DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

DEFINICIÓN PERFILES DE CERTIFICADO EMITIDOS POR AC ADMINISTRACIÓN PÚBLICA

v1.10

Referencia:

Documento clasificado como: Público

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	Especificaciones
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado (Entidad de Certificación) ou= AC RAIZ FNMT-RCM	Sí	UTF8 String, tamaño máximo 128 (rfc5280)

5. Validity		12 años	Sí	
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí	
	6.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	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	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
7. Authority Key Identifier		Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC raíz.
8. Subject Public Key Info		Clave pública de la CA Subordinada para la Administración Pública, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública de la CA Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	0	Sí	Ver X509 y RFC 5280
	10.2. Content Commitment	0	Sí	Ver X509 y RFC 5280
	10.3. Key Encipherment	0	Sí	Ver X509 y RFC 5280
	10.4. Data Encipherment	0	Sí	Ver X509 y RFC 5280
	10.5. Key Agreement	0	Sí	Ver X509 y RFC 5280
	10.6. Key Certificate Signature	1	Sí	Ver X509 y RFC 5280

	10.7. CRL Signature		1	Sí	Ver X509 y RFC 5280
11. Certificate Policies			Política de certificación	Sí	
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí	Atendiendo a la rfc5280: "*PolicyInformation SHOULD only contain an OID.* *In a CA certificate,these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }*"
	11.2. Policy Qualifier Id				
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí	UTF8 String. Longitud máxima 200 caracteres.
12. CRL Distribution Point				Sí	
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí	Ruta donde reside la CRL (punto de distribución 1).
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí	Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Authority Info Access					
	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	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
	1.2. Acces Location 1		http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Sí	URL del servicio OCSP (no autenticado)
	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	Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"

	1.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Sí	Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado raíz de la FNMT-RCM.
14. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".		
	14.1. Subject Type	CA		Tipo de sujeto: Autoridad de Certificación.
	14.2. Path Length	0		Un pathLenConstraint de cero indica que ningún no pueden existir más certificados de CA intermedios en la ruta de certificación.

3. PERFILES DE CERTIFICADO DE ENTIDADES FINALES

3.1. CERTIFICADO DE SEDE ELECTRÓNICA

Campo		Contenido	Obligatoriedad	Especificaciones
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. +Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	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	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		3 años	Sí	Validez máxima limitada por "Esquema de Identificación y Firma. Perfiles de Certificados"
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí	
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

Campo		Contenido	Obligatoriedad	Especificaciones
	6.2. LocalityName	Nombre de la localidad del suscriptor (organización)	Sí	UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=sede electrónica	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.5. Organizational Unit	El nombre descriptivo de la sede.	Sí	Por ejemplo: ou=Oficina Virtual del MEH. UTF8 String, tamaño máximo 128 (rfc5280)
	6.6. Serial Number	Número único de identificación de la Entidad suscriptora de srvicios de certificación. En este caso el NIF	Sí	Por ejemplo: serialNumber=Q2826004J PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.7. Common Name	Denominación de nombre de dominio (DNS o IP) donde residirá el certificado y que identificara a la sede	Sí	Por ejemplo: cn=www.meh.es UTF8 String (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.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública de la sede, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	1		Ver X509 y RFC 5280
	10.2. Content Commitment	0		Ver X509 y RFC 5280
	10.3. Key Encipherment	1		Ver X509 y RFC 5280
	10.4. Data Encipherment	0		Ver X509 y RFC 5280
	10.5. Key Agreement	0		Ver X509 y RFC 5280
	10.6. Key Certificate Signature	0		Ver X509 y RFC 5280
	10.7. CRL Signature	0		Ver X509 y RFC 5280

Campo			Contenido	Obligatoriedad	Especificaciones
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	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.		ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance		Certificado es qualificado. (0.4.0.1862.1.1)	Sí	Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod		15 años (OID: 0.4.0.1862.1.3)	Sí	Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro 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. QcSSCD		Claves generadas en un DSCF (OID: 0.4.0.1862.1.4)	No	Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo seguro de creación de firma de acuerdo al Anexo III de la Directiva del Parlamento Europeo 1999/93/EC, sobre un framework comunitario para firmas electrónicas. Este valor sólo se consignará cuando se pueda asegurar que las clave privada ha sido generada en un DSCF de forma fehaciente (mecanismo técnico o proceso auditado)
13. Certificate Policies			Política de certificación	Sí	
	13.1. Policy Identifier		Identificador unívoco de la política de certificación asociada a los certificados de tipo “Sede electrónica”. En este caso: 1.3.6.1.4.1.5734.3.3.2.2	Sí	Identificador de la política de certificado para Sede-Nivel medio
	13.2. Policy Qualifier Id			Sí	
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado reconocido de sede electrónica. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí	UTF8 String. Longitud máxima 200 caracteres.

