Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

DEFINICIÓN PERFILES DE CERTIFICADO EMITIDOS PARA EL SECTOR PÚBLICO

Referencia:

Documento clasificado como: *Público*

1. Introducción 3
2. Perfil de certificado de CA 4
3. Perfiles de certificado de entidades finales 8
3.1. Certificado de Empleado Público 8
3.2. Certificado con Seudónimo de la Administración de Justicia 17
3.3. Certificado con Seudónimo 25
3.4. Certificado de Firma Centralizada para Empleado Público 31
3.5. Certificado de Firma Centralizada con seudónimo de la Administración de Justicia. 39
3.6. Certificado de Empleado Público en QSCD nivel medio 47
3.7. Certificado de Autenticación Empleado Público en QSCD nivel alto 57
3.8. Certificado de Firma Empleado Público en QSCD nivel alto 65
3.9. Certificado Centralizado de Carrera Judicial 73
4. Perfil de certificado de AC Sector Público G2 80
5. Perfiles de certificado de entidades finales 86
5.1. Certificado de Empleado Público 86
5.2. Certificado con Seudónimo de la Administración de Justicia 95
5.3. Certificado con Seudónimo 102
5.4. Certificado de Firma Centralizada para Empleado Público 108
5.5. Certificado de Firma Centralizada con seudónimo de la Administración de Justicia. 117
5.6. Certificado de Empleado Público en QSCD nivel medio 126
5.7. Certificado de Autenticación Empleado Público en QSCD nivel alto 135
5.8. Certificado de Firma Empleado Público en QSCD nivel alto 144
5.9. Certificado Centralizado de Carrera Judicial 152

1. INTRODUCCIÓN

El presente documento describe en detalle los perfiles de los distintos tipos de certificados de persona física que emiten las Autoridades de Certificación "*AC Sector Público*", que sustituyó a la "*AC Administración Pública*" previamente gestionada por la FNMT-RCM y la "*AC Sector Público G2"*.

Los tipos de certificado que emite la "*AC Sector Público*" son:

- Certificado de Empleado Público
- Certificado con Seudónimo de la Administración de Justicia
- Certificado con Seudónimo
- Certificado de Firma Centralizada para Empleado Público
- Certificado de Firma Centralizada con seudónimo de la Administración de Justicia
- Certificado de Empleado Público en QSCD nivel medio
- Certificado de Autenticación Empleado Público en QSCD nivel alto
- Certificado de Firma Empleado Público en QSCD nivel alto
- Certificado Centralizado de Carrera Judicial

Los tipos de certificado que emite la "*AC Sector Público G2*" son:

- Certificado de Empleado Público G2
- Certificado con Seudónimo de la Administración de Justicia G2
- Certificado con Seudónimo G2
- Certificado de Firma Centralizada para Empleado Público G2
- Certificado de Firma Centralizada con seudónimo de la Administración de Justicia G2
- Certificado de Empleado Público en QSCD nivel medio G2
- Certificado de Autenticación Empleado Público en QSCD nivel alto G2
- Certificado de Firma Empleado Público en QSCD nivel alto G2
- Certificado Centralizado de Carrera Judicial G2

2. PERFIL DE CERTIFICADO DE CA

Campo		Contenido	Obligatoriedad	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 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 (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. 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 (rfc5280)
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 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador	Sí	UTF8 String, tamaño máximo 64 (rfc5280)

Campo		Contenido	Obligatoriedad	Especificaciones
		de servicios de certificación (emisor del certificado). o=FNMT-RCM.		
	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 (rfc5280)
	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. 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 (rfc5280)
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	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 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	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 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

Campo		Contenido	Obligatoriedad	Especificaciones
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	Atendiendo a la rfc5280: "*PolicyInformation SHOULD only contain an OID.* *In a CA certificate,these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }*"
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 FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí	UTF8 String. Longitud máxima 200 caracteres.
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)	Sí	Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).

Campo		Contenido	Obligatoriedad	Especificaciones
		http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl		
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) 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.*"
	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. PERFILES DE CERTIFICADO DE ENTIDADES FINALES

3.1. CERTIFICADO DE EMPLEADO PÚBLICO

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 certificado. 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	Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
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. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. Ou=CERES	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
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. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	4.5. Common Name	cn= AC Sector Público	Sí		UTF8 String (rfc5280)
5. Validity		Hasta el 31 de diciembre de 2028	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" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de organización) del suscriptor del certificado	Sí		UTF8 String, tamaño máximo 200. Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				este campo no estará presente en el certificado.
6.6. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
6.7. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte)	Sí		UTF8String tamaño máximo 50 caracteres. Por ejemplo: gn=JUAN
6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Sí		UTF8String tamaño máximo 168 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. 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 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 asociada al empleado público, 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	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).

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	de rutas de certificación.			
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	1			Ver X509 y RFC 5280
10.4. Data Encipherment	0			Ver X509 y RFC 5280 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
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.
11.4. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Sí		*Necesaria para realizar logon en Windows*
12. Qualified Certificate Statements		Sí	No	
12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado 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 certificado que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga:

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					"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)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.5 id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Sí		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
13. Certificate Policies		Política de certificación	Sí	No	
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.2	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 firma electrónica de empleado público. 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-n (OID:0.4.0.194112.1.0)	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-natural (0)
13.4. Policy Identifier	2.16.724.1.3.5.7.2	Sí		Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional.
14. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
14.1. rfc822 Name	Correo electrónico del empleado público	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. UPN	UPN (nombre de login de red) para smartcard logon.	Opcional		Campo destinado a incluir el Smartcard logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.3. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.
14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)	Sí		UTF8 String. 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)
14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor:	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	2.16.724.1.3.5.7.2.2=< Entidad Suscriptora>			
14.3.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.2.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.3=Q2826004 J
14.3.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.2.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.4 =99999999R
14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.2.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.5=ADM123 47 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.6=JUAN
14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.7=ESPAÑO L
14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor:	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.8=ESPAÑO L

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		2.16.724.1.3.5.7.2.8 =<Apellido 2>			
	14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.9=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.
	14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.2.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point		Punto de distribución (localizador) de la CRL	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-	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	RCM,C=ES?certificate RevocationList;binary? base?objectclass=cRL DistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)			
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) 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. 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". 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

3.2. CERTIFICADO CON SEUDÓNIMO DE LA ADMINISTRACIÓN DE JUSTICIA

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 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 Subordinada)	Sí		
	4.1. Country	ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	4.2. Organization	FNMT-RCM	Sí		Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). UTF8 String.
	4.3. Organizational Unit	CERES	Sí		UTF8 String.
	4.4. Organization Identifier	VATES-Q2826004J	Sí		UTF8 String
	4.5. CommonName	AC Sector Público	Sí		UTF8 String.
5. **Validity**		Hasta el 31 de diciembre de 2028	Sí		Validez del Certificado

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
6. **Subject**		Identificación del titular	Sí		
	6.1. Country	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 suscriptor del certificado	Sí		Por ejemplo: O=ADMINISTRACION DE JUSTICIA
	6.3. Organizational Unit	Habitualmente, Unidad Organizativa. En este caso, para mejorar la compatibilidad de los certificados de seudónimo del ámbito de la AGE, se incluye una indicación al respecto. (UTF8String tamaño máximo 64 caracteres)	Sí		Descripción del tipo de certificado. En este caso: "CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO"
	6.4. Organizational Unit	Unidad, dentro de la administración, en la que está incluida el suscriptor del certificado Ver apartado 2.3 (UTF8String tamaño máximo 64 caracteres)	No		UTF8String, tamaño máximo 64 caracteres Ejemplo: OU = CONSEJO GENERAL DEL PODER JUDICIAL OU = ADMINISTRACIÓN DE JUSTICIA
	6.5. Pseudonym (Oid 2.5.4.65)	"JU:ES-${ID}" ${ID} es el identificador para el profesional del ámbito de la Justicia Ver apartado 2.1 (UTF8String tamaño máximo 40 caracteres)	Sí		UTF8String (rfc5280), tamaño máximo 128 caracteres. ${ID} = CARGO (1) + CODIGO (9) + DG (1) Por ejemplo: JU:ES-L123456789W
	6.6. Title	Profesión o cargo de la persona física, que le	Sí		UTF8String, tamaño máximo 64 caracteres. Por ejemplo:

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2 (UTF8String tamaño máximo 64 caracteres)			Title=CARRERA JUDICIAL Title=CARRERA FISCAL Title=C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA
	6.7. CommonName	Tendrá el formato ${title} – JU:ES-${ID} – ${Organización} ${title} es el puesto o cargo ${ID} es el identificador para el profesional del ámbito de la Justicia ${Organización} es la organización a la que pertenece. Ver apartado 2.4	Sí		UTF8String tamaño máximo 108 caracteres. Por ejemplo: "C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA – JU:ES-L123456789W – ADMINISTRACIÓN DE JUSTICIA"
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		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 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 2048 bits
9. **Subject Key Identifier**		Identificador de la clave pública del *Firmante*. Medio para identificar certificados que contienen una clave pública	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).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		particular y facilita la construcción de rutas de certificación.			
10. Key Usage		Uso permitido de las claves certificadas.	Sí	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		Ver X509 y RFC 5280.
	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		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.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Sigue vigente para el OID la norma TS 101 862
	12.2. QcType	Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS	{https://www.cert.fnmt.es/pds/PDS_SP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_SP_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	12.4. QcEuRetentionPeriod	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.
13. Certificate Policies		Política de certificación	Sí		
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.3	Sí		Identificador de la política establecido por el Prestador.
	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 empleado público con seudónimo del ámbito de Justicia. 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.
	13.3. Policy Identifier	0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.4. Policy Identifier	2.16.724.1.3.5.4.2	Sí		Identificador de la política asociado al certificado de empleado público con seudónimo de nivel medio según normativa nacional
14. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Sí	No	
	14.1. rfc822 Name	Correo electrónico del profesional del ámbito de la Justicia empleado público	Opcional		
	14.2. User Principal name	UPN para Smart card logon	No		
	14.3. Directory Name				

