PERFIL TÉCNICO

Certificado de Empleado Público

(AUTENTICACION) (FIRMA) (CIFRADO)

TOKEN POR SOFTWARE - TOKEN HSM

Campo	OID	valor		Norma	APP	Aclaración	Crít	Oblig
Versión		2 = (V3)		RFC 5280	Emisor	Integer:=2 ([RFC5280] describe la versión del certificado al usar extensiones es decir v3 su valor debe ser 2)		SI
Número de serie				RFC 5280	Emisor	Establecido automáticamente por ANF AC. [RFC5280] integer positivo, no mayor 20 octetos (1- 2^{159}) Se utiliza para identificar de manera unívoca el certificado		SI
Algoritmo de firma. *SignatureAlgorithm*	1.2.840.113549.1.1.11	sha256WithRSAEncryption		RFC 5280	Emisor	Identificador del Algoritmo de firma String UTF8 (40). Identificando el tipo de algoritmo.		SI
Algoritmo Hash de firma - *SignatureHashAlgorithm*	2.16.840.1.101.3.4.2.1	sha256			Emisor	Identificador del Algoritmo hash de firma		SI
Emisor	2.5.4.3	Common Name (CN)	*p.e. ANF High Assurance AP CA1*		AR Manager	Nombre común de la CA emisora del certificado		SI
	2.5.4.5	SERIALNUMBER	G63287510		AR Manager	CIF de ANF AC		SI
	2.5.4.97	Organisation Identifier	*Se trata del VAT number, en España denominado NIF-IVA no es el CIF. Es el NIF para el IVA en la UE* *En la actualidad ANF AC no lo incluye*	eIDAS	Emisor	Identificación de la organización emisora. Como se especifica en cláusula 5.1.4 de ETSI EN 319 412-1 [7].		
		EmailAddress (E)	info@anf.es		Emisor	Email CA		
	2.5.4.11	Organisational Unit (OU)	Unidad organizativa dentro del Prestador de Servicios de Certificación responsable de la emisión del certificado		AR Manager	Tal y como aparece en el certificado del emisor. (String UTF8) Size [RFC 5280] 128		SI
	2.5.4.10	Organisation (O)	*p.e. ANF Autoridad de Certificacion*		Emisor	Nombre oficial del Prestador de Servicios de Certificación		SI
		Locality (L)	*p.e. Barcelona (ver dirección actual en http://www.anf.es/es/address-direccion.html)*		Emisor	Localidad/dirección del Prestador de Servicios de Certificación (String UTF8) Size [RFC 5280] 128		
		State (ST)	*p.e. Barcelona*		Emisor	Provincia del Prestador de Servicios de Certificación		
	2.5.4.6	Country (C)	*p.e. ES*	(2 character ISO 3166 country code [5])	AR Manager	País del Prestador de Servicios de Certificación (PrintableString) Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements" Size 2 [RFC 5280]		SI
AuthorityCertIssuer				(String UTF8) Size 128	Emisor	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier		
AuthorityCertSerialNumber				(Integer)	Emisor	Número de serie del certificado de CA		

