Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DIGITALES E INNOVACIÓN
DEPARTAMENTO CERES

DEFINICIÓN PERFILES DE CERTIFICADOS DE SELLOS ELECTRÓNICOS

Referencia:

Documento clasificado como: *Público*

1. INTRODUCCIÓN

El presente documento describe en detalle los perfiles de los distintos tipos de certificado de sello electrónico y sello de Entidad que emiten desde las siguientes Autoridades de Certificación: "AC Representación", "AC Sector Público" y "*AC Entidades G2*".

2. PERFIL DEL CERTIFICADO DE AC ENTIDADES G2

Campo	Contenido	Obligatorio	Criticidad	Descripción
1. Versión	2	Si		Integer:= 2 [RFC5280] Identifica la versión del certificado. El valor 2 equivale a decir que el certificado es versión 3 (X509v3)
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si		Integer. SerialNumber = ej: 111222. Número de identificación del certificado establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2159).
3. Signature Algorithm	ecdsa-with-SHA384	Si		String. Algoritmo utilizado para la encriptación OID: 1.2.840.10045.4.3.3
4. Issuer Distinguish Name	Autoridad de Certificación emisora del certificado	Si		Los valores del Issuer debe ser exactamente igual al Subject de la AC Raíz.
4.1. Country	C=ES	Si		PrintableString, tamaño 2 (rfc5280). Codificación del país de acuerdo con la ISO 3166. En el caso de España "ES" Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
4.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Si		UTF8 String, tamaño máximo 64 (rfc5280)
4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J			UTF8 String, tamaño máximo 64 (X520). Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) - 3 caracteres para indicar el tipo legal de identificador (VAT= documento de identificación fiscal) - 2 caracteres para identificar el país ISO 3166-1 [2]

Campo		Contenido	Obligatorio	Criticidad	Descripción
					- 1 carácter "-" 0x2D (ASCII), U+002D (UTF-8)
	4.4. Common Name	CA del prestador de servicios de confianza bajo la cual se generar el certificado electrónico cn= AC RAIZ FNMT-RCM G2	Si		UTF8 String, tamaño máximo 64 (rfc5280).
5. Validity		15 años	Si		String Validez del certificado electrónico
	5.1. Not before	UTCTime YYMMDDHHMMSSZ	Si		Fecha desde la que es válida el certificado
	5.2. Not after	UTCTime YYMMDDHHMMSSZ	Si		Fecha hasta la que es válida el certificado
6. Subject			Si		Identificación del titular asociado a la clave pública
	6.1. Country	C=ES	Si		PrintableString, tamaño 2 (rfc5280). Codificación del país de acuerdo con la ISO 3166. En el caso de España "ES" Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
	6.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Si		UTF8 String, tamaño máximo 64 (rfc5280)
	6.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J			UTF8 String, tamaño máximo 64 (X520). Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) - 3 caracteres para indicar el tipo legal de identificador (VAT= documento de identificación fiscal) - 2 caracteres para identificar el país ISO 3166-1 [2] - 1 carácter "-" 0x2D (ASCII), U+002D (UTF-8)

Campo	Contenido	Obligatorio	Criticidad	Descripción
6.4. Common Name	CA del prestador de servicios de confianza bajo la cual se generar el certificado electrónico. El valor que tomará será (según CA subordinada) cn= AC ENTIDADES G2	Si		UTF8 String, tamaño máximo 64 (rfc5280) -
7. Autority Key Identifier	Identificador de la clave pública de la AC RAIZ FNMT-RCM G2. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info	Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico. En este caso Secp256r1.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. ECC P-256 bits
9. Subject Key Identifier	Identificador de la clave pública del Firmante. Es el medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Sí	Sí	Normalizado en norma X509 y RFC 5280.
10.1. Digital Signature	0	Sí		Ver X509 y RFC 5280
10.2. Content Commitment	0	Sí		Ver X509 y RFC 5280
10.3. Key Encipherment	0	Sí		Ver X509 y RFC 5280
10.4. Data Encipherment	0			Ver X509 y RFC 5280
10.5. Key Agreement	0	Sí		Ver X509 y RFC 5280
10.6. Key Certificate Signature	1	Sí		Ver X509 y RFC 5280
10.7. CRL Signature	1	Sí		Ver X509 y RFC 5280
11. Extended Key Usage	Uso mejorado o extendido de las claves			Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.

