PERFIL TÉCNICO

Certificado de Sello Electrónico

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
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
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 Assured ID CA1*		AR Manager	Nombre común de la CA emisora del certificado		SI
	2.5.4.5	SERIALNUMBER	G63287510		AR Manager	NIF 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	2.5.29.18							

Name								
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)*	2.5.4.6	Country (C)	*País del sujeto=suscriptor*	*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 suscriptor 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		
	2.5.4.10	OrganizationName (O)	*p.e. Nombre empresa. S.L.*	*ETSI EN 319 412-1 [i.4], clause 5*	AR manager	Razón Social, tal como figura en los registros oficiales		SI
	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 (titular del órgano) 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 - 00000000G"*	*(String UTF8) Size 80. Obligatorio según ETSI EN 319 412-2*	AR manager	Primer apellido, espacio en blanco, segundo apellido del responsable del certificado, de acuerdo con documento de identidad (DNI/Pasaporte), guión y DNI o pasaporte		SI
	2.5.4.3	Common Name (CN)	*p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA*	*(String UTF8) Size 132 [RFC 5280]*	AR manager	Denominación de sistema o aplicación de proceso automático.		SI
	2.5.4.11	Organisational Unit (OU)	**Certificado de Sello Electronico**		String UTF8) Size [RFC 5280] 128	AR Manager El sufijo Nivel ALTO Nivel MEDIO lo incluye ANF CT	Descripción del tipo de certificado	SI
			Certificado de Sello Electronico AA.PP. Nivel Medio					
			Certificado de Sello Electronico AA.PP. Nivel Alto	*Solo en dispositivos HSM*				
	2.5.4.11	Organisational Unit (OU)	*p. ej: SUBDIRECCION DE EXPLOTACION*		String UTF8) Size [RFC 5280] 128	AR Manager	Denominación de la unidad dentro de la organización que presta el	

							servicio		
	2.5.4.11	Organisational Unit (OU)	SOLO en certificados AA.PP.	*p. ej: E04976701*	*String UTF8) Size [RFC 5280] 128*	AR Manager	Código DIR3 de la unidad		
	2.5.4.13	Description	*p.e.* *Reg: XXX /Hoja: XXX /Tomo: XXX /Sección: XXX /Libro: XXX /Folio: XXX /Fecha: dd-mm-aaaa /Inscripción: XXX* *Notario: Nombre Apellido1 Apellido2 /Núm. Protocolo: XXX* */Fecha Otorgamiento: dd-mm-aaaa* *En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX*			AR manager	Codificación del documento público que acredita las facultades del firmante o los datos registrales		SI
	2.5.4.12	Titulo (T)	*p.e. Administrador Único*			AR manager	Tipo de apoderamiento legal del representante legal.		
Nombre alternativo del sujeto – SubjectAlternativeName	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	Puede incluir URL web		
	Sello Electrónico	*1.3.6.1.4.1.18332.10.1*	*p.e. Pedro*			ANF CT	Nombre de pila del representante legal		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.2*	*p.e. López*			ANF CT	Primer apellido del representante legal		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.3*	*p.e. García*			ANF CT	Segundo apellido del representante legal		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.4*	*p.e. 8907234W*			ANF CT	NIF del representante legal		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.7*	*p.e. pedrolopez@anf.es*			ANF CT	Dirección correo electrónico representante legal		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.1*	*p.e. Juan Antonio*			ANF CT	Nombre del Responsable del Certificado		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.2*	*Ej: "DE LA CAMARA"*			ANF CT	Primer Apellido del Responsable del Certificado		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.3*	*Ej: "ESPAÑOL"*			ANF CT	Segundo Apellido del Responsable del Certificado		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.4*	*p.e. 896789234J*			ANF CT	NIF del Responsable del Certificado		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.5*	*p.e. juanesp@anf.es*			ANF CT	E-mail del Responsable del		SI