Identificador de la clave de la entidad emisora - *Authority KeyIdentifier*	2.5.29.35	Hash con SHA1 de la clave pública utilizada para firmar el certificado		RFC 5280 (String UTF8)	Emisor	Identificador derivado de utilizar la función de hash sobre la clave pública del sujeto. Es un medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado		SI
Issuer Alternative Name	2.5.29.18							
Válido desde *NotBefore*					Emisor	Fecha inicio validez		SI
Válido hasta *NotAfter*					Emisor	Fecha fin de validez		SI
Sujeto *(todos los campos codificados utilizando UTF-8)* Ver NOTA 2	2.5.4.6	Country (C)	*p.e.= ES*	*Código de país dos dígitos ISO 3166-1*	AR manager	Según ETSI-QC este campo se debe cumplimentar obligatoriamente Ver RFC 3739 / ETSI 101862		SI
	2.5.4.7	Locality (L)	*Ciudad del sujeto*	*(String UTF8) Size [RFC 5280] 128*	AR manager			SI
	2.5.4.8	State (ST)	*Provincia del sujeto*		AR manager			SI
	1.2.840.113549.1.9.1	EmailAddress (E)	*Email del sujeto*		AR manager			
	2.5.4.5	SERIAL NUMBER (SN)	*Por ejemplo* *p. ej.: 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*	AR manager	NIF del sujeto Preferiblemente se utilizará la semántica propuesta por la norma ETSI EN 319 412-1		SI
	2.5.4.97	OrganizationIdentifier	*El certificado debe de incluir al menos = Serial Number o OrganizationIdentifier (NIF-IVA), p.e. VATES-B0085974Z*	*Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)*	AR manager	VAT number. NIF, tal como figura en los registros oficiales. Codificado Según la Norma Europea EN 319 412-1 No confundir con el DNI, se trata del NIF de IVA para la UE		
	2.5.4.42	Given Name (G)	*p. ej.: "JUAN ANTONIO"*	*(String UTF8) Size 40. Obligatorio según ETSI EN 319 412-2*	AR manager	Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte.		SI
	2.5.4.4	SurName (SN)	*p. ej.: "DE LA CAMARA ESPAÑOL - DNI 00000000G*	*(String UTF8) Size 80* Obligatorio según ETSI EN 319 412-2.	AR manager	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público).		SI
	2.5.4.3	Common Name (CN)	*ej.: JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G*	*(String UTF8)) Size [RFC 5280] 132*	AR manager	Se deben introducir el nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI (Ver NOTA 1)		SI
	2.5.4.11	Organisational Unit (OU)	Certificado de Empleado Publico Nivel Alto **(AUTENTICACION)** Certificado de Empleado Publico Nivel Alto **(FIRMA)** Certificado de Empleado Publico Nivel Alto **(CIFRADO)** Certificado de Empleado Publico Nivel Medio	*(String UTF8) Size [RFC 5280] 128*	AR Manager el concepto. ANF CT los sufijos FIRMA AUTENTICACIÓN, y CIFRADO	Descripción del tipo de certificado Es de nivel ALTO si se emplea dispositivo HSM		SI

			p. ej.: SUBDIRECCION GENERAL DE PROCESO DE DATOS	*(String) Size [RFC 5280] 128*	AR manager	*Unidad, dentro de la Administración, en la que está incluida el empleado público responsable del certificado*		
			OU = p. ej.: E04976701		AR manager	Código DIR3 de la unidad		
			Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. Ver NOTA 3	*(String UTF8) Size = 10*	AR manager	Número de identificación del empleado público responsable del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP Ver NOTA 3		
	2.5.4.10	Organization (O)	*p. ej.: MINISTERIO DE FOMENTO.*	*(String UTF8) Size [RFC 5280] 128*	AR manager	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.		
	2.5.4.12	Titulo (T)	*p. ej.: ANALISTA PROGRAMADOR. Nombre descriptivo del puesto o cargo que ostenta el responsable del certificado*	*(String UTF8) Size [RFC 5280] 128*	AR manager	Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado		
Nombre alternativo del sujeto – *SubjectAlternativeName* Ver NOTA 2	Nombre alternativo del sujeto – *SubjectAlternativeName* - 2.5.29.17							
	eMail ejemplo: pedro@cial.com			*Nombre RFC822 (String) Size [RFC 5280] 255*	ANF CT	Correo electrónico de la persona responsable del certificado		SI
	DNSName *Directory Name*				AR manager	Campos específicos definidos por la Administración para los certificados RD 1671/2009. (Sequence)		
	Nivel ALTO	2.16.724.1.3.5.7.1.1	*Certificado de Empleado Público Nivel Alto (AUTENTICACIÓN)* *Certificado de Empleado Público Nivel Alto (FIRMA)* *Certificado de Empleado Público Nivel Alto (CIFRADO)*	(String UTF8) Size = 80	ANF CT	Indica la naturaleza del certificado Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.1	*Certificado de Empleado Público Nivel Medio*					
	Nivel ALTO	2.16.724.1.3.5.7.1.2	*p. ej.: MINISTERIO DE FOMENTO*	*(String UTF8) Size = 80*	ANF CT	La entidad propietaria de dicho certificado Nombre de la entidad suscriptora Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.2						
	Nivel ALTO	2.16.724.1.3.5.7.1.3	*p. ej.: S2833002*	*(String UTF8) Size = 9*	ANF CT	NIF entidad suscriptora Número único de identificación de la entidad. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.3						
	Nivel ALTO	2.16.724.1.3.5.7.1.4	*p. ej.: 00000000G*	*(String UTF8) Size = 10*	ANF CT	DNI/NIE del firmante. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.4						
	Nivel ALTO	2.16.724.1.3.5.7.1.5	*p. ej.: A02APE1056*	*(String UTF8) Size = 10*	ANF CT	Número de identificación de personal Se corresponde con el NRP o NIP. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.5						
	Nivel ALTO	2.16.724.1.3.5.7.1.6	*Ej.: "JUAN ANTONIO"*	*(String UTF8) Size 40*	ANF CT	Nombre de pila del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.6						
	Nivel ALTO	2.16.724.1.3.5.7.1.7	*Ej.: "DE LA CAMARA"*	*String UTF8) Size 40*	ANF CT	Primer apellido del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte.		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.7						

