



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 ADMINISTRACIÓN PÚBLICA

Referencia:

Documento clasificado como: *Público*

1.	Introducción.....	3
2.	Perfil de certificado de la CA Subordinada para la Administración Pública	3
3.	Perfiles de certificado de entidades finales	6
3.1.	Certificado de Sede Electrónica	6
3.2.	Certificado de Sello Electrónico.....	11
3.3.	Certificado de personal al servicio de la administración (Tarjeta).....	15
3.4.	Certificado de personal al servicio de la administración (Software).....	19
3.5.	Certificado con seudónimo de personal al servicio de la Administración de Justicia.....	23
3.6.	Certificado de empleado público con seudónimo	27
3.7.	Perfil de certificado de personal al servicio de la administración de firma centralizada.....	30

1. INTRODUCCIÓN

En el presente documento se describen en detalle los perfiles de los distintos tipos de certificado que emite la Autoridad de Certificación “AC Administración Pública” gestionada por la FNMT-RCM.

Los tipos de certificado que emite esta CA son:

- Certificado de sede electrónica. Este tipo de certificado se emite para los sitios web, que debido a su naturaleza y a la necesidad de prestar un servicio autenticado, necesitan disponer de un certificado para identificar a la Sede.
- Certificado de sello electrónico para procesos automatizados, cuyo objetivo es permitir a aplicaciones automatizadas autenticarse frente a otras y establecer sesiones seguras.
- Certificado de personal adscrito a la Administración o funcionario con generación de claves en tarjeta inteligente
- Certificado de personal adscrito a la Administración o funcionario con generación de claves en medio equivalente (software)

2. PERFIL DE CERTIFICADO DE LA CA SUBORDINADA PARA LA ADMINISTRACIÓN PÚBLICA

Campo		Contenido	Obligatoriedad
1. Version		2	Sí
2. Serial Number		Número identificativo único del certificado.	Sí
3. Signature Algorithm		Sha256withRsaEncryption	Sí
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	Denominación (nombre “oficial” de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí
	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
5. Validity		12 años	Sí
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí
	6.1. Country	C=ES	Sí



	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	
	6.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	
	6.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí	
	6.5. Common Name	cn=AC Administración Pública	Sí	
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	
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	
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	
10. Key Usage		Uso permitido de las claves certificadas.	Sí	
	10.1. Digital Signature	0	Sí	
	10.2. Content Commitment	0	Sí	
	10.3. Key Encipherment	0	Sí	
	10.4. Data Encipherment	0	Sí	
	10.5. Key Agreement	0	Sí	
	10.6. Key Certificate Signature	1	Sí	
	10.7. CRL Signature	1	Sí	
11. Certificate Policies		Política de certificación	Sí	
	11.1. Policy Identifier	2.5.29.32.0 (anyPolicy)	Sí	
	11.2. Policy Qualifier Id			
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí
12. CRL Distribution Point			Sí	
	12.1. Distribution Point 1	Punto de distribución 1 de la CRL (ARL)	Sí	

		ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	
	12.2. Distribution Point 2	Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí
13. Authority Info Access			
	1.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí
	1.2. Access Location 1	http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Sí
	1.3. 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
	1.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí
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	
	14.2. Path Length	0	

3. PERFILES DE CERTIFICADO DE ENTIDADES FINALES

3.1. CERTIFICADO DE SEDE ELECTRÓNICA

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version	2	Si		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. Este número se asigna de forma aleatoria.	Si		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	Si		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name	Entidad emisora del certificado (CA Subordinada)	Si		
4.1. Country	4.1. Country	C=ES	Si	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	O=FNMT-RCM.	Si	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). UTF8 String, tamaño máximo 64 (rfc5280)
	4.3. Organizational Unit	OU=Ceres	Si	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. UTF8 String, tamaño máximo 64 (rfc5280)
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptor. serialNumber=Q2826004J	Si	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Si	UTF8 String (rfc5280).
5. Validity	1 año	Si		Periodo de vigencia de los certificados
6. Subject	Identificación/descripción del responsable de las claves certificadas	Si		
6.1. Country	6.1. Country	C=ES	Si	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. stateOrProvinceName	Nombre del estado o Provincia	Si	UTF8String (rfc5280). Por ejemplo: ST=Madrid

