PÚBLICO

Perfiles de Certificados de la Entidad de Certificación

CENTRO TECNOLÓGICO DEL NOTARIADO

Información general

Control documental

Proyecto:	Perfiles de Certificados de la Entidad de Certificación
Entidad de destino:	Agencia Notarial de Certificación, S.L.U.
Versión:	4.0
Estado:	Aprobado
Confidencialidad:	Público
Fecha de la edición:	06/05/2024
Fecha de aprobación:	11/06/2024
Fecha de publicación:	13/06/2024
Archivo:	Perfiles_Certificados_ANCERT_2024.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 CountryOfCiticenship	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 Servidor Seguro	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 SubjectAlternativeNames.	16/03/2015	17/06/2015
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 Corporativode 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 Corporativode 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	Certifcado 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 Actualización de referencias	14/12/2020	08/04/2021

3.8	Certificado de servidor seguro Todos los perfiles	Periodo de validez de 397 días Actualización de referencias	24/02/2022	
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 certififcados de firma electrónica para ciudadanos en la Sede Electrónica Notarial	06/02/2023	
4.0	Todos los perfiles	Revisión de longitudes de claves RSA para permitir tamaños de clave superiores a 2048 bits en los ceritifcados de entidad final. Actualización de referencias	06/05/2024	13/06/2024

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 v2.3.1 Certificate Profiles Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 v1.3.1 Certificate Profiles Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-4 v1.3.1 Certificate Profiles Part 4: Certificate profile for web site certificates issued to organisations
- ETSI EN 319 412-5 v2.4.1 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 v2.0.5.
- Política de certificación del Consejo General del Notariado de España.

Índice

1. Introducción

Este documento recoge los perfiles de certificados que expedirá la Agencia Notarial de Certificación S.L.Unipersonal (Centro Tecnológico del Notariado, ANCERT o CTNotariado indistintamente), 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 siguientes[1]:

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

[1] Se ha optado por emplear el último arco del OID de cada política para señalizar 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 aplicación segura (sin dispositivo seguro)	ANCERT.1.2.6.1.2
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 estructure			
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 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[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 o 3072 o 4096 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 legislacion 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	

[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
2.6.1. 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
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/ANCERTCP_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCP_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/ANCERTCP_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 estructure			
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 o 3072 o 4096 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 legislacion 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	

Campo	**Contenido**	**O**	**C**
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		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 estructure			
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 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[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 o 3072 o 4096 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 legislacion 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	

Campo	Contenido	O	C
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 (1.3.6.1.5.5.7.48.1)	"http://www.ancert.com/pki/v2/certs/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 estructure			
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 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[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 o 3072 o 4096 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 legislacion vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNPRPFirma"		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		

[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. Subject Directory Attributes		Sí	
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/ANCERTCP_V2.crl"		
2.8.3. distributionPoint	"http://www3.ancert.com/crl/ANCERTCP_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/ANCERTCP_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 estructure			
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 o 3072 o 4096 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 legislacion 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 estructure			
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 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[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 o 3072 o 4096 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 legislacion 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 estructure			
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 o 4096 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 legislacion 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. QcSytaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-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 estructure			
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)	Província	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 o 3072 o 4096 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 contentener 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_V2crl”		
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 estructure			
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 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[65]		Sí	
1.6.1. Country (C)	País[66]	Sí	
1.6.2. StateOrProvince (ST)	Província	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 o 3072 o 4096 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 contentener 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 estructure			
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 Certificacion 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	3072 o 4096 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 estructure			
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 Certificacion 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	3072 o 4096 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 estructure			
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 Certificacion 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	3072 o 4096 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 estructure			
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 Certificacion 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	3072 o 4096 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/CNSFCSoft"		
2.4.2.2. User Notice[101]	"Este certificado se expide de acuerdo con las condiciones de uso en https://www.ancert.com/condiciones/CNSFCSoft"		
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 estructure			
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 Certificacion 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 o 3072 o 4096 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		

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

Campo	Contenido	O	C
	/CNASHard"		
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 estructure			
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 Certificacion 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 o 3072 o 4096 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 estructure			
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 Certificacion 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 o 3072 o 4096 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 estructure			
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 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[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 legislacion 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 estructure			
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 legislacion 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 estructure			
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 legislacion 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 estructure			
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 o 3072 o 4096 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 legislacion vigente. Condiciones de uso en https://www.ancert.com/condiciones		

[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
	/CNCRFirma"		
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	

[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. QcEuLimitValue (OID 0.4.0.1862.1.2)		No[158]	
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 estructure			
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 o 3072 o 4096 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 legislacion 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 estructure			
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 o 3072 o 4096 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/CNCRCifra"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Reconocido de acuerdo con la legislacion vigente. Condiciones de uso en https://www.ancert.com/condiciones/CNCRCifra"		
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 estructure			
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 o 3072 o 4096 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			