						Es nivel ALTO si el dispositivo es un		
	Nivel ALTO	2.16.724.1.3.5.7.1.8	*Ej.: "ESPAÑOL"*	*String UTF8) Size 40*	ANF CT	Segundo apellido del firmante de acuerdo con el DNI o en caso de extranjero en el pasaporte. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.8						
	Nivel ALTO	2.16.724.1.3.5.7.1.9	*P. ej.: juanantonio.delacamara.espanol@mfom.es*	*(String) Size [RFC 5280] 255*	ANF CT	Correo electrónico del firmante. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.9						
	Nivel ALTO	2.16.724.1.3.5.7.1.10	*p. ej.: SUBDIRECCION GENERAL DE PROCESO DE DATOS*	*(String) Size [RFC 5280] 128*	ANF CT	Unidad, dentro de la Administración, en la que está incluido el firmante. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.10						
	Nivel ALTO	2.16.724.1.3.5.7.1.11	*p. ej.: ANALISTA PROGRAMADOR (*	*(String) Size [RFC 5280] 128*	ANF CT	Puesto desempeñado por el firmante dentro de la administración. Es nivel ALTO si el dispositivo es un HSM		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.11						
SubjectDirectoryAttributes Ver NOTA 2	SubjectDirectoryAttributes - 2.5.29.9							
	2.5.4.13	*Description*			AR manager	Información de interés del suscriptor		
	2.5.4.20	*TelephoneNumber*			AR manager	Teléfono del suscriptor		
	2.5.4.23	*Facsimile*			AR manager	Fax del suscriptor		
	2.5.4.9	*StreetAddress*			AR manager	Dirección del suscriptor		
	2.5.4.16	*PostalAddress*			AR manager	Dirección postal del suscriptor		
	2.5.4.17	*PostalCode*			AR manager	Código postal del suscriptor		
	1.3.6.1.4.1.18332.10.10	*Ejemplo: SHA256-gsq33wq/udldyk5ZN84paMeYx*			AR manager	Es el hash del documento que acredita mandato o poder a favor del sujeto		
	1.3.6.1.4.1.18332.10.10.1	*Ejemplo: https://tomcat2.anf.es/cliente_archivo_ws/poderes/(localizador AR=OID1.3.6.1.4.1.18332.19)*			AR manager	Es el enlace que permite descargar el documento que acredita mandato o poder a favor del sujeto		
	2.5.4.2	*knowldgeinformation*			AR manager	Datos relativos al documento de representación		
	2.5.4.65	*Seudónimo –Pseudonym (elegido por el suscriptor)*			AR manager	Especifica que el certificado ha sido emitido con un seudónimo		
	1.3.6.1.4.1.18332.30.1	*Nombre completo del país al que corresponde la emisión*			AR manager	El certificado se somete a la legislación de ese país		
	1.3.6.1.4.1.18332.40.1	*p.e. Certificado reconocido*			AR manager	Calificación con la que ha sido emitido el certificado		
	1.3.6.1.4.1.18332.42.1				AR manager	Identificador de la Autoridad de Registro Reconocida a la que pertenece el operador AR		
	1.3.6.1.4.1.18332.42.11				AR manager	titular despacho AR		
	1.3.6.1.4.1.18332.42.13				AR manager	dpto. operador AR		
	1.3.6.1.4.1.18332.47.1	*Ejemplo= 8&1EB4F96F*			ANF CT	UUID del Dispositivo de Firma Electrónica que almacena el certificado		
	1.3.6.1.4.1.18332.47.3	*Modelo del token HSM*			AR manager	SOLO SI es un token HSM		
	1.3.6.1.4.1.18332.600	*Ejemplo: AR Manager desktop v.3.6*			AR manager	Programa AR Manager empleado para la tramitación y versión		