Campo	Contenido	Obligatorio	Criticidad	Descripción
				Nota: Se trata de una AC Subordinada técnicamente restringida.
11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente.
11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos.
11.3. Adobe Authentic Document Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Certificate Policies		Sí		Políticas de certificación
12.1. Policy Identifier	2.5.29.32.0 (anyPolicy)	Sí		Identificador de la política de identificación. Política a definida por el PSC en el que se encuadre este certificado
13. CRL Distribution Point	Puntos de distribución de las listas de distribución de las listas de revocación de los certificados Electrónicos	Sí	No	
13.1. Distribution Point 1	Punto de distribución 1 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl	Sí		Ruta donde reside la CRL (punto de distribución 1).
14. Authority Info Access		Sí	No	
14.1. Access Method 1	Identificador de método de acceso a la información de revocación OSCP - 1.3.6.1.5.5.7.48.1	Sí		Acceso al servicio OCSP
14.2. Access Location 1	http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder	Sí		**URI** para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
14.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: "the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."

Campo	Contenido	Obligatorio	Criticidad	Descripción
14.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
15. Basic Constrains	Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación". También sirve para distinguir una CA de las entidades finales	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
15.1. cA	Entidad Final (valor TRUE)	Sí		Boolean Indica que el certificado es de una autoridad de certificación. Con este certificado se pueden emitir otros.
15.2. pathLength	0			

2.1. PERFILES DE ENTIDAD FINAL DE CERTIFICADOS DE SELLO DE AC ENTIDADES G2

2.1.1. Certificado de Sello de Entidad de AC Entidades G2

Campo	Contenido	Oblig.	Crit.	Especificaciones
1. Version	2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number	Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm	ecdsa-with-SHA256	Sí		Identificando el tipo de algoritmo OID: 1.2.840.10045.4.3.2

Campo		Contenido	Oblig.	Crit.	Especificaciones
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String,
	4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J	Sí		UTF8 String, tamaño máximo 64 (X520).
	4.4. CommonName	CN=AC ENTIDADES G2			UTF8 String.
5. Validity		Variable	Sí		La duración será variable (1, 2 ó 3 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8 String, tamaño máximo 64 (rfc5280) OU=Departamento de Informática

Campo		Contenido	Oblig.	Crit.	Especificaciones
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo:SN= Q0000000J
	6.6. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VAT ES- Q0000000J
	6.7. Common Name	Denominación del componente	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo:CN=Servicio de Registro
7. Authority Key Identifier		Identificador de la clave pública de la CA emisora. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA emisora.
8. Subject Public Key Info		Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico. En este caso Secp256r1.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. ECC P-256 bits
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.		Sí	Normalizado en norma X509
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment	0	Sí		Ver X509 y RFC 5280.
	10.4. Data Encipherment	0	Sí		Ver X509 y RFC 5280.
	10.5. Key Agreement	0	Sí		Ver X509 y RFC 5280.

Campo		Contenido	Oblig.	Crit.	Especificaciones
	10.6. Key Certificate Signature	0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature	0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
	11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		
	11.3. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Sí		
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance (0.4.0.1862.1.1)	Certificado cualificado	Sí		Indicación de certificado cualificado
	12.2. QcType (0.4.0.1862.1.6)	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		Indica que el certificado es de sello. Certificate for electronic seals as defined in Regulation (EU) No 910/2014
	12.3. QcPDS(0.4.0.1862.1.5)	{https://www.cert.fnmt.es/pds/PDS_Entidades_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_Entidades_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS
	12.4. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan