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

Campo	Contenido	O	C
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CNCRFirma"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislacion 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. QcSytaxV2 (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 estructure			
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 o 3072 o 4096 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"		

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

Campo	Contenido	O	C
2.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislacion 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**	**Longitud[191]**
NIF	Número DNI/NIE del representate	10
Nombre	Nombre del representate tal y como fiugura en el DNI / NIE	4
Apellido 1	Primer apellido del representate tal y como fiugura 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 estructure			
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 o 3072 o 4096 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 estructure			
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 Certificacion 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 o 3072 o 4096 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

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/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. QcSytaxV2 (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 estructure			
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 Certificacion 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 o 3072 o 4096 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

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/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. QcSytaxV2 (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 estructure			
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 Certificacion 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 o 4096 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 legislacion 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. QcSytaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-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 estructure			
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 o 3072 o 4096 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 garantia 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 estructure			
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 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[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 (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[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 o 3072 o 4096 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/CCPAuth”		
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 garantia 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	

Campo	Contenido	O	C
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"		

3.1.3 Certificado de cifrado

Campo	Contenido	O	C
1. Basic estructure			
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 o 3072 o 4096 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 garantia 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	

Campo	Contenido	O	C
2.8.1. emailProtection	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"		

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

3.2.1 Perfil propuesto

Campo	Contenido	O	C
1. Basic estructure			
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 o 3072 o 4096 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 garantia 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 estructure			
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 o 3072 o 4096 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		

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/ANCERTCCS_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/certs/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 estructure			
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 o 3072 o 4096 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	

Campo	Contenido	O	C
3.6. Basic Constraints		Sí	Sí
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/ANCERTCCS_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/certs/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 estructure			
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 o 3072 o 4096 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	

[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
2.6.1. ANCERT.10.1.1	"Sin garantia 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. 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 estructure			
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 o 3072 o 4096 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 garantia 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	

Campo	Contenido	O	C
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/ 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 estructure			
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 o 3072 o 4096 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 garantia 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	

Campo	Contenido	O	C
2.8.1. emailProtection	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"		

4.2. 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 estructure			
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 Certificacion S.L.U. - CIF B83395988"	Sí	
1.4.4. Common Name (CN)	"ANCERT Corporaciones de Derecho Publico 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 o 3072 o 4096 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 estructure			
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 o 3072 o 4096 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 legislacion vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNFERNFirma”		

[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. 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/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 Certifcado de autenticacón

Campo	Contenido	O	C
1. Basic estructure			
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 o 3072 o 4096 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 legislacion 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

[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
2.6.1. 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"		
2.8.3. 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 Certficado de cifrado

Campo	Contenido	O	C
1. Basic estructure			
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 o 3072 o 4096 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 legislacion vigente. Condiciones de uso en https://www.ancert.com/condiciones/CCGNFERNCifra”		
2.5. Subject Alternative Names		Sí	
2.5.1. rfc822Name	Correo electrónico		

[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. 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	
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 estructure			
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 o 4096 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 legislacion 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/ANCERTFERN_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. QcSytaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-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 estructure			
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 o 4096 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 legislacion 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. QcSytaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-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 estructure			
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 o 3072 o 4096 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 legislacion 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 estructure			
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 o 3072 o 4096 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 legislacion 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 estructure			
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 o 3072 o 4096 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 legislacion 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 Notariado[326]:
  - No se utilizan los atributos OU1 y OU2
- Junta directiva de Colegio Notarial:
  - OU1=Colegio Notarial de <>
  - OU2=Junta Directiva de Colegio
- Otros cargos dentro del Colegio Notarial:
  - OU1=Colegio Notarial de <>
  - No se utiliza el atributo OU2
- Cargos de distrito:
  - OU1=Colegio Notarial de <>
  - 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 estructure			
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 o 3072 o 4096 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		

[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
	Certificado Reconocido de acuerdo con la legislacion 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 estructure			
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 o 3072 o 4096 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 legislacion vigente. Condiciones de		

[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
	uso en 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 estructure			
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 o 3072 o 4096 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 legislacion 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 estructure			
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 Oranizativa 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 o 3072 o 4096 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			

[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
2.4.2.1. CPS Pointer	"https://www.ancert.com/condiciones/CCGNESoft"		
2.4.2.2. User Notice	"Este certificado se expide como Certificado Cualificado de acuerdo con la legislacion 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. QcSytaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (OID 0.4.0.194121.1.1)	Sí	

5.3.5 Certificado de firma remota cualificada

Campo	Contenido	O	C
1. Basic estructure			
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 o 4096 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 legislacion 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. QcSytaxV2 (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 estructure			
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 o 4096 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 legislacion 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. QcSytaxV2 (OID 1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-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 garantia 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 acudirse 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 representación[378].
- "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 ls 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 atribito 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 alegaría sencillamente la representación, incluso sin conocimiento de la persona jurídica representada[380].

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 actua 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 porqué 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 estructure			
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 o 3072 o 4096 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 estructure			
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 fín 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 recominda 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.