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	6.2. LocalityName	Nombre de la localidad del suscriptor (organización)	Si		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor	Si		UTF8 String, tamaño máximo 64 (rfc5280)
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: OU=SEDE ELECTRONICA	Si		UTF8 String, tamaño máximo 64 (rfc5280)
	6.5. Organizational Unit	El nombre descriptivo de la sede.	Si		UTF8 String, tamaño máximo 64 (rfc5280) Establecido por la entidad solicitante en el formulario de solicitud.
	6.6. SerialNumber	NIF del suscriptor	Si		PrintableString (rfc5280). Tamaño 64 (X520). En nuestro caso, el tamaño es 9. Por ejemplo: serialNumber=Q0000000J
	6.7. BusinessCategory (OID 2.5.4.15)	businessCategory=Government Entity	Si		UTF8String Guidelines For The Issuance And Management Of Extended Validation Certificates (v1.6.0) – Apartado 9.2.4 OID 2.5.4.15
6.8. jurisdictionCountryName	jurisdictionCountryName=ES	Si		Guidelines For The Issuance And Management Of Extended Validation Certificates (v1.6.0) – Apartado 9.2.5: ASN.1 – X520countryName as specified in RFC 5280 OID: 1.3.6.1.4.1.311.60.2.1.3 Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)	
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.	Si	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 de la sede, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Si	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave es 2048 bits.
9. Subject Key Identifier		Identificador de la clave pública de la sede.	Si	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.	Si	Si	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



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. 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. Server Authentication	1.3.6.1.5.5.7.3.1	Sí		Autenticación TSL web Server
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)	Certificado cualificado	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.2.1 Indica que el certificado es cualificado acorde al Reglamento UE 910/2014.
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.3 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. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Legal (0.4.0.194121.1.2)	No		ETSI EN 319 412-1 Semántica de persona jurídica
	12.4. QcType(0.4.0.1862.1.6)	qct-web (0.4.0.1862.1.6.3)			ETSI EN 319 412-5 V2.1.1 – Apartado 4.2.3 Certificado de autenticación web
	12.5. QcPDS (0.4.0.1862.1.5)	{ https://www.cert.fmmt.es/pds/PDS_AP_es.pdf , { https://www.cert.fmmt.es/pds/PDS_AP_en.pdf , en}			ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.4 Lugar donde se encuentra la declaración PDS, así como el idioma del documento.
13. Certificate Policies		Política de certificación	Sí	No	



Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	13.1. Policy Identifier	QCP-w (0.4.0.194112.1.4)	Si		Certificado cualificado de sitio web acorde al Reglamento UE 910/2014 Itu-t(0) Identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web(4)
	13.2. Policy Identifier	evcp (0.4.0.2042.1.4)	Si		{itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)}
	13.3. Policy Identifier	2.16.724.1.3.5.5.2	Si		OID asociado a los certificados de Sede nivel medio/sustancial según normativa nacional
	13.4. Policy Identifier	1.3.6.1.4.1.5734.3.3.12.1	Si		Identificador de la política asociado a la DPC o PC
	13.4.1 Policy Qualifier Id		Si		
		13.4.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Si	IA5String String. URL de las condiciones de uso.
		13.4.1.2 User Notice	“Certificado cualificado de sede electrónica, nivel medio/sustancial. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)”	Si	UTF8 String. Longitud máxima 200 caracteres.
14. SignedCertificateTimestampList (SCT)					
	14.1. signed certificate timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en un log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.	Si		RFC 6962.
15. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Si	No	
	15.1. DNS Name	Nombre de Dominio (DNS) de la Sede	Si		UTF8 String, tamaño máximo 128. Nombre Dominio donde se encuentra la Sede. Por ejemplo: DNSName = www.sede.meh.gob.es
16. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Si	No	
	16.1. Distribution Point 1	Punto de publicación de la CRL. <a href="http://www.cert.fnmt.es/crlsacp/CRL<xxx*>.crl">http://www.cert.fnmt.es/crlsacp/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Si		Ruta donde reside la CRL (punto de distribución 1).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	16.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Si		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
	17. Authority Info Access		Si	No	
	17.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Si		
	17.2. Access Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Si		
	17.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Si		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: <i>"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."</i>
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Si		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
	18. 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".	Si	Si	De la rfc5280: <i>"This extension MAY appear as a critical or non-critical extension in end entity certificates."</i>
	18.1. Subject Type	Entidad final (valor FALSE)			Con este certificado no se pueden emitir otros