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
14.3.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)	Sí		UTF8 String. OID=2.16.724.1.3.5.4.2.1 CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)
14.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.2.
14.3.3. NIF de la entidad suscriptora	Número único de identificación de la entidad. En caso del CGPJ: S2804008G y en el caso del MJU: S2813001A	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.3.
14.3.4. Correo electrónico	Correo electrónico de contacto	No		UTF8String. OID=2.16.724.1.3.5.4.2.9.
14.3.5. Unidad organizativa	Unidad, dentro de la administración, en la que está incluida el firmante del certificado Ver apartado 2.3	No		UTF8String. OID=2.16.724.1.3.5.4.2.10 2.16.724.1.3.5.4.2.2= ADMINISTRACIÓN DE JUSTICIA 2.16.724.1.3.5.4.2.2=CONSEJO GENERAL DEL PODER JUDICIAL
14.3.6. Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2	Sí		UTF8String. OID=2.16.724.1.3..4.2.11.
14.3.7. Seudónimo	Seudónimo: JU:ES-${ID} Ver apartado 2.1	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.12
14.3.8. Nombre	Nombre de pila del profesional del ámbito de la Justicia	Sí		UTF8String. OID=2.16.724.1.3.5.7.2.6

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	14.3.9. Primer apellido	Primer apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.2.7
	14.3.10. Segundo apellido	Segundo apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.2.8
15. CRL Distribution Point			Sí	No	
	15.1. Distribution Point 1	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 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 publicación de la CRL1 http://www.cert.fnmt.es/crlsacsp/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).). <nnn> es el identificador de la CRL particionada concreta donde se halla el certificado.
16. Authority Info Access			Sí	No	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación:	Sí		OCSP (1.3.6.1.5.5.7.48.1)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		1.3.6.1.5.5.7.48.1 (ocsp)			
	16.2. Acces Location 1	http://ocspsp.cert.fnmt.es/ocspsp/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		Certificado de la CA emisora: 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. 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. En este caso la ruta del certificado de la CA subordinada de Representación.
17. **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".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. cA	Valor FALSE (entidad final)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

3.3. CERTIFICADO CON SEUDÓNIMO

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 certificado es versión 3 (X509v3).
2. **Serial Number**	Número identificativo único del certificado.	Sí		Integer. Establecido aleatoriamente y de forma automática por la Entidad de Certificación. RFC5280: Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). Ejemplo: SerialNumber = 111222
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	ES	Sí		PrintableString. Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
4.2. Organization	FNMT-RCM	Sí		UTF8 String. Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado).
4.3. Organizational Unit	CERES	Sí		UTF8 String.
4.4. Organization Identifier	VATES-Q2826004J	Sí		UTF8 String.
4.5. CommonName	AC Sector Público	Sí		UTF8 String.
5. **Validity**	Hasta el 31 de diciembre de 2028	Sí		Validez del Certificado
6. **Subject**	Identificación del titular	Sí		
6.1. Country	ES	Sí		PrintableString.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
6.2. Organization	Denominación (nombre "oficial" de la organización) del suscriptor del certificado	Sí		UTF8String tamaño máximo 64 caracteres. Por ejemplo: O=FNMT
6.3. Organizational Unit	Habitualmente, Unidad Organizativa. En este caso, para mejorar la compatibilidad de los certificados de seudónimo del ámbito de la Administración, se incluye una indicación al respecto. (UTF8String tamaño máximo 64 caracteres)	Sí		Descripción del tipo de certificado. En este caso: "CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO".
6.4. Organizational Unit	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	No		UTF8String (rfc5280) Por ejemplo: OU=Ceres
6.5. Pseudonym (Oid 2.5.4.65)	Seudónimo del empleado público (UTF8String tamaño máximo 40 caracteres)	Sí		UTF8String (rfc5280) Por ejemplo: Pseudonym=L123456789W
6.6. Title	Profesión o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. (UTF8String tamaño máximo 64 caracteres)	No		UTF8String (rfc5280) Por ejemplo: Title=Director
6.7. CommonName	Tendrá el formato: - Si se incluye el campo *Title:* ${title} – ${Pseudonym} – ${Organización} - Si no se incluye el campo Title: SEUDÓNIMO – ${Pseudonym} – ${Organización}	Sí		UTF8String tamaño máximo 174 caracteres . Por ejemplo: - Si se incluye el campo *Title:* CN= Director - L123456789W – FNMT - Si no se incluye el campo Title:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				CN= SEUDÓNIMO - L123456789W – FNMT
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 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 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 bits.
9. **Subject Key Identifier**	Identificador de la clave pública del *Firmante*. 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**	Uso permitido de las claves certificadas.	Sí	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	Ver X509 y RFC 5280.
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.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
12. Qualified Certificate Statements	Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
12.1. QcCompliance	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Sigue vigente para el OID la norma TS 101 862.
12.2. QcType	Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
12.3. QcPDS	{https://www.cert.fnmt.es/pds/PDS_SP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_SP_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.4. QcEuRetentionPeriod	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.
13. Certificate Policies	Política de certificación.	Sí	No	
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.4	Sí		Identificador de la política establecido por el Prestador.
13.2. Policy Qualifier Id				
13.2.1. PS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
13.2.2. User Notice	Certificado cualificado de empleado público con seudónimo. Sujeto a las condiciones de uso de la DPC. FNMT-RCM, NIF Q2826004-J C/Jorge Juan 106 – 28009 – Madrid – España	Sí		UTF8 String.
13.3. Policy Identifier	0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
13.4. Policy Identifier	2.16.724.1.3.5.4.2	Sí		Identificador de la política según normativa nacional.
14. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
14.1. rfc822 Name	Correo electrónico del empleado público.	No		
14.2. User Principal name	UPN para Smart card logon	No		
14.3. Directory Name				
14.3.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)	Sí		UTF8 String. OID=2.16.724.1.3.5.4.2.1 CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)
14.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.2.
14.3.3. NIF de la entidad suscriptora	Número único de identificación de la entidad.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.3.
14.3.4. Correo electrónico	Correo electrónico de contacto.	No		UTF8String. OID=2.16.724.1.3.5.4.2.9.
14.3.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluido el firmante del certificado.	No		UTF8String. OID=2.16.724.1.3.5.4.2.10
14.3.6. Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.	No		UTF8String. OID=2.16.724.1.3.5.4.2.11.
14.3.7. Seudónimo	Seudónimo.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.12
15. CRL Distribution Point		Sí	No	
15.1. Distribution Point 1	Punto de publicación de la CRL. ldap://ldapsp.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Sector%20Publico,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?bas	Sí		Ruta del servicio LDAP donde reside la CRL. <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	e?objectclass=cRLDistributionPoint			
15.2. Distribution Point 2	Punto de publicación de la CRL http://www.cert.fnmt.es/crlsacsp/CRL<xxx*>.crl	Sí		Ruta http donde obtener la CRL. <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
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. Acces Location 1	http://ocspsp.cert.fnmt.es/ocspsp/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		Certificado de la CA emisora. RFC5280: "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. 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. En este caso la ruta del certificado de la CA subordinada AP.
17. 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".	Sí	Sí	RFC5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
17.1. cA	Valor FALSE (entidad final).	Sí		RFC5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

3.4. CERTIFICADO DE FIRMA CENTRALIZADA PARA EMPLEADO PÚBLICO

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 certificado. 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	Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
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. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
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. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	4.5. Common Name	cn=AC Sector Público	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
5. Validity		Hasta el 31 de diciembre de 2028	Sí		Validez del certificado
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí		
	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 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el firmante (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del firmante (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				este campo no estará presente en el certificado.
6.6. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
6.7. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: cn= ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
6.10. Title	Puesto de trabajo o cargo	Opcional		UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. 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 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 asociada al empleado público,	Sí	No	Campo para transportar la clave pública y para identificar el

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.			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 firmante. 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	Normalizado en norma X509 y RFC 5280
10.1. Digital Signature	0			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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
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. Qualified Certificate Statements			No	
11.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
11.2. 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

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				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.".
11.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
11.4. 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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
11.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	No		Indica que el campo subject sigue la semántica propuesta por la EN 319 412-1
11.6. QcSSCD (0.4.0.1862.1.4)		Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
12. Certificate Policies	Política de certificación	Sí	No	
12.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.5	Sí		Identificador de la política asociado a la DPC o PC
12.2. Policy Qualifier Id				
12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
12.2.2 User Notice	Certificado cualificado de firma electrónica centralizada de empleado público. Sujeto a las condiciones de uso expuestas en la DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
12.3. Policy Identifier	QCP-n-qscd (OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
12.4. Policy Identifier	2.16.724.1.3.5.7.1	Sí		Identificador de la política asociado al certificado de empleado público de nivel alto según normativa nacional.
13. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
13.1. rfc822 Name	Correo electrónico del empleado público	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.
13.2. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.
13.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel alto)	Sí		UTF8 String. 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel alto)
13.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.2=MINISTERIO DE ECONOMÍA Y HACIENDA
13.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.1.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.3 =Q2826004J
13.2.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF).	Sí		UTF8 String, tamaño 9. Por ejemplo:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	Id Campo/Valor: 2.16.724.1.3.5.7.1.4 =<NIF>			2.16.724.1.3.5.7.1.4 =99999999R
13.2.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.1.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.5 =ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
13.2.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.6 =JUAN
13.2.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.7 =ESPAÑOL
13.2.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.8 =<Apellido 2>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.8=ESPAÑOL
13.2.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.9 =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.
13.2.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	13.2.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.1.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.11 =ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	No	
	14.1. 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).
	14.2. 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).
15. Authority Info Access			Sí	No	
	15.1. 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
	15.2. Acces Location 1	http://ocspsp.cert.fnmt.es/ocspsp/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
	15.3. Access Method 2	Identificador de método de acceso a la información de	Sí		Emisor de la entidad emisora de certificados (CA Raíz)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)			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.*"
15.4. 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.
16. 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.*
16.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

