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. 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) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí
	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. Acces 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	

2. PERFILES DE CERTIFICADO DE ENTIDADES FINALES

2.1. CERTIFICADO DE SEDE ELECTRÓNICA

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 (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	O=FNMT-RCM.	Sí
	4.3. Organizational Unit	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		6 meses	Sí
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí
	6.1. Country	C=ES	Sí
	6.2. stateOrProvinceName	Nombre del estado o Provincia	Sí
	6.2. LocalityName	Nombre de la localidad del suscriptor (organización)	Sí
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor	Sí

Campo		Contenido	Obligatoriedad
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: OU=SEDE ELECTRONICA	Sí
	6.5. Organizational Unit	El nombre descriptivo de la sede.	Sí
	6.6. SerialNumber	NIF del suscriptor	Sí
	6.7. BusinessCategory (OID 2.5.4.15)	businessCategory=Government Entity	Sí
	6.8. jurisdictionCountryName	jurisdictionCountryName=ES	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 de la sede, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
9. Subject Key Identifier		Identificador de la clave pública de la sede.	Sí
10. Key Usage		Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature	1	
	10.2. Content Commitment	0	
	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	Sí
	11.1. Server Authentication	1.3.6.1.5.5.7.3.1	Sí
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si
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. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Legal (0.4.0.194121.1.2)	No
	12.4. QcType(0.4.0.1862.1.6)	qct-web (0.4.0.1862.1.6.3)	
	12.5. 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}	

Campo				Contenido	Obligatoriedad
13. Certificate Policies				Política de certificación	Sí
	13.1. Policy Identifier			ev-guidelines (2.23.140.1.1)	Sí
	13.2. Policy Identifier			QCP-w (0.4.0.194112.1.4)	Sí
	13.3. Policy Identifier			evcp (0.4.0.2042.1.4)	Sí
	13.4. Policy Identifier			2.16.724.1.3.5.5.2	Sí
	13.5. Policy Identifier			1.3.6.1.4.1.5734.3.3.12.1	Sí
		13.5.1 Policy Qualifier Id			Sí
			13.5.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
			13.5.1.2 User Notice	"Certificado cualificado de sede electrónica, nivel medio/sustancial. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM, NIF:Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)"	Sí
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.	Sí
15. Subject Alternative Names				Identificación/ descripción de Identidad Administrativa	Sí
	15.1. DNS Name			Nombre de Dominio (DNS) de la Sede	Sí
16. CRL Distribution Point				Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	16.1. Distribution Point 1			Punto de publicación de la CRL. http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí
	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)	Sí
17. Authority Info Access					Sí
	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)	Sí
	17.2. Acces Location 1			http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Sí

Campo		Contenido	Obligatoriedad
	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)	Sí
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Sí
18. 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
	18.1. Subject Type	Entidad final (valor FALSE)	

2.2. 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		1 año	Sí
6. Subject		Identificación/descripción del custodio/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. 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
	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	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	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	

Campo				Contenido	Obligatoriedad
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/	Sí
		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-l (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

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

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

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

Campo		Contenido	Obligatoriedad
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		1 año	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. 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 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	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 (NIF/Pasaporte)	Sí
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Sí
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

Campo			Contenido	Obligatoriedad
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 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		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	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	Sí
	11.3. Microsoft Smart Card Logon		1.3.6.1.4.1.311.20.2.2	Sí
12. Qualified Certificate Statements				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)		Qct-esign (0.4.0.1862.1.6.1)	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		1.3.6.1.4.1.5734.3.3.4.4.1	Sí
	13.1.1 Policy Qualifier Id			

Campo				Contenido	Obligatoriedad
		13.1.1.1	CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		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)"	Sí
	13.2. Policy Identifier			QCP-n (OID:0.4.0.194112.1.0)	Sí
	13.3. Policy Identifier			2.16.724.1.3.5.7.2	Sí
14. Subject Alternative Names				Identificación/ descripción de Identidad Administrativa	Sí
	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	Sí
		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)	Sí
		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
		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
		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
		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>	Sí
		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

Campo			Contenido	Obligatoriedad
		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
		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	Sí
	15.1. Distribution Point 1		Punto de publicación de la CRL1 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
	16.2. Acces Location 1		http://ocspap.cert.fnmt.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.fnmt.es/certs/ACAP.crt	Sí
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

Campo		Contenido	Obligatoriedad
	17.1. Subject Type	Entidad final (valor FALSE)	