Campo			Contenido	Oblig.	Crit.	Especificaciones
						verificarse las firmas efectuadas con el mismo
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.22.1.0	Sí		Identificador de la política
	13.2. Policy Qualifier Id			Sí		
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado cualificado de sello electrónico según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de FNMT-RCM con NIF: Q2826004J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.3. Policy Identifier		QCP-l (0.4.0.194112.1.1)	Sí		Certificado cualificado de sello, acorde al Reglamento UE 910/2014 Itu-t(0) Identified-organizatio(4) etsi(0) qualifed-certificate-policies(194112) policy-identifiers(1) qcp-legal(1)
14. Subject Alternative Names				Sí	No	
	14.1. rfc822 Name		Correo electrónico del *Suscriptor*	Opciona l		
	14.2. Directory Name					
		14.2.1 Entidad suscriptora	Nombre de la entidad propietaria del Sello Id Campo/Valor: 1.3.6.1.4.1.5734.1.6=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Ministerio de Economía y Hacienda
		14.2.2 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 1.3.6.1.4.1.5734.1.7=<NIF entidad suscriptora>	Sí		UTF8 String, tamaño 9. Por ejemplo: 1.3.6.1.4.1.5734.1.7=Q2826004J

Campo		Contenido	Oblig.	Crit.	Especificaciones
	14.2.3 Denominación del componente	Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí		
15. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	15.1. Distribution Point 1	Punto de distribución 1 de la CRL http://www.cert.fnmt.es/crlacentiG2/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
16. Authority Info Access			Sí	No	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Access Location 1	http://ocspentiG2.cert.fnmt.es/ocspentiG2/OcspResponder	Sí		URL del servicio de OCSP
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACENTIG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.

Campo	Contenido	Oblig.	Crit.	Especificaciones
17. Basic Contraints	Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*
17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.1.2. Certificado de Sello Electrónico de AC Entidades G2

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version	2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number	Número identificativo único del Sello. Este número se asigna de forma aleatoria.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos ($1- 2^{159}$).
3. Signature Algorithm	ecdsa-with-SHA256	Sí		OID: 1.2.840.10045.4.3.2
4. Issuer Distinguish Name	Entidad emisora del certificado	Sí		
4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora.	Sí		UTF8 String, tamaño máximo 64 (X520). Por ejemplo: organizationidentifier=VATES-Q0000000J

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		organizationIdentifier=VAT ES-Q2826004J			
	4.4. Common Name	cn= AC ENTIDADES G2	Sí		UTF8 String (rfc5280)
5. Validity		3 años	Sí		Validez del certificado
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí		
	6.1. Country	Estado cuya ley rige el nombre, que será "España". C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Locality	Nombre de la localidad del suscriptor (organización)	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del creador del Sello	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=SELLO ELECTRONICO	Sí		(UTF8String tamaño máximo 64 caracteres)
	6.5. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) (UTF8String tamaño máximo 15 caracteres)	Sí		OrganizationIdentifier p. ej: VATESS2833002.
	6.6. Serial Number	Número único de identificación de la Entidad suscriptora de servicios de certificación. En este caso el NIF	Sí		Por ejemplo: serialNumber=Q2826004J PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9.
	6.7. Common Name	Denominación de sistema o aplicación de proceso automático. Se deberá asegurar que dicho nombre tenga sentido y no de lugar a ambigüedades (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=SERVICIO DE REGISTRO DEL MEH
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info	Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico. En este caso Secp256r1.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. ECC P-256 bits
9. Subject Key Identifier	Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Sí	Sí	Normalizado en norma X509 y RFC 5280
10.1. Digital Signature	1			Ver X509 y RFC 5280
10.2. Content Commitment	1			Ver X509 y RFC 5280
10.3. Key Encipherment	0			Ver X509 y RFC 5280
10.4. Data Encipherment	0			Ver X509 y RFC 5280
10.5. Key Agreement	0			Ver X509 y RFC 5280
10.6. Key Certificate Signature	0			Ver X509 y RFC 5280
10.7. CRL Signature	0			Ver X509 y RFC 5280
11. Extended Key Usage	Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente.
11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos.
11.3. Adobe Authentic Document Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Qualified Certificate Statements		Sí	No	