3.5. CERTIFICADO DE FIRMA CENTRALIZADA CON SEUDÓNIMO DE LA ADMINISTRACIÓN DE JUSTICIA.

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 certificado. 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}).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
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. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
	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. 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, tamaño máximo 64 (rfc5280)
5. Validity		Hasta el 31 de diciembre de 2028	Sí		Validez del certificado
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí		
	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 (rfc5280)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
6.2. Organization	Denominación (nombre "oficial" de la organización) del suscriptor del certificado	Sí		Por ejemplo: O=ADMINISTRACION DE JUSTICIA
6.3. Organizational Unit	Habitualmente, Unidad Organizativa. En este caso, para mejorar la compatibilidad de los certificados de seudónimo del ámbito de la AGE, se incluye una indicación al respecto. (UTF8String tamaño máximo 64 caracteres)	Sí		Descripción del tipo de certificado. En este caso: "CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO"
6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el firmante Ver apartado 2.3 (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Ejemplo: OU = CONSEJO GENERAL DEL PODER JUDICIAL OU = ADMINISTRACIÓN DE JUSTICIA
6.5. Pseudonym (Oid 2.5.4.65)	"JU:ES-${ID}" ${ID} es el identificador para el profesional del ámbito de la Justicia (UTF8String tamaño máximo 40 caracteres)	Sí		UTF8String (rfc5280), tamaño máximo 128 caracteres. ${ID} = CARGO (1) + CODIGO (9) + DG (1) Por ejemplo: JU:ES-L123456789W
6.6. Title	Profesión o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2 (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8String, tamaño máximo 64 caracteres. Por ejemplo: Title=CARRERA JUDICIAL Title=CARRERA FISCAL Title=C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA
6.7. Common Name	Tendrá el formato ${title} – JU:ES-${ID} – ${Organización} ${title} es el puesto o cargo	Sí		UTF8String tamaño máximo 108 caracteres. Por ejemplo: "C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA – JU:ES-L123456789W

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	${ID} es el identificador para el profesional del ámbito de la Justicia ${Organización} es la organización a la que pertenece. Ver apartado 2.4			– ADMINISTRACIÓN DE JUSTICIA”
7. Authority Key Identifier	Identificador de la clave pública de la CA para el Sector Público. 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 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 2048
9. Subject Key Identifier	Identificador de la clave pública del firmante. 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	Uso permitido de las claves certificadas	Sí	Sí	Normalizado en norma X509 y RFC 5280
10.1. Digital Signature	0			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

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
11. Qualified Certificate Statements	Extensiones cualificadas		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
11.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
11.2. 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.".
11.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
11.4. 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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
11.5. QcSSCD (0.4.0.1862.1.4)		Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
12. Certificate Policies	Política de certificación	Sí	No	
12.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.6	Sí		Identificador de la política asociado a la DPC o PC
12.2. Policy Qualifier Id				
12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
12.2.2 User Notice	Certificado cualificado firma electrónica centralizada con seudónimo (Administración Justicia). Sujeto a condiciones de uso de DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
12.3. Policy Identifier	QCP-n-qscd(OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
12.4. Policy Identifier	2.16.724.1.3.5.4.1	Sí		Identificador de la política asociado al certificado de empleado público con seudónimo de nivel alto según normativa nacional.
13. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
13.1. rfc822 Name	Correo electrónico del empleado público	No		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.
13.2. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados.
13.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. Id Campo/Valor: 2.16.724.1.3.5.4.1.1= CERTIFICADO ELECTRÓNICO EMPLEADO PUBLICO	Sí		UTF8 String. OID=2.16.724.1.3.5.4.1.1

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	SEUDONIMO (nivel alto)			
13.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado.	Sí		UTF8 String. OID=2.16.724.1.3.5.4.1.2
13.2.3 NIF entidad	Número único de identificación de la entidad (NIF) En caso del CGPJ: S2804008G y en el caso del MJU: S2813001A	Sí		UTF8 String OID= 2.16.724.1.3.5.4.1.3
13.2.4 Correo electrónico	Correo electrónico de contacto	No		UTF8String. OID=2.16.724.1.3.5.4.1.9.
13.2.5 Unidad organizativa	Unidad, dentro de la administración, en la que está incluida el firmante del certificado Ver apartado 2.3	No		UTF8String. OID=2.16.724.1.3.5.4.1.10 2.16.724.1.3.5.4.1.2= ADMINISTRACIÓN DE JUSTICIA 2.16.724.1.3.5.4.1.2=CONSEJO GENERAL DEL PODER JUDICIAL
13.2.6 Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2	Sí		UTF8String. OID=2.16.724.1.3.5.4.1.11.
13.2.7 Seudónimo	Seudónimo: JU:ES-${ID} Ver apartado 2.1	Sí		UTF8String. OID=2.16.724.1.3.5.4.1.12
13.2.8 Nombre	Nombre de pila del profesional del ámbito de la Justicia	Sí		UTF8String. OID=2.16.724.1.3.5.7.1.6
13.2.9 Primer apellido	Primer apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.1.7

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
13.2.10 Segundo apellido	Segundo apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.1.8
14. CRL Distribution Point	Punto de distribución (localizador) de la CRL	Sí	No	
14.1. 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).
14.2. 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).
15. Authority Info Access		Sí	No	
15.1. 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
15.2. Acces Location 1	http://ocspsp.cert.fnmt.es/ocspsp/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación:	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*

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	1.3.6.1.5.5.7.48.2 (ca cert)			*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."*
15.4. 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.
16. 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.*
16.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

3.6. CERTIFICADO DE EMPLEADO PÚBLICO EN QSCD NIVEL MEDIO

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 certificado. 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	Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
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. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. Ou=CERES	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
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. 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 (rfc5280)
5. Validity	Hasta el 31 de diciembre de 2028	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" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
6.2. Organization	Denominación (nombre "oficial" de organización) del	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)			o=MINISTERIO DE ECONOMÍA
6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String
6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.6. Title	Puesto de trabajo o cargo	Opcional		UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.7. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) +

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	(UTF8String tamaño máximo 15 caracteres)			Número de identidad (Printable String)) Size [RFC 5280] 64
6.8. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.9. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
6.10. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. 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 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 asociada al empleado público, 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	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).

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
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	1			Ver X509 y RFC 5280
10.4. Data Encipherment	0			Ver X509 y RFC 5280 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
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. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Opcional		*Necesaria para realizar logon en Windows. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado*
11.3. Document Signing	1.3.6.1.4.1.311.10.3.12	Si		Firma de documentos.
11.4. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Si		Firma de documentos PDF.
12. Qualified Certificate Statements		Sí	No	
12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado 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 certificado que se dispone de los datos de registro

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				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)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Sí		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
12.6. QcSSCD (0.4.0.1862.1.4)		Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
13. Certificate Policies	Política de certificación	Sí	No	
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.7	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 firma electrónica cualificada de empleado público. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106–	Sí		UTF8 String. Longitud máxima 200 caracteres.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	28009–Madrid–España)			
13.3. Policy Identifier	QCP-n-qscd (OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
13.4. Policy Identifier	2.16.724.1.3.5.7.2	Sí		Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional.
14. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
14.1. rfc822 Name	Correo electrónico del empleado público	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. UPN	UPN (nombre de login de red) para smartcard logon.	Opcional		Campo destinado a incluir el Smartcard logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.3. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración.
14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)	Sí		UTF8 String. 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
14.3.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.2.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.3=Q2826004J
14.3.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.2.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.4 =99999999R
14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.2.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.6=JUAN
14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor:	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.7=ESPAÑOL

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		2.16.724.1.3.5.7.2.7 =<Apellido 1>			
	14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.8 =<Apellido 2>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.8=ESPAÑOL
	14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.9=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.
	14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.2.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point		Punto de distribución (localizador) de la CRL	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).

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
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).
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://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) 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/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	Sí	Sí	De la rf5280: "*This extension MAY appear as a critical or non-critical extension in end entity certificates.*

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	cadenas de certificación". También sirve para distinguir una CA de las entidades finales			
17.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

3.7. CERTIFICADO DE AUTENTICACIÓN EMPLEADO PÚBLICO EN QSCD NIVEL ALTO

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 certificado. 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	Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
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. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable	Sí		UTF8 String, tamaño máximo 64 (rfc5280)

		de la emisión del certificado. Ou=CERES		
	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. 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 (rfc5280)
5. Validity		Hasta el 31 de diciembre de 2028	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" por tratarse de entidades públicas. C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de organización) del suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)	Sí	UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí	UTF8 String
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional	UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso

				contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional	UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.6. Title	Puesto de trabajo o cargo	Opcional	UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.7. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí	Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
	6.8. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí	UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
	6.9. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí	UTF8String (rfc5280). Por ejemplo: gn=JUAN
	6.10. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí	UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier		Identificador de la clave pública de la CA	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT

	para la Administración Pública. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.			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 asociada al empleado público, 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	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	0			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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
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.
12. Certificate Policies	Política de certificación	Sí	No	
12.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.9	Sí		Identificador de la política asociado a la DPC o PC
12.2. Policy Qualifier Id				
12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
12.2.2 User Notice	Certificado de autenticación de empleado público nivel alto. 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.
12.3. Policy Identifier	NCP+ 0.4.0.2042.1.2	Sí		Certificado acorde a una política normalizada, en dispositivo seguro acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
12.4. Policy Identifier	2.16.724.1.3.5.7.1	Sí		Identificador de la política asociado al certificado de empleado público de nivel alto según normativa nacional.
13. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
13.1. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración.
13.1.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO DE	Sí		UTF8 String. 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO DE AUTENTICACION (nivel alto)

	AUTENTICACION (nivel alto)		
13.1.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.2=< Entidad Suscriptora>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.2=MINISTERIO DE ECONOMÍA Y HACIENDA
13.1.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.1.3 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.3=Q2826004J
13.1.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.1.4 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.4 =99999999R
13.1.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.1.5 =<NRP>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
13.1.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.6 =<Nombre de pila>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.6=JUAN
13.1.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor:	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.7=ESPAÑOL

		2.16.724.1.3.5.7.1.7 =<Apellido 1>		
	13.1.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.8 =<Apellido 2>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.8=ESPAÑOL
	13.1.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.9 =<email de contacto>	Opcional	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.9=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.
	13.1.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.10 =<Unidad Organizativa>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	13.1.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.1.11 =<Puesto/Cargo>	Opcional	UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	No
	14.1. 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).

