Política de Certificación de Certificados de Clase 2 de Persona Física

Perfil Técnico

Paseo de la Castellana, 79 – 28046 - Madrid (Spain)
Telephone: 902 902 172 (Calls from Spain)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es/en

Nivel de Seguridad

Publico

AVISO IMPORTANTE

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (Spain)

Teléfono: 902 902 172 (Llamadas desde España) Internacional (+34) 933 935 946

Fax: (+34) 933 031 611. Web: www.anf.es

Certificado de Clase 2 de Persona Física
(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. *Signature Algorithm*	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 - *Signature HashAlgorithm*	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.		SI

						(String UTF8) Size [RFC 5280] 128		
	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 (see current address at 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
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	*Subject*							
	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 sujeto Preferiblemente se utilizará la semántica propuesta por la norma ETSI EN 319 412-1 No se incluye este campo en el certificado cuando es de seudónimo.		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. No se incluye este campo en el certificado cuando es de seudónimo.		
	2.5.4.42	Given Name (G)	*Nombre del sujeto.* *Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)*	*(String UTF8) Size 40.* *Obligatorio según ETSI EN 319 412-2*	AR manager	Nombre del sujeto (tal como consta en su DNI/ NIE/pasaporte). No se incluye este campo en el certificado cuando es de seudónimo.		SI
	2.5.4.4	SurName (SN)	*Apellidos del sujeto.* *Primer apellido, espacio en blanco, segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte*	*(String UTF8) Size 80.* *Obligatorio según ETSI EN 319 412-2*	AR manager	Apellido(s) del sujeto (tal como consta en su DNI/NIE/pasaporte). No se incluye este campo en el certificado cuando es de seudónimo.		SI

	2.5.4.65	Seudónimo	*Seudónimo elegido por el suscriptor.*	*Según ETSI EN 319 412-2*	AR manager	Especifica que el certificado ha sido emitido con un seudónimo		
	2.5.4.3	Common Name (CN)	*Nombre completo + DNI sujeto*	*(String UTF8) Size 132 [RFC 5280]*	AR manager	Se deben introducir el nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI Con seudónimo se incluye el seudónimo elegido por el suscriptor y la mención (SEUDONIMO)		SI
	2.5.4.11	Organisational Unit (OU)	**AUTENTICACION**	*Certificado de Clase 2 de Persona Fisica (AUTENTICACION)*	String UTF8) Size [RFC 5280] 128	AR Manager el concepto. ANF CT los sufijos FIRMA AUTENTICACIÓN, y CIFRADO. Certificados con seudónimo se incluye la mención CON SEUDONIMO	Descripción del tipo de certificado	SI
			FIRMA token software criptográfico.	*Certificado de Clase 2 de Persona Fisica (FIRMA)*				
			FIRMA Token SSCD	*Certificado de Clase 2 de Persona Fisica (FIRMA) SSCD*				
			FIRMA Servicio Centralizado	*Certificado de Clase 2 de Persona Fisica (FIRMA) D*				
			CIFRADO	*Certificado de Clase 2 de Persona Fisica (CIFRADO)*				
	2.5.4.10	Organisation (O)	*Ej: O = Nombre Colegio / número colegiado.* *En el caso de capacitación profesional: puede incluir el nombre de la asociación, gremio o agrupación a la que pertenece. O emisor de la titulación de capacitación profesional. Adicionalmente se puede incluir el número de asociado o agremiado como se especifica en el supuesto anterior.* *En el caso de autónomos puede incluir: Nombre comercial registrado o Marca registrada a nombre del sujeto.*	*(String UTF8) Size [RFC 5280] 128*	AR manager	En el caso de titulación colegiada: Nombre del Colegio Oficial del que es miembro activo. Adicionalmente se incluye el número de colegiado separado por el carácter "/".		
	2.5.4.12	Titulo (T)	*Título del sujeto*	*(String UTF8) Size [RFC 5280] 128*	AR manager	Profesión del sujeto, Título/ cargo / rol del suscriptor		
	2.5.4.13	Description			AR manager	Describe el objeto asociado (T) y (O)		
	Nombre alternativo del sujeto - 2.5.29.17							

Nombre alternativo del sujeto – SubjectAlternativeName Ver NOTA 2	*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			
	1.3.6.1.4.1.18332.11	*Nombre completo de una persona física o jurídica, que otorga una representación al suscriptor*		AR manager	No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.12	*Nombre de pila de la persona física que otorga una representación al suscriptor*		AR manager	No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.13	*Apellidos de la persona física que otorga una representación al suscriptor*		AR manager	No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.14	*NIF / DNI / NIE de la entidad jurídica o persona física que otorga una representación al suscriptor*		AR manager	No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.20.3	*Nombre suscriptor*		AR manager	Nombre (suscriptor) No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.20.4	*Apellido 1 suscriptor*		AR manager	Primer apellido (suscriptor) No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.20.5	*Apellido 2 suscriptor*		AR manager	Segundo apellido (suscriptor) No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.20.8	*p.e.: DNI*		AR manager	Tipo de cédula de identidad presentada por el suscriptor No se incluye este campo en el certificado cuando es de seudónimo.		
	1.3.6.1.4.1.18332.20.13	*p.e.: española*		AR manager	Nacionalidad (suscriptor)		
SubjectDirect	*SubjectDirectoryAttributes* - 2.5.29.9						
	2.5.4.20	*TelephoneNumber*		AR manager	Teléfono del suscriptor		