3.2. CERTIFICADO DE SELLO ELECTRÓNICO

Campo		Contenido	Obligatoriedad
1. Version		2	Sí
2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí
3. Signature Algorithm		Sha256withRsaEncryption	Sí
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí
	4.5. Common Name	cn=AC Administración Pública	Sí
5. Validity		2 años	Sí
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
	6.2. Locality	Nombre de la localidad del suscriptor (organización)	Sí
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)	Sí
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=SELLO ELECTRONICO	Sí
	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)	Sí
	6.6. Serial Number	Número único de identificación de la Entidad suscriptora de servicios de certificación. En este caso el NIF	Sí

Campo		Contenido	Obligatoriedad
	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	Sí
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
8. Subject Public Key Info		Clave pública del sello, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
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
10. Key Usage			Sí
	10.1. Digital Signature	1	
	10.2. Content Commitment	1	
	10.3. Key Encipherment	1	
	10.4. Data Encipherment	1	
	10.5. Key Agreement	0	
	10.6. Key Certificate Signature	0	
	10.7. CRL Signature	0	
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Sí
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí
	12.1. QcCompliance (0.4.0.1862.1.1)	Certificado cualificado	Sí
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí
	12.3. QcType (0.4.0.1862.1.6)	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí
	12.4. QcPDS(0.4.0.1862.1.5)	{https://www.cert.fnmt.es/pds/PDS_AP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_AP_en.pdf, en}	Sí
13. Certificate Policies		Política de certificación	Sí
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.3.9.1	Sí
	13.1.1 Policy Qualifier Id		
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/

Campo		Contenido	Obligatoriedad
	13.1.1.2 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
	13.2. Policy Identifier	QCP-1 (0.4.0.194112.1.1)	Sí
	13.3. Policy Identifier	2.16.724.1.3.5.6.2	Sí
14. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Sí
	14.1. rfc822 Name	Correo electrónico de contacto de la entidad suscriptora	Opcional
	14.2. Directory Name	Identidad Administrativa	Sí
	14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.6.2.1=SELLO ELECTRONICO DE NIVEL MEDIO	Sí
	14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.6.2.2=<Entidad Suscriptora>	Sí
	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
	14.2.4 Denominación de sistema o componente	Breve descripción del componente asociado al certificado de sello. 2.16.724.1.3.5.6.2.5=<Denominación del Sistema>	Sí
15. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	15.1. Distribution Point 1	Punto de publicación de la CRL1 <a href="http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl">http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí
	15.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí
16. Authority Info Access			Sí
	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

Campo		Contenido	Obligatoriedad
	16.2. Acces Location 1	http://ocspap.cert.fimt.es/ocspap/OcspResponder	Sí
	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
	16.4. Acces Location 2	http://www.cert.fimt.es/certs/ACAP.crt	Sí
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
	17.1. Subject Type	Entidad final (valor FALSE)	