14.2. 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).
15. Authority Info Access		Sí	No	
15.1. 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
15.2. Access Location 1	http://ocspsp.cert.fnmt.es/ocspsp/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
15.3. 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.*"
15.4. Access 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.
16. 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.*

16.1. Subject Type	Entidad final (valor FALSE)	Con este certificado no se pueden emitir otros

3.8. CERTIFICADO DE FIRMA EMPLEADO PÚBLICO EN QSCD NIVEL ALTO

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 certificado. 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	Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
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. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. Ou=CERES	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
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. 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 (rfc5280)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
5. Validity		Hasta el 31 de diciembre de 2028	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" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de organización) del suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.6. Title	Puesto de trabajo o cargo	Opcional		UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
6.7. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
6.8. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.9. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
6.10. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. 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 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 asociada al empleado público, 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	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			Ver X509 y RFC 5280

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
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. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos.
11.2. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Qualified Certificate Statements		Sí	No	
12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado 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 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.”.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Sí		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
12.6. QcSSCD (0.4.0.1862.1.4)		Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
13. Certificate Policies	Política de certificación	Sí	No	
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.10	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 firma electrónica de empleado público nivel alto. 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-n-qscd (OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
13.4. Policy Identifier	2.16.724.1.3.5.7.1	Sí		Identificador de la política asociado al certificado de empleado público de nivel alto según normativa nacional.
14. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
14.1. rfc822 Name	Correo electrónico del empleado público	Opcional		Por ejemplo: rfc822Name=jespanol@meh.es Se establecerá el valor del e-mail contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.2. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración.
14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.1.1 = CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO (nivel alto)	Sí		UTF8 String. 2.16.724.1.3.5.7.1.1 = CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO (nivel alto)
14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.2=MINISTERIO DE ECONOMÍA Y HACIENDA
14.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.1.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.3=Q2826004J
14.2.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.1.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.4 =99999999R
14.2.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.1.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.2.6 Nombre	Nombre de pila del suscriptor del certificado	Sí		UTF8 String. Por ejemplo:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	Id Campo/Valor: 2.16.724.1.3.5.7.1.6 =<Nombre de pila>			2.16.724.1.3.5.7.1.6=JUAN
14.2.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.7=ESPAÑOL
14.2.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.8 =<Apellido 2>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.8=ESPAÑOL
14.2.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.9=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.
14.2.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.2.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.1.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point	Punto de distribución (localizador) de la CRL	Sí	No	
15.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacsp/CRL<xxx*>.crl	Sí		Ruta donde reside la CRL (punto de distribución 1).

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	*xxx: número entero identificador de la CRL (CRL particionadas)			
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).
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://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) 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/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". 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

3.9. CERTIFICADO CENTRALIZADO DE CARRERA JUDICIAL

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	Sha256withRsaEncryption	Si		String. Algoritmo utilizado para la encriptación OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name	Autoridad de Certificación emisora del certificado	Si		
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. Organizational Unit	Unidad organizativa dentro del prestador de servicios de confianza, responsable de la emisión del certificado. ou=CERES	Si		UTF8 String, tamaño máximo 64 (rfc5280)
4.4. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora.			UTF8 String. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)

Campo		Contenido	Obligatorio	Criticidad	Descripción
		organizationIdentifier=VATES-Q2826004J			
	4.5. Common Name	CA del prestador de servicios de confianza bajo la cual se genera el certificado electrónico cn=AC Sector Público	Si		UTF8 String, tamaño máximo 64 (rfc5280)
5. Validity		Hasta el 31 de diciembre de 2028	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 en el que resida el titular de servicios de confianza PSC de acuerdo con la ISO 3166.
	6.2. Organization	O=PODER JUDICIAL	Si		UTF8 String, tamaño máximo 64 (rfc5280) Nombre oficial de la organización al que pertenece el titular del certificado
	6.3. Organizational Unit	OU=CERTIFICADO ELECTRÓNICO DE LA CARRERA JUDICIAL	Si		UTF8 String, tamaño máximo 64 (rfc5280)
	6.4. Organizational Unit	Ejemplo: "OU=0100241002 - Juzgado de Primera Instancia e Instrucción Nº 2 de Amurrio"	No		UTF8 String, tamaño máximo 200 (rfc5280). Órgano en el que presta servicio el titular. Codificación es código de unidad funcional CTEAJE[1] – descripción.
	6.5. Id (Serial Number)	Ejemplo: SN=JU:ES-J000000000R	Sí		PrintableString, tamaño 17 (rfc5280).

[1] Tablas de datos maestros - cteaje

Campo		Contenido	Obligatorio	Criticidad	Descripción
					Identificador unívoco diferente al NIF del titular del certificado electrónico. Seguirá el formato JU:ES-J000000000R
	6.6. Title (2.5.4.12)	Ejemplo: T=MAGISTRADA	Sí		UTF8String, tamaño máximo 64 caracteres (rfc5280). Categoría profesional del titular: - Magistrado/a del Tribunal Supremo - Magistrado/a - Juez/a - Magistrado/a Suplente - Juez/a Sustituto/a
	6.7. Surname	Apellidos del titular del certificado de acuerdo con el documento de identidad Ejemplo: sn=ESPAÑOL ESPAÑOL	Sí		UTF8String, tamaño máximo 50 caracteres.
	6.8. Given Name	Nombre del titular certificado de acuerdo con el documento de identidad. Ejemplo: gn=JUAN	Sí		UTF8String, tamaño máximo 50 caracteres.
	6.9. Common Name	Tendrá el formato PODER JUDICIAL-${title}-${GivenName} ${Surname}-${ID} Ejemplo: PODER JUDICIAL-MAGISTRADO-JUAN ESPAÑOL ESPAÑOL-JU:ES-J000000000R	Sí		UTF8String tamaño máximo 200 caracteres. Es el nombre amigable del certificado se compondrá de la concatenación de los siguientes campos: - "Poder Judicial" - "-" - Title - "-" - Given Name - Surname - "-" - Id
7. Autority Key Identifier		Identificador de la clave pública de la CA para el Sector Público. 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.

Campo	Contenido	Obligatorio	Criticidad	Descripción
8. Subject Public Key Info	Clave pública del Firmante, 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 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	1	Sí		Uso de autenticación (0 – NO / 1 – SI)
10.2. Content Commitment	1	Sí		Firma Electrónica (0 – NO / 1 – SI)
10.3. Key Encipherment	1	Sí		Cifra de claves (0 – NO / 1 – SI)
10.4. Data Encipherment	0			Cifra de datos (0 – NO / 1 – SI)
10.5. Key Agreement	0	Sí		Negociado de claves(0 – NO / 1 – SI)
10.6. Key Certificate Signature	0	Sí		Verificar firmas de otros certificados (0 – NO / 1 – SI)
10.7. CRL Signature	0	Sí		Firma de Certification Revocation List CRL (0 – NO / 1 – SI)
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.
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	Extensiones cualificadas		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.

Campo	Contenido	Obligatorio	Criticidad	Descripción
12.1. QcCompliance (0.4.0.1862.1.1)	Certificado es cualificado	Sí		Indica que el certificado 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 certificado que se dispone de los datos de registro y otra información relevante
12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
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}	Si		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Si		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
	NameRegistrationAuthorities https://poderjudicial.es	Si		
12.6. QcSSCD (0.4.0.1862.1.4)		Si		La clave privada asociada al certificado reside en un dispositivo QSCD
13. Certificate Policies		Sí		Políticas de certificación
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.8	Sí		Identificador de la política de identificación . Política a definida por el PSC en el que se encuadre este certificado
13.2. Policy Qualifier ID				
13.2.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URI a la CPS o declaración de política de certificación
13.2.2. User Notice	Certificado Electrónico de la Carrera Judicial. Consulte condiciones de uso en la DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres Texto para mostrar al usuario de forma previa a usar el certificado electrónico "Certificado Electrónico de la Carrera Judicial. Consulte condiciones de uso en la DPC de FNMT-RCM,

Campo	Contenido	Obligatorio	Criticidad	Descripción
				NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)"
13.3. **Policy Identifier**	QCP-n-qscd (OID:0.4.0.194112.1.2)	Si		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
13.4. **Policy Identifier**	2.16.724.6.0.1.1.5	Sí		String. Identificador de política de Consejo General del Poder Judicial 2.16.724.6.0.1.1.5- Con dispositivo cualificado de creación de firma: HSM
14. Subject Alternative Names		Sí	No	Identificación/descripción del Representante y de la Entidad representada
14.1. Directory Name		Si		
14.1.1. Entidad Suscriptora	Id Campo/Valor: 1.3.6.1.4.1.5734.1.6=CONSEJO GENERAL DEL PODER JUDICIAL	Si		UTF8 String Nombre de la entidad propietaria del certificado
14.1.2. NIF Entidad Suscriptora	1.3.6.1.4.1.5734.1.7=S2804008G	Si		UTF8 String. NIF del Consejo General del Poder Judicial codificado según ETSI TS 319 412-1.
14.1.3. Nombre	Id Campo/Valor: 1.3.6.1.4.1.5734.1.1=<nombre>	Sí		UTF8 String Nombre de pila del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.1=JUAN
14.1.4. Apellido 1	Id Campo/Valor: 1.3.6.1.4.1.5734.1.2=<apellido1>	Sí		UTF8 String Primer apellido del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
14.1.5. Apellido2	Id Campo/Valor: 1.3.6.1.4.1.5734.1.3=<apellido2>	Sí		UTF8 String. Segundo apellido del suscriptor del certificado Id Campo/Valor:

Campo	Contenido	Obligatorio	Criticidad	Descripción
				1.3.6.1.4.1.5734.1.3=ESPAÑOL
15. CRL Distribution Point	Puntos de distribución de las listas de distribución de las listas de revocación de los certificados Electrónicos	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		URI. 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		URI. Ruta del servicio LDAP 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 OSCP - 1.3.6.1.5.5.7.48.1	Sí		Acceso al servicio OCSP
16.2. Access 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) 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/ACSP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.