						Certificado		
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.1	Certificado de Sello Electrónico AA.PP. Nivel Alto	*String UTF8) Size = 31*	ANF CT	Indica tipo de certificado Es nivel ALTO si el dispositivo es un HSM		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.1	Certificado de Sello Electrónico AA.PP. Nivel Medio	*UTF8 String.*	ANF CT			SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.2	*p.e. Nombre empresa. S.L.*	*(String UTF8) Size = 80*	ANF CT	Nombre de la entidad suscriptora		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.2	*p.e. Nombre empresa. S.L.*	*(String UTF8) Size = 80*	ANF CT	Nombre de la entidad suscriptora		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.3	*p. ej: S2833002*	(String UTF8) Size = 9	ANF CT	NIF entidad suscriptora		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.3	*p. ej: S2833002*	(String UTF8) Size = 9	ANF CT	NIF entidad suscriptora		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.4	*p. ej: 00000000G*	*(String UTF8) Size = 9*	ANF CT	DNI o NIE del responsable del Sello		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.4	*p. ej: 00000000G*	*(String UTF8) Size = 9*	ANF CT	DNI o NIE del responsable del Sello		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.5	*p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA.*	*(String UTF8) Size = 128*	ANF CT	Breve descripción de la componente que posee el certificado de sello		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.5	*p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA.*	*(String UTF8) Size = 128*	ANF CT	Breve descripción de la componente que posee el certificado de sello		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.6	*Ej: "JUAN ANTONIO"*	*(String UTF8) Size 40*	ANF CT	Nombre de pila del responsable del certificado		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.6	*Ej: "JUAN ANTONIO"*	*(String UTF8) Size 40*	ANF CT	Nombre de pila del responsable del certificado		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.7	*Ej: "DE LA CAMARA"*	*String UTF8) Size 40*	ANF CT	Primer apellido del responsable del certificado		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.7	*Ej: "DE LA CAMARA"*	*String UTF8) Size 40*	ANF CT	Primer apellido del responsable del certificado		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.8	*Ej: "ESPAÑOL"*	*String UTF8) Size 40*	ANF CT	Segundo apellido del responsable del		SI

						certificado		
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.8	*Ej: "ESPAÑOL"*	*String UTF8) Size 40*	ANF CT	Segundo apellido del responsable del certificado		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.9	*p.e. juanesp@anf.es*	*(String) Size [RFC 5280] 255*	ANF CT	Correo electrónico		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.9	*p.e. juanesp@anf.es*	*(String) Size [RFC 5280] 255*	ANF CT	Correo electrónico		SI
SubjectDirectoryAttributes	SubjectDirectoryAttributes - 2.5.29.9							
	1.3.6.1.4.1.18332.10.10	*Ejemplo: SHA256-gsq33wq/udldyk5ZN84paMeYx*						
	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 representante			
	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 Operador AR que tramitó la solicitud. NOTA: en el caso de certificados de Operador AR, RDE o PKI, este OID corresponde al identificador del operador titular del certificado, reseñado en la parte primera del código)			
	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			
	1.3.6.1.4.1.18332.41.1	*1000*		AR manager	Límite de responsabilidad asumido por la CA			
	1.3.6.1.4.1.18332.41.2	*p.e. firma de contratos compra*		AR manager	Uso del certificado limitado al concepto expresado en este campo			
	1.3.6.1.4.1.18332.41.3	*p.e. 10.000*		AR manager	Limitación de uso del			

					certificado por importe		
	1.3.6.1.4.1.18332.41.4	*p.e. euros*		AR manager	Divisa en la que se expresan los valores 1.3.6.1.4.1.18332.41.1 1.3.6.1.4.1.18332.41.3		
	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		
	1.3.6.1.4.1.18332.90			AR manager	Aspectos profesionales o empresariales descriptivos de la actividad		
	1.3.6.1.4.1.18332.90.1			AR manager	aspectos profesionales de interés sufijo 01		
	1.3.6.1.4.1.18332.90.2			AR manager	aspectos profesionales de interés sufijo 02		
	1.3.6.1.4.1.18332.90.3			AR manager	aspectos profesionales de interés sufijo 03		
	1.3.6.1.4.1.18332.91.2			AR manager	Año de origen de la actividad		
	1.3.6.1.4.1.18332.92			AR manager	Marcas o denominaciones comerciales propias		
	1.3.6.1.4.1.18332.92.1			AR manager	Marcas que distribuye sufijo 1		
	1.3.6.1.4.1.18332.92.2			AR manager	Marcas que distribuye sufijo 2		
	1.3.6.1.4.1.18332.92.3			AR manager	Marcas que distribuye sufijo 3		
	1.3.6.1.4.1.18332.93			AR manager	Ámbito geográfico en el que desarrolla su actividad		
	1.3.6.1.4.1.18332.94			AR manager	Direcciones sitios sedes		
	1.3.6.1.4.1.18332.94.1			AR manager	Delegaciones sufijo 01		
	1.3.6.1.4.1.18332.94.2			AR manager	Delegaciones sufijo 02		
	1.3.6.1.4.1.18332.94.3			AR manager	Delegaciones sufijo 03		
	1.3.6.1.4.1.18332.95			AR manager	compañías con las que se relaciona		