3.3. CERTIFICADO DE PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN (TARJETA)

Campo		Contenido	Obligatoriedad
1. Version		2	Si
2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si
3. Signature Algorithm		Sha256withRsaEncryption	Si
4. Issuer Distinguish Name		Entidad emisora del certificado	Si
	4.1. Country	C=ES	Si
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Si
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Si
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptor. serialNumber=Q2826004J	Si
	4.5. Common Name	cn=AC Administración Pública	Si
5. Validity		2 años	Si
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Si
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Si
	6.2. Organization	Denominación (nombre "oficial" de la organización) titular de los servicios de certificación	Si
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO	Si
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado.	Opcional
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público.	Opcional
	6.6. Serial Number	NIF/NIE del empleado público. Se utilizará la semántica propuesta por la norma ETSI EN 319 412-1	Si
	6.7. Surname	Apellidos de acuerdo con documento de identificación	Si



Campo		Contenido	Obligatoriedad
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte)	Si
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Si
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.	Si
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Si
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.	Si
10. Key Usage			Si
	10.1. Digital Signature	1	
	10.2. Content Commitment	1	
	10.3. Key Encipherment	1	
	10.4. Data Encipherment	0	
	10.5. Key Agreement	0	
	10.6. Key Certificate Signature	0	
	10.7. CRL Signature	0	
11. Extended Key Usage		Uso mejorado o extendido de las claves	Si
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Si
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si
	11.3. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Si
12. Qualified Certificate Statements			Si
	12.1. QcCompliance (0.4.0.1862.1.1)	Certificado cualificado.	Si
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Si
	12.3. QcType (0.4.0.1862.1.6)	QcT-esign (0.4.0.1862.1.6.1)	Si
	12.4. QcPDS (0.4.0.1862.1.5)	{ https://www.cert.fnmt.es/pds/PDS_AP_es.pdf , es},{ https://www.cert.fnmt.es/pds/PDS_AP_en.pdf , en}	Si





Campo		Contenido	Obligatoriedad
13. Certificate Policies		Política de certificación	Si
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.3.4.4.1	Si
	13.1.1 Policy Qualifier Id		
	13.1.1.1 CPS Pointer	http://www.cert.fmmt.es/dpcs/	Si
	13.1.1.2 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)”	Si
	13.2. Policy Identifier	QCP-n (OID:0.4.0.194112.1.0)	Si
	13.3. Policy Identifier	2.16.724.1.3.5.7.2	Si
14. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Si
	14.1. rfc822 Name	Correo electrónico del empleado público	Opcional
	14.2. UPN	UPN (nombre de login de red) para smartcard logon.	Opcional
	14.3. Directory Name	Identidad Administrativa	Si
	14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: OID: 2.16.724.1.3.5.7.2.1 = CERTIFICADO DE EMPLEADO PUBLICO (de nivel medio)	Si
	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>	Si
	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>	Si
	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>	Si
	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



Campo		Contenido	Obligatoriedad
	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>	Si
	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>	Si
	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>	Si
	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
	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
	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
15. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Si
	15.1. Distribution Point 1	Punto de publicación de la CRL1 <a href="http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl">http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Si
	15.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Si
16. Authority Info Access			Si
	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)	Si
	16.2. Acces Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Si

Campo		Contenido	Obligatoriedad
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Si
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Si
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". También sirve para distinguir una CA de las entidades finales	Si
	17.1. Subject Type	Entidad final (valor FALSE)	

3.4. CERTIFICADO DE PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN (SOFTWARE)

Campo		Contenido	Obligatoriedad
1. Version		2	Si
2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si
3. Signature Algorithm		Sha256withRsaEncryption	Si
4. Issuer Distinguish Name		Entidad emisora del certificado	Si
	4.1. Country	C=ES	Si
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Si
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Si
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Si
	4.5. Common Name	cn=AC Administración Pública	Si
5. Validity		2 años	Si
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Si