Campo		Contenido	Obligatoriedad	Especificaciones
14. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Sí	
	14.1.			
	14.2. DNS Name	Nombre de Dominio (DNS) de la Sede	Sí	UTF8 String, tamaño máximo 128. Nombre Dominio donde se eneuntra la Sede. Por ejemplo: DNSName = www.sede.meh.gob.es
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	Ruta donde reside la CRL (punto de distribución 1).
	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	Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
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	Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Sí	Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
17. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".		De la rf5280: " *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Entidad final (valor FALSE)		Con este certificado no se pueden emitir otros

3.2. CERTIFICADO DE SELLO ELECTRÓNICO

Campo		Contenido	Obligatoriedad	Especificaciones
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	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	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		3 años	Sí	Validez máxima limitada por "Esquema de Identificación y Firma. Perfiles de Certificados"
6. Subject		Identificación/descripción del c ustodio/responsable de las claves certificadas	Sí	
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Locality	Nombre de la localidad del suscriptor (organización)	Sí	UTF8String (rfc5280). Por ejemplo: L=Madrid

Campo		Contenido	Obligatoriedad	Especificaciones
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)	Sí	UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=sello electrónico	Sí	UTF8 String, tamaño máximo 128 (rfc5280)
	6.5. Serial Number	Número único de identificación de la Entidad suscriptora de servicios de certificación. En este caso el NIF	Sí	Por ejemplo: serialNumber=Q2826004J PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.6. 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	UTF8String (rfc5280). Por ejemplo: cn=SERVICIO DE REGISTRO DEL MEH
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	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.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage				Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	1		Ver X509 y RFC 5280
	10.2. Content Commitment	1		Ver X509 y RFC 5280
	10.3. Key Encipherment	1		Ver X509 y RFC 5280
	10.4. Data Encipherment	1		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	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. Email protection	1.3.6.1.5.5.7.3.4	Sí	Proteción de correo electrónico

Campo			Contenido	Obligatoriedad	Especificaciones
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2		Autenticación de cliente
12. Qualified Certificate Statements			Extensiones cualificadas.		ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance		Certificado es qualificado (OID: 0.4.0.1862.1.1)	Sí	Indica que el certificado es qualificado. Solo si no está explicito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod		15 años (OID: 0.4.0.1862.1.3)	Sí	Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro 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. QcSSCD		Claves generadas en un DSCF (OID: 0.4.0.1862.1.4)	No	Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo seguro de creación de firma de acuerdo al Anexo III de la Directiva del Parlamento Europeo 1999/93/EC, sobre un framework comunitario para firmas electrónicas. Este valor sólo se consignará cuando se pueda asegurar que las clave privada ha sido generada en un DSCF de forma fehaciente (mecanismo técnico o proceso auditado)
13. Certificate Policies			Política de certificación	Sí	
	13.1. Policy Identifier		Identificador unívoco de la política de certificación asociada a los certificados de tipo "sello electrónico". En este caso: 1.3.6.1.4.1.5734.3.3.3.2	Sí	Identificador de la política de certificado para Sello-Nivel medio
	13.2. Policy Qualifier Id				
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí	IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	Certificado reconocido de sello electrónico de Admon., órgano o entidad de derecho público. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí	UTF8 String. Longitud máxima 200 caracteres.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	

Campo			Contenido	Obligatoriedad	Especificaciones
	14.1. rfc822 Name		Correo electrónico de contacto de la Sede (entidad suscriptora)	Opcional	Por ejemplo: rfc822Name=sellomeh@meh.es Se establecerá el valor del e-mail contacto entidad suscriptora si se aporta en la solicitud de certificado. En caso contrario no se rellenerá este valor
	14.2. Directory Name		Identidad Administrativa	Sí	Campos específicos definidos por la Administración para los certificados LAECSP.
		14.2.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.2.2.1 =sello electrónico	Sí	UTF8 String.
		14.2.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.2.2.2=<Entidad Suscriptora>	Sí	UTF8 String. Por ejemplo: 2.16.724.1.3.5.2.2.2=Ministerio de Economía y Hacienda
		14.2.3 NIF Entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.2.2.3 =<NIF>	Sí	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.2.2.3=Q2826004J
		14.2.4 Denominación de Sistema o componente	Breve descripción del componente asociado al certificado de sello. 2.16.724.1.3.5.2.2.5 =<Denominación del Sistema>	Sí	UTF8 String, tamaño máximo 128. Por ejemplo: 2.16.724.1.3.5.2.2.5= SERVICIO DE REGISTRO DEL MEH
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	Ruta donde reside la CRL (punto de distribución 1).
	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	Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	