Campo	Contenido	Obligatorio	Criticidad	Descripción
17. 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.
17.1. cA	Entidad Final (valor False)	Sí		Boolean Indica que el certificado no es de una autoridad de certificación. Con este certificado no se pueden emitir otros.

4. PERFIL DE CERTIFICADO DE AC SECTOR PÚBLICO 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)

Campo	Contenido	Obligatorio	Criticidad	Descripción
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 64 (X520). Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
4.4. Common Name	CA del prestador de servicios de confianza bajo la cual se genera 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
6. Subject		Si		Identificación del titular asociado a la clave pública

Campo		Contenido	Obligatorio	Criticidad	Descripción
	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. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
	6.4. Common Name	CA del prestador de servicios de confianza bajo la cual se genera el certificado electrónico. El valor que tomará será (según CA subordinada) cn= AC SECTOR PÚBLICO G2	Si		UTF8 String, tamaño máximo 64 (rfc5280) -
7. Authority 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).

Campo	Contenido	Obligatorio	Criticidad	Descripción
10. Key Usage		Sí	Sí	Normalizado en norma X509 y RFC 5280.
10.1. Digital Signature	0	Sí		Uso de autenticación (0 – NO / 1 – SI)
10.2. Content Commitment	0	Sí		Firma Electrónica (0 – NO / 1 – SI)
10.3. Key Encipherment	0	Sí		Cifra de claves (0 – NO / 1 – SI)
10.4. Data Encipherment	0			Cifra de datos (0 – NO / 1 – SI)
10.5. Key Agreement	0	Sí		Negociado de claves(0 – NO / 1 – SI)
10.6. Key Certificate Signature	1	Sí		Verificar firmas de otros certificados (0 – NO / 1 – SI)
10.7. CRL Signature	1	Sí		Firma de Certification Revocation List CRL (0 – NO / 1 – SI)
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. 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 publicación de la CRL1	Sí		Ruta donde reside la CRL (punto de distribución 1).

Campo	Contenido	Obligatorio	Criticidad	Descripción
	http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl			
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."
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			

5. PERFILES DE CERTIFICADO DE ENTIDADES FINALES

5.1. CERTIFICADO DE EMPLEADO PÚBLICO

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 certificado. 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. organizationIdentifier=VAT ES-Q2826004J	Sí		UTF8 String. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
	4.4. Common Name	cn= AC SECTOR PÚBLICO G2	Sí		UTF8 String (rfc5280)
5. Validity		3 años	Sí		Validez del certificado

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí		
	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 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de organización) del suscriptor del certificado	Sí		UTF8 String, tamaño máximo 200. Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí		
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.6. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	6.7. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte)	Sí		UTF8String tamaño máximo 50 caracteres. Por ejemplo: gn=JUAN
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Sí		UTF8String tamaño máximo 168 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier		Identificador de la clave pública de la CA para la Administración Pública. 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 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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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.
	11.4. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Sí		*Necesaria para realizar logon en Windows*
12. Qualified Certificate Statements			Sí	No	
	12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado 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 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.".
	12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.5 id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Sí		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
13. Certificate Policies		Política de certificación	Sí	No	
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.23.1.0	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 firma electrónica de empleado público. 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-n (OID:0.4.0.194112.1.0)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)
	13.4. Policy Identifier	2.16.724.1.3.5.7.2	Sí		Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional.
14. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Sí	No	
	14.1. rfc822 Name	Correo electrónico del empleado público	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.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
14.2. UPN	UPN (nombre de login de red) para smartcard logon.	Opcional		Campo destinado a incluir el Smartcard logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.3. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.
14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)	Sí		UTF8 String. 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)
14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
14.3.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.2.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.3=Q2826004J
14.3.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.2.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.4 =00000000T
14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		Id Campo/Valor: 2.16.724.1.3.5.7.2.5 =<NRP>			se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.6=JUAN
	14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.7=ESPAÑOL
	14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.8 =<Apellido 2>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.8=ESPAÑOL
	14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.9=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.
	14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.2.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				este campo no estará presente en el certificado.
15. CRL Distribution Point	Punto de distribución (localizador) de la CRL	Sí	No	
15.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacspG2/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		Acceso al servicio OCSP
16.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspG2/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/ACSPG2.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.*

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
17.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

5.2. CERTIFICADO CON SEUDÓNIMO DE LA ADMINISTRACIÓN DE JUSTICIA

	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 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**	ecdsa-with-SHA256	Sí		OID: 1.2.840.10045.4.3.2
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.
	4.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Sí		Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). 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
	4.4. CommonName	cn= AC SECTOR PÚBLICO G2	Sí		UTF8 String.
5.	**Validity**	3 Años	Sí		Validez del Certificado
6.	**Subject**	Identificación del titular	Sí		

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
6.1. Country	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 suscriptor del certificado	Sí		Por ejemplo: O=ADMINISTRACION DE JUSTICIA
6.3. Organizational Unit	Habitualmente, Unidad Organizativa. En este caso, para mejorar la compatibilidad de los certificados de seudónimo del ámbito de la AGE, se incluye una indicación al respecto. (UTF8String tamaño máximo 64 caracteres)	Sí		Descripción del tipo de certificado. En este caso: "CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO"
6.4. Organizational Unit	Unidad, dentro de la administración, en la que está incluida el suscriptor del certificado Ver apartado 2.3 (UTF8String tamaño máximo 64 caracteres)	No		UTF8String, tamaño máximo 64 caracteres Ejemplo: OU = CONSEJO GENERAL DEL PODER JUDICIAL OU = ADMINISTRACIÓN DE JUSTICIA
6.5. Pseudonym (Oid 2.5.4.65)	"JU:ES-${ID}" ${ID} es el identificador para el profesional del ámbito de la Justicia Ver apartado 2.1 (UTF8String tamaño máximo 40 caracteres)	Sí		UTF8String (rfc5280), tamaño máximo 128 caracteres. ${ID} = CARGO (1) + CODIGO (9) + DG (1) Por ejemplo: JU:ES-L123456789W
6.6. Title	Profesión o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2 (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8String, tamaño máximo 64 caracteres. Por ejemplo: Title=CARRERA JUDICIAL Title=CARRERA FISCAL Title=C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA
6.7. CommonName	Tendrá el formato	Sí		UTF8String tamaño máximo 108 caracteres. Por ejemplo:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	${title} – JU:ES-${ID} – ${Organización} ${title} es el puesto o cargo ${ID} es el identificador para el profesional del ámbito de la Justicia ${Organización} es la organización a la que pertenece. Ver apartado 2.4			"C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA – JU:ES-L123456789W – ADMINISTRACIÓN DE JUSTICIA"
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		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*. 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**	Uso permitido de las claves certificadas.	Sí	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.
10.6. Key Certificate Signature	0	Sí		Ver X509 y RFC 5280.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
10.7. CRL Signature	0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage	Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
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		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.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
12.1. QcCompliance	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Sigue vigente para el OID la norma TS 101 862
12.2. QcType	Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
12.3. QcPDS	{https://www.cert.fnmt.es/pds/PDS_SP_es.pdf,es} {https://www.cert.fnmt.es/pds/PDS_SP_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.4. QcEuRetentionPeriod	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.
13. Certificate Policies	Política de certificación	Sí		
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.23.3.0	Sí		Identificador de la política establecido por el Prestador.
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 empleado público con seudónimo del ámbito de Justicia. Sujeto a las condiciones de uso	Sí		UTF8 String.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid–España)			
13.3. Policy Identifier	0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
13.4. Policy Identifier	2.16.724.1.3.5.4.2	Sí		Identificador de la política asociado al certificado de empleado público con seudónimo de nivel medio según normativa nacional
14. **Subject Alternative Names**	Identificación/ descripción de Identidad Administrativa	Sí	No	
14.1. rfc822 Name	Correo electrónico del profesional del ámbito de la Justicia empleado público	Opcional		
14.2. User Principal name	UPN para Smart card logon	No		
14.3. Directory Name				
14.3.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)	Sí		UTF8 String. OID=2.16.724.1.3.5.4.2.1 CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)
14.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.2.
14.3.3. NIF de la entidad suscriptora	Número único de identificación de la entidad. En caso del CGPJ: S2804008G y en el caso del MJU: S2813001A	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.3.
14.3.4. Correo electrónico	Correo electrónico de contacto	No		UTF8String. OID=2.16.724.1.3.5.4.2.9.
14.3.5. Unidad organizativa	Unidad, dentro de la administración, en la que	No		UTF8String. OID=2.16.724.1.3.5.4.2.10

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		está incluida el firmante del certificado Ver apartado 2.3			2.16.724.1.3.5.4.2.2= ADMINISTRACIÓN DE JUSTICIA 2.16.724.1.3.5.4.2.2=CONSEJO GENERAL DEL PODER JUDICIAL
	14.3.6. Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2	Sí		UTF8String. OID=2.16.724.1.3..4.2.11.
	14.3.7. Seudónimo	Seudónimo: JU:ES-${ID} Ver apartado 2.1	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.12
	14.3.8. Nombre	Nombre de pila del profesional del ámbito de la Justicia	Sí		UTF8String. OID=2.16.724.1.3.5.7.2.6
	14.3.9. Primer apellido	Primer apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.2.7
	14.3.10. Segundo apellido	Segundo apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.2.8
15. CRL Distribution Point			Sí	No	
	15.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacspG2/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		URI. 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)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
16.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspG2/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		Certificado de la CA emisora: 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/ACSPG2.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 Representación.
17. **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".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
17.1. cA	Valor FALSE (entidad final)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