Campo		Contenido	Obligatoriedad
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Si
	6.2. Organization	Denominación (nombre "oficial" de la organización) titular de los servicios de certificación	Si
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO	Si
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado.	Opcional
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público.	Opcional
	6.6. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1	Si
	6.7. Surname	Apellidos de acuerdo con documento de identificación	Si
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte)	Si
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Si
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.	Si
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Si
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.	Si
10. Key Usage			Si
	10.1. Digital Signature	1	
	10.2. Content Commitment	1	
	10.3. Key Encipherment	1	
	10.4. Data Encipherment	0	
	10.5. Key Agreement	0	
	10.6. Key Certificate Signature	0	
	10.7. CRL Signature	0	
11. Extended Key Usage		Uso mejorado o extendido de las claves	Si
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Si
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si

Campo		Contenido	Obligatoriedad
	11.3. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Si
12. Qualified Certificate Statements			Si
	12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Si
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Si
	12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Si
	12.4. QcPDS (0.4.0.1862.1.5)	{ https://www.cert.fnmt.es/pds/PDS_AP_es.pdf , { https://www.cert.fnmt.es/pds/PDS_AP_en.pdf , en}	Si
13. Certificate Policies		Política de certificación	Si
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.3.4.4.2	Si
	13.1.1 Policy Qualifier Id		
	13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Si
	13.1.1.2 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)”	Si
	13.2. Policy Identifier	QCP-n (OID:0.4.0.194112.1.0)	Si
	13.3. Policy Identifier	2.16.724.1.3.5.7.2	Si
14. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Si
	14.1. rfc822 Name	Correo electrónico del empleado público	Opcional
	14.2. UPN	UPN (nombre de login de red) para smartcard logon.	Opcional
	14.3. Directory Name	Identidad Administrativa	Si
	14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.2.1 = CERTIFICADO DE EMPLEADO PUBLICO (de nivel medio)	Si
	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>	Si

Campo		Contenido	Obligatoriedad
	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>	Si
	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>	Si
	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
	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>	Si
	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>	Si
	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>	Si
	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
	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
	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
15. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Si
	15.1. Distribution Point 1	Punto de publicación de la CRL1 <a href="http://www.cert.fnmt.es/erlsacap/CRL<xxx*>.crl">http://www.cert.fnmt.es/erlsacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Si

Campo		Contenido	Obligatoriedad
	15.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList,binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Si
	16. Authority Info Access		Si
	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)	Si
	16.2. Acces Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Si
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Si
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Si
	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". También sirve para distinguir una CA de las entidades finales	Si
	17.1. Subject Type	Entidad final (valor FALSE)	

3.5. CERTIFICADO CON SEUDÓNIMO DE PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN DE JUSTICIA

Campo		Contenido	Obligatoriedad
1.	Version	2	Si
2.	Serial Number	Número identificativo único del certificado.	Si
3.	Signature Algorithm	Sha256withRsaEncryption	Si
4.	Issuer Distinguish Name	Entidad emisora del certificado (CA Subordinada)	Si
	4.1. Country	ES	Si
	4.2. Organization	FNMT-RCM	Si
	4.3. Organizational Unit	CERES	Si

Campo		Contenido	Obligatoriedad
	4.4. serialNumber	Q2826004J	Si
	4.5. CommonName	AC Administración Pública	Si
5.	Validity	2 años	Si
6.	Subject	Identificación del titular	Si
	6.1. Country	ES	Si
	6.2. Organization	Razón social de la <i>Entidad Representada</i>	Si
	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.	Si
	6.4. Organizational Unit	Unidad, dentro de la administración, en la que está incluida el suscriptor del certificado Ver apartado 2.3	No
	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	Si
	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	Si
	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	Si
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.	Si
8.	Subject Public Key Info	Clave pública del <i>Firmante</i> , codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Si
9.	Subject Key Identifier	Identificador de la clave pública del <i>Firmante</i> . Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Si
10.	Key Usage	Uso permitido de las claves certificadas.	Si
	10.1. Digital Signature	1	Si
	10.2. Content Commitment	1	Si
	10.3. Key Encipherment	1	Si
	10.4. Data Encipherment	0	Si
	10.5. Key Agreement	0	Si