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
12.1. QcCompliance(0.4.0.1862.1.1)	Sello cualificado.	Sí		Indica que el sello es cualificado.
12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del Sello que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".
12.3. QcType (0.4.0.1862.1.6)	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		Indica que el certificado es de sello electrónico. *Certificate for electronic seals as defined in Regulation (EU) No 910/2014*
12.4. QcPDS (0.4.0.1862.1.5)	{https://www.cert.fnmt.es/pds/PDS_Entidades_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_Entidades_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
13. Certificate Policies	Política de certificación	Sí	No	
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.22.2.0	Sí		Identificador de la política asociado a la DPC o PC
13.2. Policy Qualifier Id				
13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
13.2.2 User Notice	"Certificado cualificado de sello electrónico. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106–28009–Madrid–España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
13.3. Policy Identifier	QCP-l (OID:0.4.0.194112.1.1)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)
13.4. Policy Identifier	2.16.724.1.3.5.6.2	Sí		OID asociado a certificado de sello de nivel medio
14. Subject Alternative Names	Identificación/ descripción del titular	Sí	No	
14.1. rfc822 Name	Correo electrónico del titular	Opcional		Por ejemplo: rfc822Name=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.2. Directory Name		Sí		
14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.6.2.1=SELLO ELECTRONICO DE NIVEL MEDIO	Sí		UTF8 String.
14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del Sello. Id Campo/Valor: 2.16.724.1.3.5.6.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.6.2.2=Ministerio de Economía y Hacienda
14.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.6.2.3=<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.6.2.3=Q2826004J
14.2.4 Denominación de sistema o componente	Breve descripción del componente asociado al sello. 2.16.724.1.3.5.6.2.5=<Denominación del Sistema>	Sí		UTF8 String, tamaño máximo 64. Por ejemplo: 2.16.724.1.3.5.6.2.5= SERVICIO DE REGISTRO DEL MEH
15. CRL Distribution Point	Punto de distribución (localizador) de la CRL	Sí	No	
15.1. Distribution Point 1	Punto de distribución 1 de la CRL	Sí		

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	http://www.cert.fnmt.es/crlacentiG2/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)			Ruta donde reside la CRL (punto de distribución 1).
16. Authority Info Access		Sí	No	
16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		Acceso al servicio OCSP
16.2. Access Location 1	http://ocspentiG2.cert.fnmt.es/ocspentiG2/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACENTIG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
17. Basic Contraints	Esta extensión sirve para identificar si el sujeto de certificación es una CA, así como el máximo nivel de "profundidad" permitido para las cadenas de certificación". También sirve para distinguir una CA de las entidades finales	Sí	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*
17.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

3. PERFIL DEL CERTIFICADO DE AC SECTOR PÚBLICO

Campo		Contenido	Oblig	Especificaciones
1. Version		2	Sí	Integer:=2 ([RFC 5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3).
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC 5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (RFC 5280).
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 64 (RFC 5280).
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado (Entidad de Certificación) ou= AC RAIZ FNMT-RCM	Sí	UTF8 String, tamaño máximo 64 (RFC 5280).
5. Validity		10 años	Sí	
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí	
	6.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (RFC 5280).
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 64 (RFC 5280).
	6.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 64 (RFC 5280).

Campo			Contenido	Oblig	Especificaciones
	6.4. Organization Identifier		Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J	Sí	UTF8 String, tamaño máximo 64 (X520). Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad).
	6.5. Common Name		cn=AC Sector Público	Sí	UTF8 String, tamaño máximo 64 (RFC 5280).
7. Authority Key Identifier			Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí	Ver RFC 5280: hash SHA-1 de 20 bytes. Coincide con el campo Subject Key Identifier de la AC raíz.
8. Subject Public Key Info			Clave pública de la CA Subordinada para la Administración Pública, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 4096.
9. Subject Key Identifier			Identificador de la clave pública de la CA Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	Ver RFC 5280: hash SHA-1 de 20 bytes.
10. Key Usage			Uso permitido de las claves certificadas.	Sí	Normalizado en X509 y RFC 5280.
	10.1. Digital Signature		0	Sí	Ver X509 y RFC 5280.
	10.2. Content Commitment		0	Sí	Ver X509 y RFC 5280.
	10.3. Key Encipherment		0	Sí	Ver X509 y RFC 5280.
	10.4. Data Encipherment		0	Sí	Ver X509 y RFC 5280.
	10.5. Key Agreement		0	Sí	Ver X509 y RFC 5280.
	10.6. Key Certificate Signature		1	Sí	Ver X509 y RFC 5280.
	10.7. CRL Signature		1	Sí	Ver X509 y RFC 5280.
11. Certificate Policies			Política de certificación	Sí	
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí	Ver RFC 5280.
	11.2. Policy Qualifier Id				
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la	Sí	UTF8 String. Longitud máxima 200 caracteres.

