Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN

DEPARTAMENTO CERES

DEFINICIÓN PERFILES DE CERTIFICADO EMITIDOS POR AC SECTOR PÚBLICO

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	27/07/2023
Revisado por:	FNMT-RCM	18/08/2023
Aprobado por:	FNMT-RCM	28/08/2023

Referencia:

Documento clasificado como: *Público*

1. Introducción 3
2. Perfil de certificado de CA 4
3. Perfiles de certificado de entidades finales 7
3.1. Certificado de Sello Electrónico 7
3.2. Certificado de Empleado Público 12
3.3. Certificado con Seudónimo de la Administración de Justicia 19
3.4. Certificado con Seudónimo 24
3.5. Certificado de Firma Centralizada para Empleado Público 29
3.6. Certificado de Firma Centralizada con seudónimo de la Administración de Justicia. 36
3.7. Certificado de Empleado Público en QSCD nivel medio 42
3.8. Certificado de Autenticación Empleado Público en QSCD nivel alto 50
3.9. Certificado de Firma Empleado Público en QSCD nivel alto 56

1. INTRODUCCIÓN

El presente documento describe en detalle los perfiles de los distintos tipos de certificado que emitirá la Autoridad de Certificación "*AC Sector Público*", que sustituirá a la actual "*AC Administración Pública*" gestionada por la FNMT-RCM.

Los tipos de certificado que serán emitidos por la nueva CA son:

- Certificado de Sello Electrónico
- 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

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 de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 64 (rfc5280)
	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	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9

Campo			Contenido	Obligatoriedad	Especificaciones
	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
	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	Sí	UTF8 String. Longitud máxima 200 caracteres.

Campo			Contenido	Obligatoriedad	Especificaciones
			de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)		
12. CRL Distribution Point				Sí	
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí	Ruta donde reside la CRL (punto de distribución 1).
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí	Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Authority Info Access					
	13.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
	13.2. Acces Location 1		http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	Sí	URL del servicio OCSP (no autenticado)
	13.3. Access Method 2		Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	Emisor de la entidad emisora de certificados (CA Raíz) 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 SELLO ELECTRÓNICO

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:= 2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del Sello. Este número se asigna de forma aleatoria.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del Sello	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del Sello). o=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del Sello. ou=CERES	Sí		UTF8 String, tamaño máximo 64 (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=VAT ES-Q2826004J	Sí		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn= AC Sector Público	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. Locality	Nombre de la localidad del suscriptor (organización)	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del creador del Sello (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=SELLO ELECTRONICO (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
	6.5. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) (UTF8String tamaño máximo 15 caracteres)	Sí		OrganizationIdentifier p. ej: VATES-S2833002.
	6.6. Serial Number	Número único de identificación de la Entidad suscriptora de servicios de certificación. En este caso el NIF	Sí		Por ejemplo: serialNumber=Q2826004J PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.7. Common Name	Denominación de sistema o aplicación de proceso automático. Se deberá asegurar que dicho nombre tenga sentido y no de lugar a ambigüedades (UTF8String tamaño máximo 64 caracteres)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn=SERVICIO DE REGISTRO DEL MEH
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo 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 sello, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	No	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	1			Ver X509 y RFC 5280
	10.4. Data Encipherment	0			Ver X509 y RFC 5280
	10.5. Key Agreement	0			Ver X509 y RFC 5280
	10.6. Key Certificate Signature	0			Ver X509 y RFC 5280
	10.7. CRL Signature	0			Ver X509 y RFC 5280
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
	11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente.
	11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos.
	11.3. Adobe Authentic Documents Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance (0.4.0.1862.1.1)	Sello cualificado	Sí		Indica que el Sello es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del sello que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".
	12.3. QcType (0.4.0.1862.1.6)	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		Indica que el certificado es de sello electrónico. *Certificate for electronic seals as defined in Regulation (EU) No 910/2014*
	12.4. QcPDS(0.4.0.1862.1.5)	{https://www.cert.fnmt.es/pds/PDS_SP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_SP_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS
	12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Legal (0.4.0.194121.1.2)	Sí		Indica que el campo subject sigue la semántica propuesta por la EN 319 412-1
13. Certificate Policies		Política de certificación	Sí	No	
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.17.1	Sí		Identificador de la política asociado a la DPC o PC