Campo		Contenido	Obligatoriedad	
	10.6. Key Certificate Signature	0	Si	
	10.7. CRL Signature	0	Si	
11. Extended Key Usage		Uso mejorado o extendido de las claves	Si	
	11.1. Email Protection	1.3.6.1.5.5.7.3.4	No	
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si	
12. Qualified Certificate Statements		Extensiones cualificadas.		
	12.1. QcCompliance	Certificado es cualificado.	Si	
	12.2. QcType	Qct-esign	Si	
	12.3. QcPDS	{ https://www.cert.fnmt.es/pdsAP/PDS_es.pdf , { https://www.cert.fnmt.es/pdsAP/PDS_en.pdf , en}}	Si	
	12.4. QcEuRetentionPeriod	15 años	Si	
13. Certificate Policies		Política de certificación	Si	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.3.5.2	
	13.1.1. Policy Qualifier Id			
		13.1.1.1. CP S Pointer	http://www.cert.fnmt.es/dpcs/	Si
		13.1.1.2. 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)	Si
	13.2. Policy Identifier		0.4.0.194112.1.0	Si
	13.3. Policy Identifier		2.16.724.1.3.5.4.2	Si
14. Subject Alternative Names		Identificación/descripción del <i>Representante</i> y de la <i>Entidad representada</i>	Si	
	14.1. rfc822 Name		Correo electrónico del profesional del ámbito de la Justicia empleado público	
	14.2. Directory Name			
		14.2.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO	Si
		14.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Si
		14.2.3. NIF de la entidad suscriptora	Número único de identificación de la entidad. En caso del CGPJ: S2804008G y en el caso del MJU: S2813001A	Si

Campo		Contenido	Obligatoriedad
	14.2.4. Correo electrónico	Correo electrónico de contacto	No
	14.2.5. Unidad organizativa	Unidad, dentro de la administración, en la que está incluida el firmante del certificado Ver apartado 2.3	No
	14.2.6. Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptor del certificado. Ver apartado 2.2	Si
	14.2.7. User Principal name	UPN para Smart card logon	No
	14.2.8. Seudónimo	Seudónimo: JU:ES- $\{ID\}$ Ver apartado 2.1	Si
	14.2.9. Nombre	Nombre de pila del profesional del ámbito de la Justicia	Si
	14.2.10. Primer apellido	Primer apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Si
	14.2.11. Segundo apellido	Segundo apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Si
15. CRL Distribution Point			Si
	15.1. Distribution Point 1	Punto de publicación de la CRL2. ldap://ldapape.cert.fimt.es/CN=CRL<xxx*>,cn=AC%20Administracion%20Publica,ou=CERES,o=FNMTRCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Si
	15.2. Distribution Point 2	Punto de publicación de la CRL1 http://www.cert.fimt.es/crlsacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Si
16. Authority Info Access			Si
	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)	Si
	16.2. Acces Location 1	http://ocspap.cert.fimt.es/ocspap/OcspResponder	Si
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Si
	16.4. Acces Location 2	http://www.cert.fimt.es/certs/ACAP.crt	Si
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".	Si