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

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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	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		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí		UTF8 String (rfc5280)
5. Validity		3 años	Sí		Validez del certificado.
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí		
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	6.2. Organization	Denominación (nombre "oficial" de la organización) titular de los servicios de certificación	Sí		UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO	Sí		
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado.	Opcional		UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público.	Opcional		UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.6. Serial Number	NIF/NIE del empleado público. Se utilizará la semántica propuesta por la norma ETSI EN 319 412-1	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
	6.7. Surname	Apellidos de acuerdo con documento de identificación	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Sí		UTF8String (rfc5280). Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier		Identificador de la clave pública de la CA para la Administración Pública. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage			Sí	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	1			Ver X509 y RFC 5280
	10.2. Content Commitment	1			Ver X509 y RFC 5280
	10.3. Key Encipherment	1			Ver X509 y RFC 5280
	10.4. Data Encipherment	0			Ver X509 y RFC 5280 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
	10.5. Key Agreement	0			Ver X509 y RFC 5280
	10.6. Key Certificate Signature	0			Ver X509 y RFC 5280
	10.7. CRL Signature	0			Ver X509 y RFC 5280
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Sí		Proteción de correo electrónico
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente
	11.3. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Sí		*Necesaria para realizar logon en Windows con tarjeta/token*
12. Qualified Certificate Statements			Sí	No	
	12.1. QcCompliance (0.4.0.1862.1.1)	Certificado cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: “Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.”.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	12.3. QcType (0.4.0.1862.1.6)		Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.4. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_AP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_AP_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.3.4.4.1	Sí		Identificador de la política asociado a la DPC o PC
	13.1.1 Policy Qualifier Id					
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2 User Notice	"Certificado cualificado de firma electrónica de empleado público, nivel medio/sustancial. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.2. Policy Identifier		QCP-n (OID:0.4.0.194112.1.0)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)
	13.3. Policy Identifier		2.16.724.1.3.5.7.2	Sí		Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	No	
	14.1. rfc822 Name		Correo electrónico del empleado público	Opcional		Por ejemplo: rfc822Name=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.2. UPN		UPN (nombre de login de red) para smartcard logon.	Opcional		Campo destinado a incluir el smart card logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3. Directory Name		Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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		UTF8 String.
		14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
		14.3.3 NIF Entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.2.3=<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.3=Q2826004J
		14.3.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.2.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.4=99999999R
		14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.2.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.6=JUAN
		14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.7=ESPAÑOL
		14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.8 =<Apellido 2>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.8=ESPAÑOL

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.9=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.10=<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.2.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
15. CRL Distribution Point			Punto de distribución (localizador) de la CRL	Sí	No	
	15.1. Distribution Point 1		Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. ldap://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		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		Acceso al servicio OCSP
	16.2. Acces Location 1		http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP

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

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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	4.3. Organizational Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. ou=CERES	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	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		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn=AC Administración Pública	Sí		UTF8 String (rfc5280)
5. Validity		3 años	Sí		Validez del certificado.
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí		
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) titular de los servicios de certificación	Sí		UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO	Sí		
	6.4. Organizational Unit	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado.	Opcional		UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	6.5. Organizational Unit	Número de identificación del suscriptor del certificado (supuestamente unívoco). Identificador del empleado público.	Opcional		UTF8 String, tamaño máximo 128 (rfc5280). Por ejemplo: ou=ADM5689 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	6.6. Serial Number	NIF/NIE del empleado público. Se usará la semántica propuesta por la norma ETSI EN 319 412-1	Sí		Por ejemplo: SerialNumber= IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64
	6.7. Surname	Apellidos de acuerdo con documento de identificación	Sí		UTF8String (rfc5280). Por ejemplo: sn=ESPAÑOL ESPAÑOL
	6.8. Given Name	Nombre de pila, de acuerdo con documento de identidad (NIF/Pasaporte)	Sí		UTF8String (rfc5280). Por ejemplo: gn=JUAN
	6.9. Common Name	Nombre y apellidos de acuerdo con documento de identidad y número del NIF	Sí		UTF8String (rfc5280). Por ejemplo: cn=ESPAÑOL ESPAÑOL JUAN – DNI 99999999R
7. Authority Key Identifier		Identificador de la clave pública de la CA para la Administración Pública. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage			Sí	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	1			Ver X509 y RFC 5280
	10.2. Content Commitment	1			Ver X509 y RFC 5280
	10.3. Key Encipherment	1			Ver X509 y RFC 5280
	10.4. Data Encipherment	0			Ver X509 y RFC 5280 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
	10.5. Key Agreement	0			Ver X509 y RFC 5280
	10.6. Key Certificate Signature	0			Ver X509 y RFC 5280
	10.7. CRL Signature	0			Ver X509 y RFC 5280