1.3.6.1.4.1.18332.19	*Ejemplo 33993893-503677*					AR manager	Localizador de la solicitud (secuencial de tramite – identificador Operador AR o RDE que la tramitó)		
1.3.6.1.4.1.18332.19.1	*Ejemplo 26144-56501328 3643648640*					AR manager	Identificador del operador AR que tramitó la solicitud (todos los certificados emitidos por este Operador AR comparten el mismo valor)		
Identificador de la clave del sujeto - Subject Key Identifier	2.5.29.14	Hash en SHA1 de la clave pública utilizada para firmar el certificado			*RFC 5280 Conforme con estándares RFC2459 & PKCS#1*	Emisor	Identificador derivado de utilizar la función de hash sobre la clave pública del sujeto.		SI
SubjectPublic KeyInfo		RSA (2048)			*(String UTF8) RSA en conformidad con la RFC 4055 [1 0] y ECC algoritmo en conformidad con la RFC 5639 [11]*	Emisor	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. Clave pública de la persona, codificada de acuerdo con el algoritmo criptográfico.		SI
Acceso a la información de entidad emisora	1.3.6.1.5.5.7.1.1	AccessMethod [1]	*[1]Acceso a información de autoridad* *Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)*			*Emisor*	Id-ad-ocsp con OID: (OCSP)		SI
		AccessLocation [1]	*Nombre alternativo: Dirección URL=http://*			*Emisor*	Dirección Respondedor OCSP		SI
		AccessMethod [2]	*1.3.6.1.5.5.7.48.2*			*Emisor*	id-ad-calssuers con OID		
		AccessLocation [2]	*Dirección URL=*			*Emisor*	localización del certificado de la CA		
Puntos de distribución CRL	2.5.29.31	cRLDistributionPoint [1]	*[1]Punto de distribución CRL* *Nombre del punto de distribución:* *Nombre completo:* *Dirección URL*			*Emisor*	Indica punto de descarga de la CRL.		SI
		DistributionPoint [2]				*Emisor*	Punto de distribución de la web donde reside la CRL (HTTP o LDAP) número 2		
		DistributionPoint [3]				*Emisor*	Punto de distribución de la web donde reside la CRL (HTTP o LDAP) número 3		
Declaraciones de certificados reconocidos *Qualified Certificate Statement* TSI EN 319 412-1, antes ETSI TS 101 862	1.3.6.1.5.5.7.1.3	0.4.0.1862.1.1	QcCompliance	**FIRMA de (NIVEL ALTO) y (NIVEL MEDIO)**	***Presente*** *si el certificado es expedido con la calificación de reconocido. Anexo I eIDAS*	ANF CT	**qcStatements** en conformidad con ETSI EN 319 412-5		SI
		0.4.0.1862.1.4	**QcSSCD**	**SOLO se incluye en el tipo Nivel ALTO (FIRMA)**	***SOLO si el dispositivo es SSCD*** Secure Signature Creation Device (SSCD)	ANF CT	**No se incluye en el de CIFRADO, ni el de AUTENTICACIÓN** *Determina que la clave privada asociada a la clave pública contenida en el certificado electrónico, está en un dispositivo seguro de creación de firma, Reglamento (UE) 910/2014 [I.8]*		SI
		0.4.0.1862.1.6.1	QcType- esign	**FIRMA de (NIVEL ALTO) y (NIVEL MEDIO)** *QcType 1*	*se reseña QcType 1 ETSI EN 319 412-5*	ANF CT	**id-etsi-qcsQcType** clausula 4.2.3 en ETSI EN 319 412-5 **No se incluye en el de CIFRADO ni AUTENTICACION; SI en el Nivel MEDIO** *Permite determinar a sistemas automáticos que es un certificado del tipo FIRMA. Sigue la codificación siguiente:* id-etsi-qct-esign		SI