Campo			Contenido	Oblig	Especificaciones
			FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)		
12. CRL Distribution Point				Sí	
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí	Ruta donde reside la CRL (punto de distribución 1).
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí	Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Authority Info Access					
	13.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
	13.2. Acces Location 1		http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	Sí	URL del servicio OCSP (no autenticado).
	13.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	Emisor de la entidad emisora de certificados (CA Raíz). Ver RFC 5280.
	13.4. Access Location 2		http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí	Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado raíz de la FNMT-RCM.
14. Basic Constraints			Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".		
	14.1. Subject Type		CA		Tipo de sujeto: Autoridad de Certificación.
	14.2. Path Length		0		Un pathLenConstraint de cero indica que ningún no pueden existir más certificados de CA intermedios en la ruta de certificación.

3.1. PERFILES DE ENTIDAD FINAL DE CERTIFICADOS DE SELLO DE AC SECTOR PÚBLICO

3.1.1. Certificado de Sello Electrónico

Campo		Contenido	Oblig	Crit	Especificaciones
1. Version		2	Sí		Integer:= 2 ([RFC 5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3).
2. Serial Number		Número identificativo único del Sello. Este número se asigna de forma aleatoria.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC 5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del Sello	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (RFC 5280).
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del Sello). o=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 64 (RFC 5280).
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del Sello. ou=CERES	Sí		UTF8 String, tamaño máximo 64 (RFC 5280).
	4.4. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J	Sí		UTF8 String, tamaño máximo 64 (X520). Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad).
	4.5. Common Name	cn= AC Sector Público	Sí		UTF8 String(RFC 5280).
5. Validity		Variable	Sí		Hasta el 31 de diciembre de 2028
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí		

Campo		Contenido	Oblig	Crit	Especificaciones
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (RFC 5280).
	6.2. Locality	Nombre de la localidad del suscriptor (organización)	Sí		UTF8String (RFC 5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del creador del Sello (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (RFC 5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=SELLO ELECTRONICO (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (RFC 5280).
	6.5. Organization Identifier	Identificador de la organización distinto del nombre (UTF8String tamaño máximo 15 caracteres)	Sí		UTF8 String, tamaño máximo 64 (X520). Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad).
	6.6. Serial Number	Número único de identificación de la Entidad suscriptora de servicios de certificación. En este caso el NIF	Sí		Por ejemplo: serialNumber=Q2826004J PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9.
	6.7. Common Name	Denominación de sistema o aplicación de proceso automático. Se deberá asegurar que dicho nombre tenga sentido y no de lugar a ambigüedades (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8String (RFC 5280) tamaño máximo 64 caracteres. Por ejemplo: cn=SERVICIO DE REGISTRO DEL MEH
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	No	Ver RFC 5280: hash SHA-1 de 20 bytes. Coincide con el campo Subject Key Identifier de la AC emisora.

Campo		Contenido	Oblig	Crit	Especificaciones
8. Subject Public Key Info		Clave pública del sello, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048.
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	No	Ver RFC 5280: hash SHA-1 de 20 bytes.
10. Key Usage			Sí	Sí	Normalizado en X509 y RFC 5280.
	10.1. Digital Signature	1			Ver X509 y RFC 5280.
	10.2. Content Commitment	1			Ver X509 y RFC 5280.
	10.3. Key Encipherment	1			Ver X509 y RFC 5280.
	10.4. Data Encipherment	0			Ver X509 y RFC 5280.
	10.5. Key Agreement	0			Ver X509 y RFC 5280.
	10.6. Key Certificate Signature	0			Ver X509 y RFC 5280.
	10.7. CRL Signature	0			Ver X509 y RFC 5280.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
	11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente.
	11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos.
	11.3. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	
	12.1. QcCompliance (0.4.0.1862.1.1)	Sello cualificado	Sí		Indica que el Sello es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del sello que se dispone de los datos de registro y otra información relevante.