5.3. CERTIFICADO CON SEUDÓNIMO

	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 certificado es versión 3 (X509v3).
2.	**Serial Number**	Número identificativo único del certificado.	Sí		Integer. Establecido aleatoriamente y de forma automática por la Entidad de Certificación. RFC5280: Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). Ejemplo: SerialNumber = 111222
3.	**Signature Algorithm**	ecdsa-with-SHA256	Sí		OID: 1.2.840.10045.4.3.2
4.	**Issuer Distinguish Name**	Entidad emisora del certificado (CA Subordinada).	Sí		
	4.1. Country	C=ES	Sí		PrintableString. Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
	4.2. Organization	o=FNMT-RCM.	Sí		UTF8 String. Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado).
	4.3. Organization Identifier	organizationIdentifier=VATES-Q2826004J	Sí		UTF8 String.
	4.4. CommonName	cn= AC SECTOR PÚBLICO G2	Sí		UTF8 String.
5.	**Validity**	3 Años	Sí		Validez del Certificado
6.	**Subject**	Identificación del titular	Sí		
	6.1. Country	C=ES	Sí		PrintableString. Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
	6.2. Organization	Denominación (nombre "oficial" de la	Sí		UTF8String tamaño máximo 64 caracteres.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	organización) del suscriptor del certificado			Por ejemplo: O=FNMT
6.3. Organizational Unit	Habitualmente, Unidad Organizativa. En este caso, para mejorar la compatibilidad de los certificados de seudónimo del ámbito de la Administración, se incluye una indicación al respecto. (UTF8String tamaño máximo 64 caracteres)	Sí		Descripción del tipo de certificado. En este caso: "CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO".
6.4. Organizational Unit	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	No		UTF8String (rfc5280) Por ejemplo: OU=Ceres
6.5. Pseudonym (Oid 2.5.4.65)	Seudónimo del empleado público (UTF8String tamaño máximo 40 caracteres)	Sí		UTF8String (rfc5280) Por ejemplo: Pseudonym=L123456789W
6.6. Title	Profesión o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. (UTF8String tamaño máximo 64 caracteres)	No		UTF8String (rfc5280) Por ejemplo: Title=Director
6.7. CommonName	Tendrá el formato: - Si se incluye el campo *Title:* ${title} – ${Pseudonym} – ${Organización} - Si no se incluye el campo Title: SEUDÓNIMO – ${Pseudonym} – ${Organización}	Sí		UTF8String tamaño máximo 174 caracteres . Por ejemplo: - Si se incluye el campo *Title:* CN= Director - L123456789W – FNMT - Si no se incluye el campo Title: CN= SEUDÓNIMO - L123456789W – FNMT
7. **Authority Key Identifier**	Identificador de la clave pública del PSC. Medio para identificar la clave	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.			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*. 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	Uso permitido de las claves certificadas.	Sí	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.
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	Ver X509 y RFC 5280.
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	Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
12.1. QcCompliance	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Sigue vigente para el OID la norma TS 101 862.
12.2. QcType	Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
12.3. QcPDS	{https://www.cert.fnmt.es/pds/PDS_SP_es.pdf,es} {https://www.cert.fnmt.es/pds/PDS_SP_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.4. QcEuRetentionPeriod	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.
13. Certificate Policies	Política de certificación.	Sí	No	
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.23.2.0	Sí		Identificador de la política establecido por el Prestador.
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 empleado público con seudónimo. Sujeto a las condiciones de uso de la DPC. FNMT-RCM, NIF Q2826004-J C/Jorge Juan 106 – 28009 – Madrid – España	Sí		UTF8 String.
13.3. Policy Identifier	0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
13.4. Policy Identifier	2.16.724.1.3.5.4.2	Sí		Identificador de la política según normativa nacional.
14. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
14.1. rfc822 Name	Correo electrónico del empleado público.	No		
14.2. User Principal name	UPN para Smart card logon	No		
14.3. Directory Name				

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	14.3.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)	Sí		UTF8 String. OID=2.16.724.1.3.5.4.2.1 CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (nivel medio)
	14.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.2.
	14.3.3. NIF de la entidad suscriptora	Número único de identificación de la entidad.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.3.
	14.3.4. Correo electrónico	Correo electrónico de contacto.	No		UTF8String. OID=2.16.724.1.3.5.4.2.9.
	14.3.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluido el firmante del certificado.	No		UTF8String. OID=2.16.724.1.3.5.4.2.10
	14.3.6. Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.	No		UTF8String. OID=2.16.724.1.3.5.4.2.11.
	14.3.7. Seudónimo	Seudónimo.	Sí		UTF8String. OID=2.16.724.1.3.5.4.2.12
15. CRL Distribution Point			Sí	No	
	15.1. Distribution Point 1	Punto de publicación de la CRL http://www.cert.fnmt.es/crlsacspG2/CRL<xxx*>.crl	Sí		Ruta http donde obtener la CRL. <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
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	Obligatoriedad	Criticidad	Especificaciones
16.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspG2/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		Certificado de la CA emisora. RFC5280: "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/ACSPG2.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 AP.
17. **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".	Sí	Sí	RFC5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
17.1. cA	Valor FALSE (entidad final).	Sí		RFC5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

5.4. CERTIFICADO DE FIRMA CENTRALIZADA PARA EMPLEADO PÚBLICO

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 certificado. 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. organizationIdentifier=VATES-Q2826004J	Sí		UTF8 String. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
4.4. Common Name	cn= AC SECTOR PÚBLICO G2	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
5. Validity	3 Años	Sí		Validez del certificado

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí		
	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 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (UTF8String tamaño máximo 64 caracteres)	Sí		
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el firmante (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del firmante (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.6. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) +

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	(UTF8String tamaño máximo 15 caracteres)			Número de identidad (Printable String)) Size [RFC 5280] 64
6.7. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: cn= ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
6.10. Title	Puesto de trabajo o cargo	Opcional		UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. 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 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. Medio para identificar certificados que contienen una clave	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		pública particular y facilita la construcción de rutas de certificación.			(excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage				Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	0			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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
	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. Qualified Certificate Statements				No	
	11.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
	11.2. 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.".
	11.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
11.4. 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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
11.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	No		Indica que el campo subject sigue la semántica propuesta por la EN 319 412-1
11.6. QcSSCD (0.4.0.1862.1.4)		Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
12. Certificate Policies	Política de certificación	Sí	No	
12.1. Policy Identifier	1.3.6.1.4.1.5734.3.23.1.1	Sí		Identificador de la política asociado a la DPC o PC
12.2. Policy Qualifier Id				
12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
12.2.2 User Notice	Certificado cualificado de firma electrónica centralizada de empleado público. Sujeto a las condiciones de uso expuestas en la DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
12.3. Policy Identifier	QCP-n-qscd (OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
12.4. Policy Identifier	2.16.724.1.3.5.7.1	Sí		Identificador de la política asociado al certificado de empleado público de nivel alto según normativa nacional.
13. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
13.1. rfc822 Name		Correo electrónico del empleado público	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.
13.2. Directory Name		Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.
	13.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel alto)	Sí		UTF8 String. 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel alto)
	13.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.2=MINISTERIO DE ECONOMÍA Y HACIENDA
	13.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.1.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.3 =Q2826004J
	13.2.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.1.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.4 =99999999R
	13.2.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.5 =ADM12347

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.1.5 =<NRP>			Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
13.2.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.6 =JUAN
13.2.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.7 =ESPAÑOL
13.2.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.8 =<Apellido 2>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.8=ESPAÑOL
13.2.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.9 =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.
13.2.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
13.2.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración.	Opcional		UTF8 String. Por ejemplo:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	Id Campo/Valor: 2.16.724.1.3.5.7.1.11 =<Puesto/Cargo>			2.16.724.1.3.5.7.1.11 =ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14. CRL Distribution Point	Punto de distribución (localizador) de la CRL	Sí	No	
14.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacspG2/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
15. Authority Info Access		Sí	No	
15.1. 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
15.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspG2/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
15.3. 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.*"
15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSPG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
16. Basic Contraints	Esta extensión sirve para identificar si el sujeto de	Sí	Sí	De la rf5280: " *This extension MAY appear as a critical or*

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	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			*non-critical extension in end entity certificates.*
16.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

5.5. CERTIFICADO DE FIRMA CENTRALIZADA CON SEUDÓNIMO DE LA ADMINISTRACIÓN DE JUSTICIA.

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 certificado. 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. organizationIdentifier=VATES-Q2826004J	Sí		UTF8 String. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
4.4. Common Name	cn= AC SECTOR PÚBLICO G2	Sí		UTF8 String, tamaño máximo 64 (rfc5280)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
5. Validity		3 Años	Sí		Validez del certificado
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí		
	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 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del suscriptor del certificado	Sí		Por ejemplo: O=ADMINISTRACION DE JUSTICIA
	6.3. Organizational Unit	Habitualmente, Unidad Organizativa. En este caso, para mejorar la compatibilidad de los certificados de seudónimo del ámbito de la AGE, se incluye una indicación al respecto. (UTF8String tamaño máximo 64 caracteres)	Sí		Descripción del tipo de certificado. En este caso: "CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO"
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el firmante Ver apartado 2.3 (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Ejemplo: OU = CONSEJO GENERAL DEL PODER JUDICIAL OU = ADMINISTRACIÓN DE JUSTICIA
	6.5. Pseudonym (Oid 2.5.4.65)	"JU:ES-${ID}" ${ID} es el identificador para el profesional del ámbito de la Justicia	Sí		UTF8String (rfc5280), tamaño máximo 128 caracteres. ${ID} = CARGO (1) + CODIGO (9) + DG (1) Por ejemplo:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	(UTF8String tamaño máximo 40 caracteres)			JU:ES-L123456789W
6.6. Title	Profesión o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2 (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8String, tamaño máximo 64 caracteres. Por ejemplo: Title=CARRERA JUDICIAL Title=CARRERA FISCAL Title=C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA
6.7. Common Name	Tendrá el formato ${title} – JU:ES-${ID} – ${Organización} ${title} es el puesto o cargo ${ID} es el identificador para el profesional del ámbito de la Justicia ${Organización} es la organización a la que pertenece. Ver apartado 2.4	Sí		UTF8String tamaño máximo 108 caracteres. Por ejemplo: "C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA – JU:ES-L123456789W – ADMINISTRACIÓN DE JUSTICIA"
7. Authority Key Identifier	Identificador de la clave pública de la CA para el Sector Público 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.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. ECC P-256 bits