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
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. Email protection		1.3.6.1.5.5.7.3.4	Sí		Protección de correo electrónico
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente
	11.3. Microsoft Smart Card Logon		1.3.6.1.4.1.311.20.2.2	Sí		*Necesaria para realizar logon en Windows*
12. Qualified Certificate Statements				Sí	No	
	12.1. QcCompliance(0.4.0.1862.1.1)		Certificado es cualificado.	Sí		Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".
	12.3. QcType (0.4.0.1862.1.6)		Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.4. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_AP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_AP_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.3.4.4.2	Sí		Identificador de la política asociado a la DPC o PC
	13.1.1 Policy Qualifier Id					
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2 User Notice	"Certificado cualificado de firma electrónica de empleado público, nivel medio/sustancial. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	13.2. Policy Identifier		QCP-n (OID:0.4.0.194112.1.0)	Sí		Certificado cualificado de firma, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)
	13.3. Policy Identifier		2.16.724.1.3.5.7.2	Sí		Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional.
14. Subject Alternative Names			Identificación/ descripción de Identidad Administrativa	Sí	No	
	14.1. rfc822 Name		Correo electrónico del empleado público	Opcional		Por ejemplo: rfc822Name=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.2. UPN		UPN (nombre de login de red) para smartcard logon.	Opcional		Campo destinado a incluir el smart card logon de Windows para el responsable del certificado. Se establecerá el valor del UPN si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
	14.3. Directory Name		Identidad Administrativa	Sí		Campos específicos definidos por la Administración para los certificados LAECSP.
		14.3.1 Tipo certificado	Naturaleza del certificado / tipo de certificado. ID Campo/Valor: 2.16.724.1.3.5.7.2.1 = CERTIFICADO DE EMPLEADO PUBLICO (de nivel medio)	Sí		UTF8 String.
		14.3.2 Entidad suscriptora	Nombre de la entidad propietaria del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.2=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
		14.3.3 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 2.16.724.1.3.5.7.2.3 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.3=Q2826004J

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		14.3.4 NIF del empleado	Identificador de identidad del suscriptor-custodio de las claves. (NIF). Id Campo/Valor: 2.16.724.1.3.5.7.2.4 =<NIF>	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.4=99999999R
		14.3.5 Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Número de identificación de funcionario/empleado público Id Campo/Valor: 2.16.724.1.3.5.7.2.5 =<NRP>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.5=ADM12347 Se establecerá el valor del identificador de funcionario/empleado público si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.6 Nombre	Nombre de pila del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.6 =<Nombre de pila>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.6=JUAN
		14.3.7 Apellido 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.7 =<Apellido 1>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.7=ESPAÑOL
		14.3.8 Apellido 2	Segundo apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.7.2.8 =<Apellido 2>	Sí		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.8=ESPAÑOL
		14.3.9 Correo electrónico	Correo electrónico de la persona responsable del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.9 =<email de contacto>	Opcional		UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.9=jespanol@meh.es Se establecerá el valor del e-email contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.10 Unidad organizativa	Unidad, dentro de la Administración, en la que desempeña su labor el suscriptor del certificado. Id Campo/Valor: 2.16.724.1.3.5.7.2.10 =<Unidad Organizativa>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Se establecerá el valor de la unidad organizativa si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.
		14.3.11 Puesto / cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración. Id Campo/Valor: 2.16.724.1.3.5.7.2.11 =<Puesto/Cargo>	Opcional		UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.11=ANALISTA DE INFORMATICA Se establecerá el valor del puesto de trabajo o cargo si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
15. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	No	
	15.1. Distribution Point 1	Punto de publicación de la CRL1 http://www.cert.fnmt.es/crlsacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://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		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
16. Authority Info Access			Sí	No	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		Acceso al servicio OCSP
	16.2. Acces Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Emisor de la entidad emisora de certificados (CA Raíz) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
17. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación". También sirve para distinguir una CA de las entidades finales	Sí	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*

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