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

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		1 año	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. 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 suscriptor del certificado.	Opcional

Campo		Contenido	Obligatoriedad
	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	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 (NIF/Pasaporte)	Sí
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Sí
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 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	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	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	Sí
	11.3. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Sí
12. Qualified Certificate Statements			Sí
	12.1. QcCompliance(0.4.0.1862.1.1)	Certificado es cualificado.	Sí
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí
	12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí

Campo				Contenido	Obligatoriedad
	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			1.3.6.1.4.1.5734.3.3.4.4.2	Sí
	13.1.1 Policy Qualifier Id				
		13.1.1.1	CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		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)"	Sí
	13.2. Policy Identifier			QCP-n (OID:0.4.0.194112.1.0)	Sí
	13.3. Policy Identifier			2.16.724.1.3.5.7.2	Sí
14. Subject Alternative Names				Identificación/ descripción de Identidad Administrativa	Sí
	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	Sí
		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)	Sí
		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
		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
		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

Campo			Contenido	Obligatoriedad
		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>	Sí
		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
		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
		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	Sí
	15.1. Distribution Point 1		Punto de publicación de la CRL1 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
	16.2. Acces Location 1		http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Sí

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)	Sí
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Sí
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
	17.1. Subject Type	Entidad final (valor FALSE)	

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

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	ES	Sí
	4.2. Organization	FNMT-RCM	Sí
	4.3. Organizational Unit	CERES	Sí
	4.4. serialNumber	Q2826004J	Sí
	4.5. CommonName	AC Administración Pública	Sí
5. Validity		1 año	Sí
6. Subject		Identificación del titular	Sí
	6.1. Country	ES	Sí
	6.2. Organization	Razón social de la *Entidad Representada*	Sí
	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.	Sí

Campo		Contenido	Obligatoriedad
	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	Sí
	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	Sí
	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
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 *Firmante*, 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		Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature	1	Sí
	10.2. Content Commitment	1	Sí
	10.3. Key Encipherment	1	Sí
	10.4. Data Encipherment	0	Sí
	10.5. Key Agreement	0	Sí
	10.6. Key Certificate Signature	0	Sí
	10.7. CRL Signature	0	Sí
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	No
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí
12. Qualified Certificate Statements		Extensiones cualificadas.	

Campo			Contenido	Obligatoriedad
	12.1. QcCompliance		Certificado es cualificado.	Sí
	12.2. QcType		Qct-esign	Sí
	12.3. QcPDS		{https://www.cert.fnmt.es/pdsAP/PDS_es.pdf, es},{https://www.cert.fnmt.es/pdsAP/PDS_en.pdf, en}	Sí
	12.4. QcEuRetentionPeriod		15 años	Sí
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.3.5.2	Sí
	13.1.1. Policy Qualifier Id			
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		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)	Sí
	13.2. Policy Identifier		0.4.0.194112.1.0	Sí
	13.3. Policy Identifier		2.16.724.1.3.5.4.2	Sí
14. Subject Alternative Names			Identificación/descripción del *Representante* y de la *Entidad representada*	Sí
	14.1. rfc822 Name		Correo electrónico del profesional del ámbito de la Justicia empleado público	No
	14.2. User Principal name		UPN para Smart card logon	No
	14.3. Directory Name			
		14.3.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO	Sí
		14.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Sí
		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
		14.3.4. Correo electrónico	Correo electrónico de contacto	No
		14.3.5. Unidad organizativa	Unidad, dentro de la administración, en la que está incluida el firmante del certificado Ver apartado 2.3	No
		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

Campo			Contenido	Obligatoriedad
		14.3.7. Seudónimo	Seudónimo: JU:ES-${ID} Ver apartado 2.1	Sí
		14.3.8. Nombre	Nombre de pila del profesional del ámbito de la Justicia	Sí
		14.3.9. Primer apellido	Primer apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí
		14.3.10. Segundo apellido	Segundo apellido del profesional del ámbito de la Justicia de acuerdo con documento de identidad	Sí
15. CRL Distribution Point				Sí
	15.1. Distribution Point 1		Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.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)	Sí
	15.2. Distribution Point 2		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl *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
	16.2. Acces Location 1		http://ocspap.cert.fnmt.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.fnmt.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. cA		Valor FALSE (entidad final)	Sí

2.6. 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

Campo		Contenido	Obligatoriedad
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		1 año	Sí
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
	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