							(id-etsi-qcs-QcType 1) id-etsi-qct-eseal (id-etsi-qcs-QcType 2) id-etsi-qct-web (id-etsi-qcs-QcType 3)		
		0.4.0.1862.1.5	QcPDS	**FIRMA - (NIVEL ALTO) (NIVEL MEDIO)**	*https://anf.es/en/* *URL que permite acceder a todas las políticas de la PKI en inglés. Protocolo https* *ETSI EN 319 412-5*	ANF CT	**No se incluye en el tipo CIFRADO**		SI
		0.4.0.1862.1.2	QcLimitValue	**FIRMA de (NIVEL ALTO) y (NIVEL MEDIO)**	*Importe límite de responsabilidad asumido por el emisor expresado en EUROS*	ANF CT	**No se incluye en el tipo CIFRADO**		SI
		0.4.0.1862.1.3	QcEuRetentionPeriod	**FIRMA de (NIVEL ALTO) y (NIVEL MEDIO)**	*Integer: =15* *([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este)*	ANF CT	<QcLimitValue> <money>EUR</money> <qcBase>1</qcBase> <qcExp>3</qcExp> </QcLimitValue> No se incluye en el tipo CIFRADO		SI
		0.4.0.194121.1.1	semnaticsId-Natural	**FIRMA de (NIVEL ALTO) y (NIVEL MEDIO)**	Para indicar semántica de persona física definida por la EN 319 412-1	ANF CT	**No se incluye en el tipo CIFRADO**		
Directivas del certificado – *Certificate Policies*	2.5.29.32	PolicyIdentifier	**Nivel ALTO**	**(AUTENTICACION)**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.1.22	AR Manager	OID propietario de ANF AC		SI
			Nivel ALTO	**(FIRMA)**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.3.22				
			Nivel ALTO	**(CIFRADO)**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.4.22				
			Nivel MEDIO		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.2.22	AR Manager	OID propietario de ANF AC.		SI
		PolicyIdentifier	Nivel ALTO	[2]Directiva de certificados: Identificador de directiva=2.16.724.1.3.5.7.1		AR Manager	Es nivel ALTO si el dispositivo es un HSM		SI
			Nivel MEDIO	[2]Directiva de certificados: Identificador de directiva=2.16.724.1.3.5.7.2					
		PolicyCPSLocation	[1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.anf.es/documentos			AR Manager			SI
		User notice	[1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado conforme a la legislación firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.			AR Manager	Máximo 200 caracteres. Se expresa una declaración realizada por la CA emisora, en la que se hace referencia a determinadas normas legales.		SI
		PolicyIdentifier	SOLO PARA TIPO **AUTENTICACION** Y SOLO PARA **DISPOSITIVO HSM**		0.4.0.2042.1.2	NCP+ (Normalized Certificate Policy requiring a secure user device)	ANF CT	Certificado acorde a una política normalizada, en dispositivo seguro acorde al Reglamento UE 910/2014 ETSI EN 319 411-3		
		PolicyIdentifier	**SOLO PARA TIPO FIRMA / AUTENTICACION**		TOKEN HSM	qcp-natural-qscd (0.4.0.194112.1.2)	ANF CT	Certificado cualificado de firma, acorde al Reglamento UE 910/2014 Conforme al Reglamento eIDAS		
					TOKEN SOFTWARE	qcp-natural (0.4.0.194112.1.0)	ANF CT			