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	13.2. Policy Qualifier Id					
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	"Certificado cualificado de sello electrónico. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106–28009–Madrid–España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.3. Policy Identifier		QCP-l (0.4.0.194112.1.1)	Sí		Certificado cualificado de sello, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)
	13.4. Policy Identifier		2.16.724.1.3.5.6.2	Sí		OID asociado a certificado de sello de nivel medio
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	No	
	14.1. rfc822 Name		Correo electrónico de contacto de la entidad suscriptora	Opcional		Por ejemplo: rfc822Name=sellomeh@meh.es Se establecerá el valor del e-email contacto entidad suscriptora si se aporta en la solicitud de certificado. En caso contrario no se rellenará este valor
	14.2. Directory Name		Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.
		14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.6.2.1=SELLO ELECTRONICO DE NIVEL MEDIO	Sí		UTF8 String.
		14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del Sello. Id Campo/Valor: 2.16.724.1.3.5.6.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.6.2.2=Ministerio de Economía y Hacienda
		14.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.6.2.3=<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.6.2.3=Q2826004J

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		14.2.4 Denominación de sistema o componente	Breve descripción del componente asociado al sello. 2.16.724.1.3.5.6.2.5=<Denominación del Sistema>	Sí		UTF8 String, tamaño máximo 64. Por ejemplo: 2.16.724.1.3.5.6.2.5= SERVICIO DE REGISTRO DEL MEH
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al Sello.	Sí	No	
	15.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacsp/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. Ldap://ldapsp.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Sector%20Publico,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
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.

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

3.2. 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=VAT ES-Q2826004J	Sí		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn= AC Sector Público	Sí		UTF8 String (rfc5280)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
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)
	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
	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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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 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	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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	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.
	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) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	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: 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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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>	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 este campo no estará presente en el certificado.
15. CRL Distribution Point			Punto de distribución (localizador) de la CRL	Sí	No	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	15.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacsp/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2	Punto de publicación de la CRL2. Ldap://ldapsp.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Sector%20Publico,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
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

3.3. 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		PrintableString
	4.5. CommonName	AC Sector Público	Sí		UTF8 String.
5. Validity		3 Años	Sí		Validez del Certificado
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"

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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 ${title} – JU:ES-${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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
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	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.
	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				

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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					
		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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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 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: 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. 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."

3.4. 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		

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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		PrintableString.
	4.5. CommonName	AC Sector Público	Sí		UTF8 String.
5. Validity		3 Años	Sí		Validez del Certificado
6. Subject		Identificación del titular	Sí		
	6.1. Country	ES	Sí		PrintableString. 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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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 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	
	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 fisica, 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?base?objectclass=cRLDistributionPoint	Sí		Ruta del servicio LDAP donde reside la CRL. <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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."

3.5. 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)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Sector Público	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
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 (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.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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 (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, 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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
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 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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
12. Certificate Policies			Política de certificación	Sí	No	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.17.5	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)
	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)

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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 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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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. 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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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. 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 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		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)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Sector Público	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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 ${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. 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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	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 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 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/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	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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: 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. 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

3.7. 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=VAT ES-Q2826004J	Sí		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn= AC Sector Público	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)
	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		

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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 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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
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	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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	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.
	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		1.3.6.1.4.1.5734.3.17.7	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 106–28009–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		2.16.724.1.3.5.7.2	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	

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-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) 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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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.
		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 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

3.8. 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 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=VAT ES-Q2826004J	Sí		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn= AC Sector Público	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
	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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
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		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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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 AUTENTICACION (nivel alto)	Sí		UTF8 String. 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRONICO DE EMPLEADO 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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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: 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	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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

3.9. 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=VAT ES-Q2826004J	Sí		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn= AC Sector Público	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
	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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
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
	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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	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.
	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.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
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. 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

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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 *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. Ldap://ldapsp.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Sector%20Publico,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
16. Authority Info Access			Sí	No	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		Acceso al servicio OCSP
	16.2. 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