Campo			Contenido	Oblig	Crit	Especificaciones
	12.3. QcType (0.4.0.1862.1.6)		Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		Indica que el certificado es de sello electrónico. *Certificate for electronic seals as defined in Regulation (EU) No 910/2014*
	12.4. QcPDS(0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_SP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_SP_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS.
	12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)		semanticsId-Legal (0.4.0.194121.1.2)	Sí		Indica que el campo subject sigue la semántica propuesta por la EN 319 412-1.
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.17.1	Sí		Identificador de la política asociado a la DPC o PC.
	13.2. Policy Qualifier Id					
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	"Certificado cualificado de sello electrónico. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106–28009–Madrid–España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.3. Policy Identifier		QCP-l (0.4.0.194112.1.1)	Sí		QCP-l: política para certificados cualificados EU emitidos a personas jurídicas.
	13.4. Policy Identifier		2.16.724.1.3.5.6.2	Sí		OID asociado a certificado de sello de nivel medio.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	No	
	14.1. rfc822 Name		Correo electrónico de contacto de la entidad suscriptora	No		Por ejemplo: rfc822Name=sellomeh@meh.es
	14.2. Directory Name		Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.

Campo			Contenido	Oblig	Crit	Especificaciones
		14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.6.2.1=SELLO ELECTRONICO DE NIVEL MEDIO	Sí		UTF8 String.
		14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del Sello. Id Campo/Valor: 2.16.724.1.3.5.6.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.6.2.2=Ministerio de Economía y Hacienda
		14.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.6.2.3=<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.6.2.3=Q2826004J
		14.2.4 Denominación de sistema o componente	Breve descripción del componente asociado al sello. 2.16.724.1.3.5.6.2.5=<Denominación del Sistema>	Sí		UTF8 String, tamaño máximo 64. Por ejemplo: 2.16.724.1.3.5.6.2.5= SERVICIO DE REGISTRO DEL MEH
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al Sello.	Sí	No	
	15.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacsp/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. Ldap://ldapsp.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Sector%20Publico,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).

Campo		Contenido	Oblig	Crit	Especificaciones
16. Authority Info Access			Sí	No	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		Acceso al servicio OCSP.
	16.2. Acces Location 1	http://ocspsp.cert.fnmt.es/ocspsp/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Emisor de la entidad emisora de certificados (CA Raíz). Ver RFC 5280.
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACSP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
17. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	Sí	Ver RFC 5280.
	17.1. Subject Type	Entidad final (valor FALSE)			Con este Sello no se pueden emitir otros.

4. PERFIL DEL CERTIFICADO DE AC REPRESENTACIÓN

Campo		Contenido	Oblig	Crit	Descripción
1. Versión		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organizational Unit	OU=CERES	Sí		UTF8 String.
	4.4. Common Name	OU=AC RAIZ FNMT-RCM	Sí		UTF8 String.
5. Validity		Hasta 31/12/2029	Sí		
6. Subject			Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	6.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String.
	6.3. Organizational Unit	OU=CERES	Sí		UTF8 String.

Campo			Contenido	Oblig	Crit	Descripción
	6.4. Common Name		CN=AC Representación	Sí		UTF8 String.
7. Autority Key Identifier			Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí		Ver RFC 5280: hash SHA-1 de 20 bytes. Coincide con el campo Subject Key Identifier de la AC raíz.
8. Subject Public Key Info			Clave pública de la CA Subordinada de Representación codificada según el estándar PKCS#1 de RSA.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits
9. Subject Key Identifier			Identificador de la clave pública de la CA Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí		Ver RFC 5280: hash SHA-1 de 20 bytes.
10. Key Usage			Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en X509 y RFC 5280.
	10.1. Digital Signature		0	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment		0	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment		0	Sí		Ver X509 y RFC 5280.
	10.4. Data Encipherment		0	Sí		Ver X509 y RFC 5280.
	10.5. Key Agreement		0	Sí		Ver X509 y RFC 5280.
	10.6. Key Certificate Signature		1	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature		1	Sí		Ver X509 y RFC 5280.
11. Certificate Policies			Política de certificación	Sí		
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí		Ver RFC 5280.
	11.2. Policy Qualifier Id			Sí		
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí		UTF8 String.
12. CRL Distribution Point				Sí		
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-	Sí		Ruta donde reside la CRL (punto de distribución 1).