Campos condicionados por el uso del certificado	2.5.4.15	BusinessCategory	PrivateOrganization	AR Manager	para organización privada		
			GovernmentEntity	AR Manager	para entidad pública		
			BusinessEntity	AR Manager	para empresa		
			Non-commercialEntity	AR Manager	para entidad no comercial		
	1.3.6.1.4.1.311.60.2.1.1	JurisdictionOfIncorporationLocalityName	Localidad	AR Manager	Localidad en la que está registrada la empresa		
	1.3.6.1.4.1.311.60.2.1.2	JurisdictionOfIncorporationStateOrProvinceName	Provincia	AR Manager	Provincia en la que está registrada la empresa		
	1.3.6.1.4.1.311.60.2.1.3	JurisdictionOfIncorporationCountryName	País	AR Manager	País en el que está registrada la empresa		
Restricciones básicas *Basic Constraints*	2.5.29.19	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno CA = FALSE		Emisor	Determina que se trata de un certificado de usuario final	**SI**	
Uso de la clave *Key usage*	2.5.29.15	*(NIVEL ALTO)* FIRMA	Sin repudio (c0)	AR Manager		**SI**	
		(NIVEL ALTO) AUTENTICACION	Firma digital				
			KeyEncipherment,				
			dataEncipherment				
		(NIVEL ALTO) CIFRADO	KeyEncipherment,	AR Manager			
			dataEncipherment				
		Nivel MEDIO	Digital Signature	AR Manager			
			Sin repudio (c0)				
			Key Encipherment				
			dataEncipherment				
Uso mejorado de las claves - *Extended key usage*	2.5.29.37	(Nivel ALTO) **Firma / Autenticación / Cifrado** (Nivel MEDIO)	1.3.6.1.5.5.7.3.2 Autenticación del cliente	AR Manager			SI
			1.3.6.1.5.5.7.3.4 Correo seguro				
Algoritmo de identificación		sha1		Emisor			SI
Signature Value				Emisor	Firma codificada como cadena de bits		SI
Huella digital				Emisor	Huella digital del certificado		SI

NOTA 1

Codificación del atributo Common Name

Criterios de composición del campo CN (CommonName) se compone bajo los siguientes criterios:

Incluir el NOMBRE, de acuerdo con lo indicado en el DNI/Pasaporte, y en mayúsculas.
Espacio en blanco
Incluir el PRIMER Y SEGUNDO APELLIDO, en mayúsculas, separados únicamente por un espacio en blanco, de acuerdo con lo indicado en el DNI/NIE. En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter).
Espacio en blanco
Guion que separe el nombre y apellidos del número de DNI/NIE, sin espacio entre los valores ni signos de puntuación
Espacio en blanco
Incluir el número de identificación fiscal, NIF, de acuerdo con lo indicado en su DNI o NIE. Al NIF, también se le llama DNI o NIE. Sin espacio entre el número y la letra de control; la letra de control en mayúsculas.

Ejemplo: GARCIA ABALOS JUAN ANTONIO - 00000000G
Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados se incluyen en atributos predefinidos en normas y especificaciones técnicas de reconocimiento general.

Si se trata de un certificado emitido con seudónimo se incluirá la mención (SEUDONIMO).

OPCIONALMENTE se puede incluir:

Etiqueta **NOMBRE**,
De usarse, va delante de apellidos y nombre del titular, separada por un espacio.

Etiqueta **NIF** o **DNI** o **NIE**
El término NIF abarca tanto a DNI como a NIE. Se colocará tras el guion, u otro símbolo o carácter de separación, y delante del número de identificación fiscal, separada, de ambos, por un espacio. Caso de optar por la etiqueta DNI o NIE, en lugar de NIF, se usará aquella que corresponda.

Literal **(AUTENTICACION, FIRMA o CIFRADO)**
Identifica la tipología del certificado. En el caso de que se agrupen varios perfiles en un único certificado, no se deberá incluir esta opción. Este identificador siempre estará al final del Common Name del Subject y entre paréntesis, separado, por un espacio en blanco, del número de identificación fiscal.

Ejemplos:

DE LA CAMARA ESPAÑOL JUAN ANTONIO - DNI 00000000G (AUTENTICACION)
DE LA CAMARA ESPAÑOL JUAN ANTONIO - DNI 00000000G
NOMBRE DE LA CAMARA ESPAÑOL JUAN ANTONIO - NIF 00000000G
DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G (AUTENTICACION)
DE LA CAMARA ESPAÑOL JUAN ANTONIO |00000000G
NOMBRE ESPAÑOL ESPAÑOL JUAN - NIF 99999999R
NOMBRE EXTRANJERO EXTRANJERO JUAN – NIF X1234567H
NOMBRE EXTRANJERO EXTRANJERO JUAN – NIE X1234567H

NOTA 2

ETSI EN **319 412-2 v2.1.1** (Part 2: *Certificate profile for certificates issued to natural persons*) define los requisitos del contenido de certificados emitidos a personas físicas.