Campo			Contenido	Obligatoriedad
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				
	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. QcSSCD (0.4.0.1862.1.4)		Claves en dispositivo cualificado	
	11.4. QcType (0.4.0.1862.1.6)		Qct-esign (0.4.0.1862.1.6.1)	Sí
	11.5. 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
	11.6. 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

Campo			Contenido	Obligatoriedad
	12.3. Policy Identifier		QCP-n-qscd (OID:0.4.0.194112.1.2)	Sí
	12.4. Policy Identifier		2.16.724.1.3.5.7.1	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: 2.16.724.1.3.5.7.1.1 = CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO (de nivel alto)	Sí
		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
		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
		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
		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
		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
		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
		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

Campo			Contenido	Obligatoriedad
		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
		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
		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
14. CRL Distribution Point			Punto de distribución (localizador) de la CRL	Sí
	14.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacap/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://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
15. Authority Info Access				Sí
	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 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
	16.1. Subject Type		Entidad final (valor FALSE)	

2.7. CERTIFICADO DE EMPLEADO PÚBLICO CON SEUDÓNIMO

Campo		Contenido	Obligatoriedad
1. Version		2	Sí
2. Serial Number		Número identificativo único del certificado.	Sí
3. Signature Algorithm		Sha256withRsaEncryption	Sí
4. Issuer Distinguished Name		Entidad emisora del certificado (CA Subordinada).	Sí
	4.1. Country	ES	Sí
	4.2. Organization	FNMT-RCM	Sí
	4.3. Organizational Unit	CERES	Sí
	4.4. serialNumber	Q2826004J	Sí
	4.5. CommonName	AC Administración Pública	Sí
5. Validity		1 año	Sí
6. Subject		Identificación del titular	Sí
	6.1. Country	ES	Sí
	6.2. Organization	Razón social de la *Entidad Representada.*	Sí
	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.	Sí
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado.	No
	6.5. Pseudonym (Oid 2.5.4.65)	Seudónimo.	Sí
	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.	No
	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
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 *Firmante*, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí

Campo			Contenido	Obligatoriedad
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			Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature		1	Sí
	10.2. Content Commitment		1	Sí
	10.3. Key Encipherment		1	Sí
	10.4. Data Encipherment		0	Sí
	10.5. Key Agreement		0	Sí
	10.6. Key Certificate Signature		0	Sí
	10.7. CRL Signature		0	Sí
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	Sí
12. Qualified Certificate Statements			Extensiones cualificadas.	
	12.1. QcCompliance		Certificado es cualificado.	Sí
	12.2. QcType		Qct-esign	Sí
	12.3. QcPDS		{ https://www.cert.fnmt.es/pds/PDS_AP_es.pdf , es},{ https://www.cert.fnmt.es/pds/PDS_AP_en.pdf , en}	Sí
	12.4. QcEuRetentionPeriod		15 años	Sí
13. Certificate Policies			Política de certificación.	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.3.11.1	Sí
	13.1.1. Policy Qualifier Id			
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		13.1.1.2. 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	Sí

Campo			Contenido	Obligatoriedad
	13.2. Policy Identifier		0.4.0.194112.1.0	Sí
	13.3. Policy Identifier		2.16.724.1.3.5.4.2	Sí
14. Subject Alternative Names			Identificación/descripción del *Representante* y de la *Entidad representada.*	Sí
	14.1. rfc822 Name		Correo electrónico del empleado público.	No
	14.2. User Principal name		UPN para smart card logon.	No
	14.3. Directory Name			
		14.3.1. Tipo de certificado	Id Campo/Valor: 2.16.724.1.3.5.4.2.1=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO	Sí
		14.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado.	Sí
		14.3.3. NIF de la entidad suscriptora	Número único de identificación de la entidad.	Sí
		14.3.4. Correo electrónico	Correo electrónico de contacto.	No
		14.3.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluido el firmante del certificado.	No
		14.3.6. Puesto o cargo	Puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.	No
		14.3.7. Seudónimo	Seudónimo.	Sí
15. CRL Distribution Point				Sí
	15.1. Distribution Point 1		Punto de publicación de la CRL. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administracion%20Publica,ou=CERES,o=FNMTRCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí
	15.2. Distribution Point 2		Punto de publicación de la CRL http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl	Sí
16. Authority Info Access				Sí

Campo		Contenido	Obligatoriedad
	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
	16.2. Acces Location 1	http://ocspap.cert.fnmt.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.fnmt.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. cA	Valor FALSE (entidad final).	Sí