Campo		Contenido	Oblig	Crit	Descripción
		RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint			
	12.2. Distribution Point 2	Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Authority Info Access			Sí	No	
	13.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	13.2. Access Location 1	http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	Sí		URL del servicio de OCSP.
	13.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Certificado de la CA emisora: Ver RFC 5280.
	13.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA raíz de la FNMT-RCM.
14. Basic Constrains			Sí	Sí	
	14.1. cA	Valor TRUE (CA)	Sí		Ver RFC 5280.
	14.2. pathLength	0	Sí		Un pathLenConstraint de cero indica que no pueden existir más certificados de CA intermedios en la ruta de certificación.

4.1. PERFILES DE ENTIDAD FINAL DE CERTIFICADOS DE SELLO DE AC REPRESENTACIÓN

4.1.1. Certificado de Sello de Entidad

Campo		Contenido	Oblig.	Crit.	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String,
	4.3. Organization Unit	OU=CERES	Sí		UTF8 String,
	4.4. CommonName	CN=AC Representación			UTF8 String.
5. Validity		Variable	Sí		La duración será variable (1 ó 2 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.

Campo		Contenido	Oblig.	Crit.	Especificaciones
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8 String, tamaño máximo 64 (rfc5280) OU=Departamento de Informática
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo:SN= Q0000000J
	6.6. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VAT ES- Q0000000J
	6.7. Common Name	Denominación del componente	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo:CN=Servicio de Registro
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA.	Sí	No	Campo que contiene la clave pública del certificado.

Campo		Contenido	Oblig.	Crit.	Especificaciones
		La longitud de la clave será 2048 bits.			
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.		Sí	Normalizado en norma X509
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment	1	Sí		Ver X509 y RFC 5280.
	10.4. Data Encipherment	0	Sí		Ver X509 y RFC 5280.
	10.5. Key Agreement	0	Sí		Ver X509 y RFC 5280.
	10.6. Key Certificate Signature	0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature	0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
	11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		
	11.3. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Sí		
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance (0.4.0.1862.1.1)	Certificado cualificado	Sí		Indicación de certificado cualificado
	12.2. QcType (0.4.0.1862.1.6)	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		Indica que el certificado es de sello.

Campo			Contenido	Oblig.	Crit.	Especificaciones
						Certificate for electronic seals as defined in Regulation (EU) No 910/2014
	12.3. QcPDS(0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_es.pdf,es},{https://www.cert.fnmt.es/pds/PDS_en.pdf,en}	Sí		Lugar donde se encuentra la declaración PDS
	12.4. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.4	Sí		Identificador de la política
	13.2. Policy Qualifier Id			Sí		
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado cualificado de sello electrónico según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de FNMT-RCM con NIF: Q2826004J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.3. Policy Identifier		QCP-l (0.4.0.194112.1.1)	Sí		Certificado cualificado de sello, acorde al Reglamento UE 910/2014 Itu-t(0) Identified-organizatio(4) etsi(0) qualifed-certificate-policies(194112) policy-identifiers(1) qcp-legal(1)
14. Subject Alternative Names				Sí	No	

Campo			Contenido	Oblig.	Crit.	Especificaciones
	14.1. rfc822 Name		Correo electrónico del *Suscriptor*	Opciona l		
	14.2. Directory Name					
		14.2.1 Entidad suscriptora	Nombre de la entidad propietaria del Sello Id Campo/Valor: 1.3.6.1.4.1.5734.1.6=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Ministe rio de Economía y Hacienda
		14.2.2 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 1.3.6.1.4.1.5734.1.7=<NIF entidad suscriptora>	Sí		UTF8 String, tamaño 9. Por ejemplo: 1.3.6.1.4.1.5734.1.7=Q2826 004J
		14.2.3 Denominación del componente	Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí		
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN =CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevoca tionList;binary?base?objectcla ss=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsre p/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)

Campo		Contenido	Oblig.	Crit.	Especificaciones
	16.2. Access Location 1	http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
17. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.