El perfil se basa en las recomendaciones IETF RFC 5280 y el estándar ITU-T X.509.
La información utilizada para definir la identidad y atributos del firmante de un certificado de persona física, sin pseudónimos, se desglosa en los siguientes campos:

- *Campo "Subject", utilizando los atributos commonName, surname (o givenName) y countryName. En el atributo SerialNumber, se puede incluir el DNI del firmante.*
- *Extensión "Subject Alternative Names". No se incluye ninguna restricción.*
- *Extensión "Subject Directory attributes". No deben incluirse los atributos del campo Subject.*

NOTA 3

El Número de Identificación Personal (NIP) en el Registro Central de Personal está compuesto por ocho posiciones numéricas y una posición de control alfanumérica. El NIP es la clave que identifica a las personas en el Sistema de Información de Registro Central de Personal.

El NIP se construye dependiendo:

1. Del tipo de documento que aportó la persona en su primera relación con la Administración General del Estado (AGE).
2. De la fecha de incorporación en su primera relación con la AGE.

NIP		**Documento presentado en la primera Relación de Servicios con la AGE**		**Ejemplos**
Número (8 posiciones)	**Control (1 posición)**			
DNI sin letra	Blanco, 1, 2	DNI		00001234 00001234-1 00001234-2
Secuencial generado por el sistema	N	Desde 01/01/2003	Otro documento	0001234-N

Construido partiendo del documento presentado	3, 4, 5, 6, 7, 8, 9	Antes de 01/01/2003		0001234-3

OID's para certificados cualificados de persona física y representante legal

La codificación de ciertas características de los certificados cualificados se señala mediante OID (Object Identifier) específicos.

La norma técnica que los indicaba era la **ETSI TS 101 862**, que los reflejaba trayendo a colación el arco (hoy obsoleto):

- 1.3.6.1.5.5.7.0.11

Y definiendo la información de la declaración de certificado cualificado (QC-Statement) con el arco:

- 0.4.0.1862

En la actualidad, la norma de aplicación es la **ETSI EN 319 412-1** lo que ha dado lugar a que la información sobre certificados cualificados no incluidos en la norma anterior se refleja con un nuevo arco OID:

- 0.4.0.194121

Por tanto, los certificados cualificados podrán indicar ciertas características de los certificados con OIDs que comienzan con **0.4.0.1862** (*originalmente diseñados para firma electrónica de personas físicas según la Directiva 1999/93, pero hoy en día adecuados también para personas jurídicas por la ampliación de conceptos como el sello electrónico del Reglamento UE 910/2014 EIDAS*) y otras con OID que comienzan con **0.4.0.194121** (específicamente para diferenciar los certificados de persona física y jurídica tal como lo hace el Reglamento UE 910/2014 EIDAS).

Estos son los principales OID:

- 0.4.0.1862.1.1 – qcStatement – QcCompliance (**Obligatorio**)
- 0.4.0.1862.1.2 – qcStatement – QcLimitValue
- 0.4.0.1862.1.3 – qcStatement – QcRetentionPeriod
- 0.4.0.1862.1.4 – qcStatement – QcSSCD
- 0.4.0.1862.1.5 – qcStatement – QcPDS (**Obligatorio**)
- 0.4.0.1862.1.6 – qcStatement – QcType

-- QC type identifiers

id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 }

-- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014

id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }

-- Certificate for electronic seals as defined in Regulation (EU) No 910/2014

id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }

-- Certificate for website authentication as defined in Regulation (EU) No 910/2014

- 0.4.0.194121.1.1 -> id-etsi-qcs-semanticsId-Natural -> **Natural person semantics** (para certificados de persona física – firma electrónica)
- 0.4.0.194121.1.2 -> id-etsi-qcs-SemanticsId-Legal -> **Legal person semantics** (para certificados de persona jurídica – sello electrónico)

Los 4 últimos OID son nuevos:

- 0.4.0.1862.1.5 – qcStatement – QcPDS (**Obligatorio**).
  Proporcionará al menos una URL a un PDS (PKI Disclosure Statements) en inglés.
  Se pueden referenciar otros documentos PDS en otros idiomas con este QCStatement siempre que sean equivalentes al PDS en inglés.
  No se debe hacer referencia a más de un PDS por idioma.
- 0.4.0.1862.1.6 – qcStatement – QcType.
  id-etsi-qct-esign (0.4.0.1862.1.6.1) *QcType 1*
  id-etsi-qct-eseal (0.4.0.1862.1.6.2) *QcType 2*
  id-etsi-qct-web (0.4.0.1862.1.6.3) *QcType 3*