Campo	Contenido	Obligatoriedad
17.1. cA	Valor FALSE (entidad final)	Si

3.6. CERTIFICADO DE EMPLEADO PÚBLICO CON SEUDÓNIMO

Campo	Contenido	Obligatoriedad
18. Version	2	Si
19. Serial Number	Número identificativo único del certificado.	Si
20. Signature Algorithm	Sha256withRsaEncryption	Si
21. Issuer Distinguished Name	Entidad emisora del certificado (CA Subordinada).	Si
21.1. Country	ES	Si
21.2. Organization	FNMT-RCM	Si
21.3. Organizational Unit	CERES	Si
21.4. serialNumber	Q2826004J	Si
21.5. CommonName	AC Administración Pública	Si
22. Validity	2 años	Si
23. Subject	Identificación del titular	Si
23.1. Country	ES	Si
23.2. Organization	Razón social de la <i>Entidad Representada</i> .	Si
23.3. 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.	Si
23.4. Organizational Unit	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado.	No
23.5. Pseudonym (Oid 2.5.4.65)	Seudónimo.	Si
23.6. Title	Profesión o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptor del certificado.	No
23.7. CommonName	Tendrá el formato: - Si se incluye el campo <i>Title</i> : \${title} – \${Pseudonym} – \${Organización} - Si no se incluye el campo <i>Title</i> : SEUDÓNIMO – \${Pseudonym} – \${Organización}	Si

Campo		Contenido	Obligatoriedad
24.	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.	Si
25.	Subject Public Key Info	Clave pública del <i>Firmante</i> , codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Si
26.	Subject Key Identifier	Identificador de la clave pública del <i>Firmante</i> . Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Si
27.	Key Usage	Uso permitido de las claves certificadas.	Si
	27.1. Digital Signature	1	Si
	27.2. Content Commitment	1	Si
	27.3. Key Encipherment	1	Si
	27.4. Data Encipherment	0	Si
	27.5. Key Agreement	0	Si
	27.6. Key Certificate Signature	0	Si
	27.7. CRL Signature	0	Si
28.	Extended Key Usage	Uso mejorado o extendido de las claves.	Si
	28.1. Email Protection	1.3.6.1.5.5.7.3.4	Si
	28.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si
29.	Qualified Certificate Statements	Extensiones cualificadas.	
	29.1. QcCompliance	Certificado es cualificado.	Si
	29.2. QcType	QcT-esign	Si
	29.3. QcPDS	{ https://www.cert.fnmt.es/pds/PDS_AP_es.pdf , es}, { https://www.cert.fnmt.es/pds/PDS_AP_en.pdf , en}	Si
	29.4. QcEuRetentionPeriod	15 años	Si
30.	Certificate Policies	Política de certificación.	Si
	30.1. Policy Identifier	1.3.6.1.4.1.5734.3.3.11.1	Si
	30.1.1. Policy Qualifier Id		
		30.1.1.1. CP S Pointer	http://www.cert.fnmt.es/dpcs/



Campo		Contenido	Obligatoriedad
	30.1.1.2. 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	Si
	30.2. Policy Identifier	0.4.0.194112.1.0	Si
	30.3. Policy Identifier	2.16.724.1.3.5.4.2	Si
31. Subject Alternative Names		Identificación/descripción del <i>Representante</i> y de la <i>Entidad representada</i> .	Si
	31.1. rfc822 Name	Correo electrónico del empleado público.	No
	31.2. Directory Name		
	31.2.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO	Si
	31.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Si
	31.2.3. NIF de la entidad suscriptora	Número único de identificación de la entidad.	Si
	31.2.4. Correo electrónico	Correo electrónico de contacto.	No
	31.2.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluido el firmante del certificado.	No
	31.2.6. 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.	No
	31.2.7. User Principal name	UPN para smart card logon.	No
	31.2.8. Seudónimo	Seudónimo.	Si
32. CRL Distribution Point			Si
	32.1. Distribution Point 1	Punto de publicación de la CRL. Idap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administracion%20Publica,ou=CERES,o=FNMTRCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Si
	32.2. Distribution Point 2	Punto de publicación de la CRL <a href="http://www.cert.fnmt.es/crlsacp/CRL<xxx*>.crl">http://www.cert.fnmt.es/crlsacp/CRL<xxx*>.crl	Si
33. Authority Info Access			Si
	33.1. Access Method 1	Identificador de método de acceso a la información de revocación. 1.3.6.1.5.5.7.48.1 (ocsp)	Si
	33.2. Access Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Si