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	En este caso Secp256r1.			
9. Subject Key Identifier	Identificador de la clave pública del firmante. 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	Uso permitido de las claves certificadas	Sí	Sí	Normalizado en norma X509 y RFC 5280
10.1. Digital Signature	0			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. Qualified Certificate Statements	Extensiones cualificadas		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
11.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
11.2. 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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
						expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.”.
	11.3. QcType (0.4.0.1862.1.6)		Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	11.4. 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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	11.5. QcSSCD (0.4.0.1862.1.4)			Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
12. Certificate Policies			Política de certificación	Sí	No	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.23.3.1	Sí		Identificador de la política asociado a la DPC o PC
	12.2. Policy Qualifier Id					
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		12.2.2 User Notice	Certificado cualificado firma electrónica centralizada con seudónimo (Administración Justicia). Sujeto a condiciones de uso de DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
	12.3. Policy Identifier		QCP-n-qscd(OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					policy-identifiers(1) qcp-natural-qscd (2)
	12.4. Policy Identifier	2.16.724.1.3.5.4.1	Sí		Identificador de la política asociado al certificado de empleado público con seudónimo de nivel alto según normativa nacional.
13. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Sí	No	
	13.1. rfc822 Name	Correo electrónico del empleado público	No		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.
	13.2. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados.
	13.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. Id Campo/Valor: 2.16.724.1.3.5.4.1.1= CERTIFICADO ELECTRÓNICO EMPLEADO PUBLICO SEUDONIMO (nivel alto)	Sí		UTF8 String. OID=2.16.724.1.3.5.4.1.1
	13.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado.	Sí		UTF8 String. OID=2.16.724.1.3.5.4.1.2
	13.2.3 NIF entidad	Número único de identificación de la entidad (NIF) En caso del CGPJ: S2804008G y en el caso del MJU: S2813001A	Sí		UTF8 String OID= 2.16.724.1.3.5.4.1.3
	13.2.4 Correo electrónico	Correo electrónico de contacto	No		UTF8String. OID=2.16.724.1.3.5.4.1.9.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	13.2.5 Unidad organizativa	Unidad, dentro de la administración, en la que está incluida el firmante del certificado Ver apartado 2.3	No		UTF8String. OID=2.16.724.1.3.5.4.1.10 2.16.724.1.3.5.4.1.2= ADMINISTRACIÓN DE JUSTICIA 2.16.724.1.3.5.4.1.2=CONSEJO GENERAL DEL PODER JUDICIAL
	13.2.6 Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado. Ver apartado 2.2	Sí		UTF8String. OID=2.16.724.1.3.5.4.1.11.
	13.2.7 Seudónimo	Seudónimo: JU:ES-${ID} Ver apartado 2.1	Sí		UTF8String. OID=2.16.724.1.3.5.4.1.12
	13.2.8 Nombre	Nombre de pila del profesional del ámbito de la Justicia	Sí		UTF8String. OID=2.16.724.1.3.5.7.1.6
	13.2.9 Primer apellido	Primer apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.1.7
	13.2.10 Segundo apellido	Segundo apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí		UTF8 String. OID=2.16.724.1.3.5.7.1.8
14. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	No	
	14.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacspG2/CRL<xxx*>.crl	Sí		Ruta donde reside la CRL (punto de distribución 1).

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	*xxx: número entero identificador de la CRL (CRL particionadas)			
15. Authority Info Access		Sí	No	
15.1. 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
15.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspG2/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
15.3. 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.*"
15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSPG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
16. 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.*

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
16.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

5.6. CERTIFICADO DE EMPLEADO PÚBLICO EN QSCD NIVEL MEDIO

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 certificado. 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. organizationIdentifier=VAT ES-Q2826004J	Sí		UTF8 String. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
4.4. Common Name	cn= AC SECTOR PÚBLICO 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		

Campo	Contenido	Obligatoriedad	Criticidad	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 (rfc5280)
6.2. Organization	Denominación (nombre "oficial" de organización) del suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí		
6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.6. Title	Puesto de trabajo o cargo	Opcional		UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
6.7. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
6.8. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.9. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
6.10. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. 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 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

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
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. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Opcional		*Necesaria para realizar logon en Windows. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado*
11.3. Document Signing	1.3.6.1.4.1.311.10.3.12	Si		Firma de documentos.
11.4. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Si		Firma de documentos PDF.
12. Qualified Certificate Statements		Sí	No	
12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado 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 certificado que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga: "Conservar registrada por

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				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)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.5 id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Sí		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
1.1. QcSSCD (0.4.0.1862.1.4)		Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
13. Certificate Policies	Política de certificación	Sí	No	
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.23.1.2	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 firma electrónica cualificada de empleado público. 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-n-qscd (OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				policy-identifiers(1) qcp-natural-qscd (2)
13.4. Policy Identifier	2.16.724.1.3.5.7.2	Sí		Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional.
14. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
14.1. rfc822 Name	Correo electrónico del empleado público	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. UPN	UPN (nombre de login de red) para smartcard logon.	Opcional		Campo destinado a incluir el Smartcard logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.3. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración.
14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)	Sí		UTF8 String. 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (nivel medio)
14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
14.3.3 NIF entidad	Número único de identificación de la entidad (NIF)	Sí		UTF8 String, tamaño 9. Por ejemplo:

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	Id Campo/Valor: 2.16.724.1.3.5.7.2.3 =<NIF>			2.16.724.1.3.5.7.2.3=Q2826004J
14.3.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.2.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.4 =99999999R
14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.2.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.6=JUAN
14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.7=ESPAÑOL
14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.8 =<Apellido 2>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.8=ESPAÑOL
14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.2.9=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.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.2.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	No	
	15.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacspG2/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		Acceso al servicio OCSP
	16.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspgG2/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*

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				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/ACSPG2.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

5.7. CERTIFICADO DE AUTENTICACIÓN EMPLEADO PÚBLICO EN QSCD NIVEL ALTO

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 certificado. 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. organizationIdentifier=VATES-Q2826004J	Sí		UTF8 String. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
4.4. Common Name	cn= AC SECTOR PÚBLICO G2	Sí		UTF8 String (rfc5280)
5. Validity	3 años	Sí		Validez del certificado

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí		
	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 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de organización) del suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí		
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
6.6. Title	Puesto de trabajo o cargo	Opcional		UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.7. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
6.8. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.9. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
6.10. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. Medio para identificar la clave pública correspondiente a la clave privada	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).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		utilizada por la CA para firmar un certificado.			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	0			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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
	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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
12. Certificate Policies			Política de certificación	Sí	No	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.23.1.4	Sí		Identificador de la política asociado a la DPC o PC
	12.2. Policy Qualifier Id					
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		12.2.2 User Notice	Certificado de autenticación de empleado público nivel alto. 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.
	12.3. Policy Identifier		NCP+ 0.4.0.2042.1.2	Sí		Certificado acorde a una política normalizada,en dispositivo seguro acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
	12.4. Policy Identifier		2.16.724.1.3.5.7.1	Sí		Identificador de la política asociado al certificado de empleado público de nivel alto según normativa nacional.
13. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	No	
	13.1. Directory Name		Identidad Administrativa	Sí		Campos específicos definidos por la Administración.
		13.1.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO	Sí		UTF8 String. 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL ALTO DE AUTENTICACION (nivel alto)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	PUBLICO DE NIVEL ALTO DE AUTENTICACION (nivel alto)			
13.1.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.2=MINISTERIO DE ECONOMÍA Y HACIENDA
13.1.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.1.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.3=Q2826004J
13.1.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.1.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.4 =99999999R
13.1.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.1.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
13.1.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.6=JUAN

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	13.1.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.7=ESPAÑOL
	13.1.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.8 =<Apellido 2>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.8=ESPAÑOL
	13.1.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.9=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.
	13.1.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	13.1.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.1.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	No	
14.1. Distribution Point 1		Punto de publicación de la CRL1	Sí		Ruta donde reside la CRL (punto de distribución 1).