	1.3.6.1.4.1.18332.95.1				AR manager	compañías con las que se relaciona sufijo 01		
	1.3.6.1.4.1.18332.95.2				AR manager	compañías con las que se relaciona sufijo 02		
	1.3.6.1.4.1.18332.95.3				AR manager	compañías con las que se relaciona sufijo 03		
	1.3.6.1.4.1.18332.96				AR manager	Entidades bancarias con las que mantiene relaciones		
	1.3.6.1.4.1.18332.96.1				AR manager	Cuentas corrientes, SWIFT		
	1.3.6.1.4.1.18332.97				AR manager	información económica		
	1.3.6.1.4.1.18332.97.1				AR manager	información económica sufijo 01		
	1.3.6.1.4.1.18332.97.2				AR manager	información económica sufijo 02		
	1.3.6.1.4.1.18332.97.3				AR manager	información económica sufijo 03		
	1.3.6.1.4.1.18332.98				AR manager	Número empleados		
	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		
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
SubjectPublicKeyInfo		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.		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]					Punto de distribución de la web donde reside la CRL (HTTP o LDAP) número 2		
			DistributionPoint [3]					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		***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 con dispositivo HSM**	***Presente si el dispositivo es SSCD*** Secure Signature Creation Device (SSCD)		ANF CT	*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
		0.4.0.1862.1.6.2	QcType-eseal	***QcType 2***	*se reseña QcType 2 ETSI EN 319 412-5*		ANF CT	**id-etsi-qcsQcType** clausula 4.2.3 en ETSI EN 319 412-5 *Sigue la codificación siguiente:* id-etsi-qct-esign (id-etsi-qcs-QcType 1) id-etsi-qct-eseal (id-etsi-qcs-QcType 2) id-etsi-qct-web (id-etsi-qcs-QcType 3)		SI
		0.4.0.1862.1.5	QcPDS	https://anf.es/en/	*Se proporciona la URL que permite acceder a todas las políticas de la PKI en inglés. Protocolo https ETSI EN 319 412-5*		ANF CT			SI
		0.4.0.1862.1.2	QcLimitValue		*Importe límite de responsabilidad asumido por el emisor expresado en EUROS*		ANF CT	<QcLimitValue> <money>EUR</money> <qcBase>1</qcBase> <qcExp>3</qcExp> </QcLimitValue>		SI
		0.4.0.1862.1.3	QcRetentionPeriod		*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			SI
		0.4.0.194121.1.2	semnaticsId-Legal		Para indicar semántica de persona jurídica definida por la EN 319 412-1		ANF CT			
Directivas del certificado – *Certificate Policies*	2.5.29.32	PolicyIdentifier		**Sello Electrónico**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.25.1.1.1		AR manager	OID propietario de ANF AC		SI
				Sello Electrónico AA.PP. Nivel Alto	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.25.1.1.2					
				Sello Electrónico AA.PP. Nivel Medio	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.25.1.1.3					
		PolicyIdentifier		**Sello Electrónico AA.PP. Nivel Alto**	2.16.724.1.3.5.6.1		AR manager			SI
				Sello Electrónico AA.PP. Nivel Medio	2.16.724.1.3.5.6.2					

		PolicyCPSLocation	[1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.anf.es/documentos		AR manager			
		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	**TOKEN HSM**	qcp-legal-qscd (0.4.0.194112.1.3)	ANF CT	Certificado cualificado de firma, acorde al Reglamento UE 910/2014 Conforme al Reglamento eIDAS		SI
			TOKEN SOFTWARE	qcp-legal (0.4.0.194112.1.1)	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	*Digital Signature*	Se utiliza cuando se realiza la función de autenticación de activo digital de la persona jurídica		AR manager		**SI**	
		Content Commitment	Se utiliza cuando se realiza la función de sello electrónico de documento expedido por persona jurídica					
		Key Encipherment	Se utiliza para gestión y transporte de claves					
		Data Encipherment	Se utiliza para el cifrado de datos.					
Uso mejorado de las claves - *Extended key usage*	2.5.29.37	Client Authentication	1.3.6.1.5.5.7.3.2		AR manager			SI
		Email Protection	1.3.6.1.5.5.7.3.4					
		Server Authentication	1.3.6.1.5.5.7.3.1					
		codeSigning	1.3.6.1.5.5.7.3.3					
Algoritmo de identificación		sha1			Emisor			SI
Signature Value					Emisor	Firma codificada como cadena de bits		SI
Huella digital					Emisor	Huella digital del certificado		SI

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.*

OID's para certificados cualificados

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 refleje 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)
- 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*