Campo	Contenido	Obligatoriedad
33.3. 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
33.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Sí
34. 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
34.1. cA	Valor FALSE (entidad final).	Sí

3.7. PERFIL DE CERTIFICADO DE PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN DE FIRMA CENTRALIZADA

Campo	Contenido	Obligatoriedad	
1. Version	2	Sí	
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí	
3. Signature Algorithm	Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name	Entidad emisora del certificado	Sí	
4.1. Country	C=ES	Sí	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí
	4.5. Common Name	cn=AC Administración Pública	Sí
5. Validity	2 años	Sí	
6. Subject	Identificación/descripción del responsable de las claves certificadas	Sí	

Campo		Contenido	Obligatoriedad
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí
	6.2. Organization	Denominación (nombre "oficial" de la organización) titular de los servicios de certificación	Sí
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO	Sí
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el firmante	Opcional
	6.5. Organizational Unit	Número de identificación del firmante (supuestamente unívoco). Identificador del empleado público.	Opcional
	6.6. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1	Sí
	6.7. Surname	Apellidos de acuerdo con documento de identificación	Sí
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)	Sí
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Sí
6.10. Title	Puesto de trabajo o cargo	Opcional	
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
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
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
10. Key Usage			
	10.1. Digital Signature	0	
	10.2. Content Commitment	1	
	10.3. Key Encipherment	0	
	10.4. Data Encipherment	0	
	10.5. Key Agreement	0	
	10.6. Key Certificate Signature	0	
	10.7. CRL Signature	0	
11. Qualified Certificate Statements			

Campo		Contenido	Obligatoriedad
	11.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí
	11.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí
	11.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí
	11.4. QcPDS (0.4.0.1862.1.5)	{ https://www.cert.fnmt.es/pds/PDS_AP_es.pdf , { https://www.cert.fnmt.es/pds/PDS_AP_en.pdf , en}	Sí
	11.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	No
12. Certificate Policies		Política de certificación	Sí
	12.1. Policy Identifier	1.3.6.1.4.1.5734.3.3.10.1	Sí
	12.2. Policy Qualifier Id		
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
	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
	12.3. Policy Identifier	QCP-n (OID:0.4.0.194112.1.0)	Sí
	12.4. Policy Identifier	2.16.724.1.3.5.7.2	Sí
13. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Sí
	13.1. rfc822 Name	Correo electrónico del empleado público	Opcional
	13.2. Directory Name	Identidad Administrativa	Sí
	13.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO (de nivel medio)	Sí
	13.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.2=<Entidad Suscriptora>	Sí
	13.2.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.2.3 =<NIF>	Sí

Campo		Contenido	Obligatoriedad
	13.2.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.2.4 =<NIF>	Sí
	13.2.5 Número de identificación personal de	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleo público Id Campo/Valor: 2.16.724.1.3.5.7.2.5 =<NRP>	Opcional
	13.2.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.6 =<Nombre de pila>	Sí
	13.2.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.7 =<Apellido 1>	Sí
	13.2.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.8 =<Apellido 2>	Opcional
	13.2.9 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
	13.2.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.10 =<Unidad Organizativa>	Opcional
13.2.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.2.11 =<Puesto/Cargo>	Opcional	
14. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí
	14.1. Distribution Point 1	Punto de publicación de la CRL1 <a href="http://www.cert.fnmt.es/crlsacp/CRL<xxx*>.crl">http://www.cert.fnmt.es/crlsacp/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí
	14.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://ldap.cer.es/cn=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%F0blica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí
15. Authority Info Access			Sí



Campo		Contenido	Obligatoriedad
	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
	15.2. Acces Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Sí
	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
	15.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Sí
16. 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. También sirve para distinguir una CA de las entidades finales	Sí
	16.1. Subject Type	Entidad final (valor FALSE)	