oryAttributes Ver NOTA 2	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://www.anf.es/app/ + (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		
	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 26144-565013283643648640*		AR Manager	Identificador del operador AR que tramitó la solicitud (todos los certificados emitidos por este Operador AR comparten el mismo valor)		
	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 cualificado*		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	*Se cumplimenta automáticamente por AR Manager*		AR manager	titular despacho AR		

	1.3.6.1.4.1.18332.42.13	*Se cumplimenta automáticamente por AR Manager*		AR manager	dpto operador AR		
	1.3.6.1.4.1.18332.47.1	*Se cumplimenta automáticamente por AR Manager*		ANF CT	UUID del Dispositivo de Firma Electrónica que almacena el certificado		
	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+Critocal+ANF CT*			AR manager	Version AR Manager + Critical + ANF CT empleado para la tramitación y versión		
	2.5.4.15	BusinessCategory	PrivateOrganization	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		
	1.3.6.1.4.1.31 1.60.2.1.1	JurisdictionOfIncorporationLocalityName	Localidad			AR manager	Localidad en la que está registrada la empresa		
	1.3.6.1.4.1.31 1.60.2.1.2	JurisdictionOfIncorporationStateOrProvinceName	Provincia			AR manager	Provincia en la que está registrada la empresa		
	1.3.6.1.4.1.31 1.60.2.1.3	JurisdictionOfIncorporationCountryName	País			AR manager	País en el que está registrada la empresa		
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) NIST P-256			*(String UTF8)* *RSA en conformidad con la RFC 4055 [10] 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-caIssuers 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 cualificados *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**	***Presente*** *si el certificado es expedido con la calificación de cualificado. Anexo I eIDAS*	ANF CT	**qcStatements** en conformidad con ETSI EN 319 412-5		SI
		0.4.0.1862.1.4	QcSSCD	**FIRMA**	***SOLO si el dispositivo es SSCD - QcSSCD*** 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** *QcType 1*	***SOLO*** *en el* ***perfil (FIRMA),*** *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** *Permite determinar a sistemas automáticos que es un certificado del tipo FIRMA. 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	**FIRMA / AUTENTICACION**	*https://anf.es/en/*	ANF CT	Se proporciona la URL que permite acceder a todas las políticas de la PKI en inglés. Protocolo https ETSI EN 319 412-5		SI
		0.4.0.1862.1.2	QcLimitValue	**FIRMA / AUTENTICACION**	*Importe límite de responsabilidad asumido por el emisor expresado en EUROS*	AR Manager	<QcLimitValue> <money>EUR</money> <qcBase>1</qcBase> <qcExp>3</qcExp> </QcLimitValue> No se incluye en el tipo CIFRADO		SI

		0.4.0.1862.1.3	QcRetentionPeriod	**FIRMA / AUTENTICACION**	*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	No se incluye en el tipo CIFRADO		SI
		0.4.0.194121.1.1	semnaticsId-Natural	**FIRMA / AUTENTICACION**	Para indicar semántica de persona fisica 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	**(AUTENTICACION)**		[1]Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.18332.3.4.1.1.22	AR Manager	OID propietario de ANF AC		SI
			(FIRMA) token software criptográfico.		[1]Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.18332.3.4.1.2.22				
			(CIFRADO)		[1]Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.18332.3.4.1.3.22				
			(FIRMA) token SSCD		[1]Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.18332.3.4.1.4.22				
			(FIRMA) Servicio Centralizado		[1]Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.18332.3.4.1.5.22				
		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		
		PolicyIdentifier	**SOLO PARA TIPO FIRMA**	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			

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	*Tipo certificado*: **FIRMA** **Token SSCD**		Sin repudio (c0)	AR Manager		SI	
		Tipo certificado: **FIRMA** ***token software criptográfico.***		Sin repudio (c0)				
		Tipo certificado: **FIRMA** **Servicio Centralizado**		Sin repudio (c0)				
		Tipo certificado: **AUTENTICACION**		Firma digital,				
		Tipo certificado: **CIFRADO**		KeyEncipherment, dataEncipherment	AR Manager		SI	
Uso mejorado de las claves - *Extended key usage*	2.5.29.37	**Firma / Autenticación**	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
Nombre descriptivo		*Se cumplimenta automáticamente por AR Manager*			AR Manager	Se deben introducir el nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI **Codificado según se indica en el pie de página NOTA 1**		

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 reflejen 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*