en mayúsculas y con signos de puntuación.

Para las entidades intermedias y raíces, por motivos de compatibilidad con los sistemas usuales para su tratamiento (servidores web, etc...) se mantienen los literales de las CAs antiguas con el sufijo "V2".

8.4. Uso de SHA2RSA como algoritmo de firma

A partir de la fecha efectiva de la publicación de la versión 3.1 de este documento de perfiles SHA256RSA es el algoritmo de firma por defecto para todos los certificados que emiten las Cas subordinadas de ANCERT. Con anterioridad a la versión 3.1 el algoritmo de firma por defecto ha sido SHA1RSA.

³⁹² A efectos de esta regla, también se considera parte fija toda parte no variable de un literal que pudiera incorporar partes variables.