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
	http://www.cert.fnmt.es/crlsacspG2/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)			
15. Authority Info Access		Sí	No	
15.1. 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
15.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspG2/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
15.3. 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.*"
15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSPG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
16. 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.*

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
16.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

5.8. CERTIFICADO DE FIRMA EMPLEADO PÚBLICO EN QSCD NIVEL ALTO

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 certificado. 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. organizationIdentifier=VATES-Q2826004J	Sí		UTF8 String. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
4.4. Common Name	cn= AC SECTOR PÚBLICO 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" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
6.2. Organization	Denominación (nombre "oficial" de organización) del suscriptor del certificado (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO UTF8String tamaño máximo 64 caracteres)	Sí		
6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público. (UTF8String tamaño máximo 64 caracteres)	Opcional		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.6. Title	Puesto de trabajo o cargo	Opcional		UTF8String (rfc5280). Por ejemplo: ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
6.7. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1 (UTF8String tamaño máximo 15 caracteres)	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
6.8. Surname	Apellidos de acuerdo con documento de identificación (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
6.9. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte) (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
6.10. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF (UTF8String tamaño máximo 168 caracteres)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier	Identificador de la clave pública de la CA para la Administración Pública. 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 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	0			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 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
				las normas ETSI EN 319 412-2, ya que es un único perfil
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. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos.
11.2. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Qualified Certificate Statements		Sí	No	
12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí		Indica que el certificado 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 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.".
12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
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		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Sí		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
12.6. QcSSCD (0.4.0.1862.1.4)		Sí		La clave privada asociada al certificado reside en un dispositivo QSCD
13. Certificate Policies	Política de certificación	Sí	No	
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.23.1.3	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 firma electrónica de empleado público nivel alto. 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-n-qscd (OID:0.4.0.194112.1.2)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
13.4. Policy Identifier	2.16.724.1.3.5.7.1	Sí		Identificador de la política asociado al certificado de empleado público de nivel alto según normativa nacional.
14. Subject Alternative Names	Identificación/ descripción de Identidad Administrativa	Sí	No	
14.1. rfc822 Name	Correo electrónico del empleado público	Opcional		Por ejemplo: rfc822Name=jespanol@meh.es Se establecerá el valor del e-mail contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
14.2. Directory Name	Identidad Administrativa	Sí		Campos específicos definidos por la Administración.
14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.1.1 = CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO (nivel alto)	Sí		UTF8 String. 2.16.724.1.3.5.7.1.1 = CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO (nivel alto)
14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.2=MINISTERIO DE ECONOMÍA Y HACIENDA
14.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.1.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.3=Q2826004J
14.2.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.1.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.4 =99999999R
14.2.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.1.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
14.2.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.6=JUAN
14.2.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor:	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.7=ESPAÑOL

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		2.16.724.1.3.5.7.1.7 =<Apellido 1>			
	14.2.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.1.8 =<Apellido 2>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.8=ESPAÑOL
	14.2.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.7.1.9=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.
	14.2.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.1.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.2.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.1.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.7.1.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	No	
15.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacspG2/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	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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://ocspspg2.cert.fnmt.es/ocspspG2/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/ACSPG2.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

5.9. CERTIFICADO CENTRALIZADO DE CARRERA JUDICIAL

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-SHA256	Si		String. Algoritmo utilizado para la encriptación OID: 1.2.840.10045.4.3.2
4. Issuer Distinguish Name	Autoridad de Certificación emisora del certificado	Si		
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. Según la norma técnica ETSI EN 319 412- 1 (VATES + NIF de la entidad)
4.4. Common Name	CA del prestador de servicios de confianza bajo la cual se genera el certificado electrónico	Si		UTF8 String, tamaño máximo 64 (rfc5280)

Campo		Contenido	Obligatorio	Criticidad	Descripción
		cn= AC SECTOR PÚBLICO G2			
5. Validity		4 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 en el que resida el titular de servicios de confianza PSC de acuerdo con la ISO 3166.
	6.2. Organization	O=PODER JUDICIAL	Si		UTF8 String, tamaño máximo 64 (rfc5280) Nombre oficial de la organización al que pertenece el titular del certificado
	6.3. Organizational Unit	OU=CERTIFICADO ELECTRÓNICO DE LA CARRERA JUDICIAL	Si		UTF8 String, tamaño máximo 64 (rfc5280)
	6.4. Organizational Unit	Ejemplo: "OU=0100241002 - Juzgado de Primera Instancia e Instrucción Nº 2 de Amurrio"	No		UTF8 String, tamaño máximo 200 (rfc5280). Órgano en el que presta servicio el titular. Codificación es código de unidad funcional CTEAJE[2] – descripción.
	6.5. Id (Serial Number)	Ejemplo: SN=JU:ES-J000000000R	Sí		PrintableString, tamaño 17 (rfc5280). Identificador unívoco diferente al NIF del titular del certificado electrónico. Seguirá el formato JU:ES-J000000000R de acuerdo con el apartado 2 del presente documento.

[2] Tablas de datos maestros - cteaje

Campo	Contenido	Obligatorio	Criticidad	Descripción
6.6. Title (2.5.4.12)	Ejemplo: T=MAGISTRADA	Sí		UTF8String, tamaño máximo 64 caracteres (rfc5280). Categoría profesional del titular: - Magistrado/a del Tribunal Supremo - Magistrado/a - Juez/a - Magistrado/a Suplente - Juez/a Sustituto/a
6.7. Surname	Apellidos del titular del certificado de acuerdo con el documento de identidad Ejemplo: sn=ESPAÑOL ESPAÑOL	Sí		UTF8String, tamaño máximo 50 caracteres.
6.8. Given Name	Nombre del titular certificado de acuerdo con el documento de identidad. Ejemplo: gn=JUAN	Sí		UTF8String, tamaño máximo 50 caracteres.
6.9. Common Name	Tendrá el formato PODER JUDICIAL-${title}-${GivenName} ${Surname}-${ID} ${ID} es el identificador para el profesional del ámbito de la Justicia ${title} es la categoria A modo de ejemplo CN= PODER JUDICIAL – Magistrado – Juan Español Español - JU:ES-J000000000R	Sí		UTF8String tamaño máximo 200 caracteres. Es el nombre amigable del certificado se compondrá de la concatenación de los siguientes campos: - “Poder Judicial” - “-“ - Title - “-“ - Given Name - Surname - “-“ - Id
7. Authority Key Identifier	Identificador de la clave pública de la CA para el Sector Público. 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

Campo	Contenido	Obligatorio	Criticidad	Descripción
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	1	Sí		Uso de autenticación (0 – NO / 1 – SI)
10.2. Content Commitment	1	Sí		Firma Electrónica (0 – NO / 1 – SI)
10.3. Key Encipherment	0	Sí		Cifra de claves (0 – NO / 1 – SI)
10.4. Data Encipherment	0			Cifra de datos (0 – NO / 1 – SI)
10.5. Key Agreement	0	Sí		Negociado de claves(0 – NO / 1 – SI)
10.6. Key Certificate Signature	0	Sí		Verificar firmas de otros certificados (0 – NO / 1 – SI)
10.7. CRL Signature	0	Sí		Firma de Certification Revocation List CRL (0 – NO / 1 – SI)
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.
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	Extensiones cualificadas		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 es cualificado	Sí		Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente

Campo	Contenido	Obligatorio	Criticidad	Descripción
12.2. 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
12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
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}	Si		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Si		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
	NameRegistrationAuthorities https://poderjudicial.es	Si		
12.6. QcSSCD (0.4.0.1862.1.4)		Si		La clave privada asociada al certificado reside en un dispositivo QSCD
13. Certificate Policies		Sí		Políticas de certificación
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.23.4.1	Sí		Identificador de la política de identificación. Política a definida por el PSC en el que se encuadre este certificado
13.2. Policy Qualifier ID				
13.2.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URI a la CPS o declaración de política de certificación
13.2.2. User Notice	Certificado Electrónico de la Carrera Judicial. Consulte condiciones de uso en la DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres Texto para mostrar al usuario de forma previa a usar el certificado electrónico "Certificado Electrónico de la Carrera Judicial. Consulte condiciones de uso en la DPC de FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)"

Campo	Contenido	Obligatorio	Criticidad	Descripción
13.3. Policy Identifier	QCP-n-qscd (OID:0.4.0.194112.1.2)	Si		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
13.4. Policy Identifier	2.16.724.6.0.1.1.5	Sí		String Identificador de política de Consejo General del Poder Judicial (por ejemplo para tipos de dispositivo de creación de firma y tipos de procedimiento de identificación inicial) Ver apartado 3 - 3. OID de Política de certificación de Consejo General del Poder Judicial 2.16.724.6.0.1.1.1 -Sin dispositivo de creación de firma -2.16.724.6.0.1.1.2 -Con dispositivo no cualificado de creación de firma: HSM-2.16.724.6.0.1.1.3 -Con dispositivo cualificado de creación de firma: tarjeta-2.16.724.6.0.1.1.4 -Con dispositivo cualificado de creación de firma: Token-**2.16.724.6.0.1.1.5 -Con dispositivo cualificado de creación de firma: HSM** Descripción del certificado. http://oid-info.com/get/2.16.724.6.0.1.1
14. Subject Alternative Names		Sí	No	Identificación/descripción del Representante y de la Entidad representada
14.1. Directory Name		Si		
14.1.1. Entidad Suscriptora	Id Campo/Valor: 1.3.6.1.4.1.5734.1.6=CONSEJO GENERAL DEL PODER JUDICIAL	Si		UTF8 String Nombre de la entidad propietaria del certificado
14.1.2. NIF Entidad Suscriptora	1.3.6.1.4.1.5734.1.7=S2804008G	Si		UTF8 String.

Campo	Contenido	Obligatorio	Criticidad	Descripción
				NIF del Consejo General del Poder Judicial codificado según ETSI TS 319 412-1.
14.1.3. Nombre	Id Campo/Valor: 1.3.6.1.4.1.5734.1.1=<nombre>	Sí		UTF8 String Nombre de pila del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.1=JUAN
14.1.4. Apellido 1	Id Campo/Valor: 1.3.6.1.4.1.5734.1.2=<apellido1>	Sí		UTF8 String Primer apellido del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
14.1.5. Apellido2	Id Campo/Valor: 1.3.6.1.4.1.5734.1.3=<apellido2>	Sí		UTF8 String Segundo apellido del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.3=ESPAÑOL
15. CRL Distribution Point	Puntos de distribución de las listas de distribución de las listas de revocación de los certificados Electrónicos	Sí	No	
15.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacspG2/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		URI. 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 OSCP - 1.3.6.1.5.5.7.48.1	Sí		Acceso al servicio OCSP
16.2. Access Location 1	http://ocspspg2.cert.fnmt.es/ocspspG2/OcspResponder	Si		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)	Si		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

Campo	Contenido	Obligatorio	Criticidad	Descripción
				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/ACSPG2.crt	Si		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
17. 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.
17.1. cA	Entidad Final (valor False)	Sí		Boolean Indica que el certificado no es de una autoridad de certificación. Con este certificado no se pueden emitir otros.