



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

PERFILES DE CERTIFICADO EMITIDOS POR AC ADMINISTRACIÓN PÚBLICA

	NOMBRE	FECHA
Elaborado por:	Soporte Técnico	15/11/2016
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	Descripción	Autor
1.0	15/11/2016	Creación del documento	Soporte Técnico

Referencia:

Documento clasificado como: *Difusión limitada*

1. Introducción.....	3
2. Certificado de personal al servicio de la administración (Tarjeta).....	4
6. Subject	10
10. Key Usage	11
12. Qualified Certificate Statements.....	11
13. Certificate Policies	11
3. Certificado de personal al servicio de la administración (Software).....	12
6. Subject	19
10. Key Usage	19
12. Qualified Certificate Statements.....	19
13. Certificate Policies	19

1. INTRODUCCIÓN

En el presente documento se describen en detalle los perfiles de los certificados de empleado público emitidos por la Autoridad de Certificación “AC Administración Pública” gestionada por la FNMT-RCM.

Los tipos de certificado que emite esta CA para empleado público son:

- 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).

Además, se detallan las diferencias que han sufrido estos certificados para adaptarse a la nueva normativa eIDAS.

2. 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=JUAN ESPAÑOL ESPAÑOL – 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 empleo 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		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 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 , { 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/dp cs/	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. 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.
	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 electrónico de empleado público	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-mail 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 INFORMÁTICA 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 <a href="http://www.cert.fnmt.es/crl/sacap/CRL<xxx*>.crl">http://www.cert.fnmt.es/crl/sacap/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://ldap.e-cert.fnmt.es/CN=CRL<xxx*>.cn=AC%20Administraci%F3n%20P%FAbrica,ou=CERES,o=F NMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		Acceso al servicio OCSP
	16.2. Access Location 1		http://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	Si	De la rfc5280: "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

6. Subject

Pasa de ser:

C=ES
O="Nombre oficial de la organización"
OU=empleado público
OU="Unidad de la Administración"
OU="Número de Identificación del suscriptor"
serialNumber ="DNI/NIE del empleado Público"
SN="APELLIDOS"
GN="NOMBRE"
CN="Nombre, apellidos y dnie/nie"

A ser:

CN = JUAN ESPAÑOL ESPAÑOL – DNI 00000000T
G = JUAN
SN = ESPAÑOL ESPAÑOL
SERIALNUMBER = IDCES-00000000T (No confundir con el número de serie del certificado)
OU = 1234567890
OU = Unidad Pruebas eIDAS
OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
O = ENTIDAD PRUEBAS DE LA ADMINISTRACIÓN PÚBLICA ESPAÑOLA
C = ES

10. Key Usage

Se elimina el uso de clave Data Encipherment, 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.

12. Qualified Certificate Statements

Se añaden dos nuevos campos:

- QcType (0.4.0.1862.1.6), indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
- QcPDS (0.4.0.1862.1.5), enlace a la PKI Disclosure Statement, así como el idioma del documento.

13. Certificate Policies

Se añaden dos nuevos identificadores de políticas:

- QCP-n (OID:0.4.0.194112.1.0), Certificado cualificado de firma, acorde al Reglamento UE 910/2014
- 2.16.724.1.3.5.7.2, Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional

3. 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 certificado 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		



Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de 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 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=JUAN ESPAÑOL ESPAÑOL – 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.



Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
8. Subject Public Key Info		Clave pública asociada al empleado público, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage			Sí	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	1			Ver X509 y RFC 5280
	10.2. Content Commitment	1			Ver X509 y RFC 5280
	10.3. Key Encipherment	1			Ver X509 y RFC 5280
	10.4. Data Encipherment	0			Ver X509 y RFC 5280 No se permite el uso de cifrado en los certificados de empleado de nivel medio/sustancial, para seguir las normas ETSI EN 319 412-2, ya que es un único perfil
	10.5. Key Agreement	0			Ver X509 y RFC 5280
	10.6. Key Certificate Signature	0			Ver X509 y RFC 5280
	10.7. CRL Signature	0			Ver X509 y RFC 5280
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
	11.1. 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.



Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y 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 , { 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/dp.cs/	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. 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.
	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-mail contacto si se aporta en la solicitud de certificado. En caso contrario este campo no estará presente en el certificado.





Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	14.2. 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 electrónico de empleado público	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





Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
		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-mail 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 <a href="http://www.cert.fnmt.es/crl/sacap/CRL<xxx*>.crl">http://www.cert.fnmt.es/crl/sacap/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta donde reside la CRL (punto de distribución 1).



Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	15.2. Distribution Point 2	Punto de publicación de la CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=F NMT-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 Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación". También sirve para distinguir una CA de las entidades finales	Sí	Sí	De la rfc5280: "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

6. Subject

Pasa de ser:

C=ES
O="Nombre oficial de la organización"
OU=empleado público
OU="Unidad de la Administración"
OU="Número de Identificación del suscriptor"
serialNumber="DNI/NIE del empleado Público"
SN="APELLIDOS"
GN="NOMBRE"
CN="Nombre, apellidos y dnie/nie"

A ser:

CN = JUAN ESPAÑOL ESPAÑOL – DNI 00000000T
G = JUAN
SN = ESPAÑOL ESPAÑOL
SERIALNUMBER = IDCES-00000000T (No confundir con el número de serie del certificado)
OU = 1234567890
OU = Unidad Pruebas eIDAS
OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
O = ENTIDAD PRUEBAS DE LA ADMINISTRACIÓN PÚBLICA ESPAÑOLA
C = ES

10. Key Usage

Se elimina el uso de clave Data Encipherment, 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.

12. Qualified Certificate Statements

Se añaden dos nuevos campos:

- QcType (0.4.0.1862.1.6), indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
- QcPDS (0.4.0.1862.1.5), enlace a la PKI Disclosure Statement, así como el idioma del documento.

13. Certificate Policies

Se añaden dos nuevos identificadores de políticas:

- QCP-n (OID:0.4.0.194112.1.0), Certificado cualificado de firma, acorde al Reglamento UE 910/2014
- 2.16.724.1.3.5.7.2, Identificador de la política asociado al certificado de empleado público de nivel medio según normativa nacional