Certification Policy for Electronic Seal and Public Administration Electronic Seal. Certificate Profile

Address: B2, Industry Street, Qormi, QRM 3000 (Malta)
Telephone: (+356) 2299 3100
Fax: (+356) 2299 3101. Web: www.anfacmalta.com

Security Level

Public Document

Important Notice

Address: B2, Industry Street, Qormi, QRM 3000 (Malta)

Telephone: (+356) 2299 3100

Fax: (+356) 2299 3101. Web: www.anfacmalta.com

Electronic Seal Certificate

TOKEN BY SOFTWARE - HSM TOKEN

Field	OID	value		Standard	APP	Clarification	Crit	Mand
Version		2 = (V3)		RFC 5280	Issuer	Integer: =2 ([RFC5280] describes the certificate version when using extensions, e.g. v3 its value must be 2)		YES
Serial number				RFC 5280	Issuer	Automatically set by ANF AC. [RFC5280] positive integer, no more than 20 octets (1- 2^{159}) It is used to univocally identify the certificate		YES
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		RFC 5280	Issuer	String UTF8 (40) Signature Algorithm identifier. Identifying the algorithm type.		YES
SignatureHashAlgorithm	2.16.840.1.101.3.4.2.1	sha256			Issuer	Identifier of the signature hash Algorithm		YES
Issuer	2.5.4.3	Common Name (CN)	*e.g. ANF Trusted ID CA1*		AR Manager	Common name of the CA issuing the certificate		YES
	2.5.4.5	SERIALNUMBER	MT23399415		AR Manager	ANF AC VAT number		YES
	2.5.4.97	Organisation Identifier	*This is the VAT number.* *At present ANF AC does not include it*	eIDAS	Issuer	Identification of the issuer organization. As specified in clause 5.1.4 of ETSI EN 319 412-1 [7].		
		EmailAddress (E)	info@anfacmalta.com		Issuer	CA Email		
	2.5.4.11	Organisational Unit (OU)	Organisational unit within the Certification Services Provider responsible for the certificate issuance		AR Manager	As it appears in the certificate of the issuer. (String UTF8) Size [RFC 5280] 128		YES
	2.5.4.10	Organisation (O)	*e.g. ANF AC Malta, Ltd*		Issuer	Official name of the Certification Services Provider		YES
		Locality (L)	*e.g. Qormi (see current address at http://www.anfacmalta.com)*		Issuer	Locality/address of the Certification Services Provider (String UTF8) Size [RFC 5280] 128		

		State (ST)	*e.g. Qormi*		Issuer	State of the Certification Services Provider		
	2.5.4.6	Country (C)	*e.g. MT*	(2 character ISO 3166 country code [5])	AR Manager	Country of the Certification Services Provider (PrintableString) It will be coded according to "ISO 3166-1-alpha-2 code elements" Size 2 [RFC 5280]		YES
AuthorityCertIssuer				(String UTF8) Size 128	Issuer	Name of the CA to which it corresponds the keyIdentifier		
AuthorityCertSerialNumber				(Integer)	Issuer	Serial number of the CA certificate		
Identifier of the issuer entity key - *Authority KeyIdentifier*	2.5.29.35	Hash with SHA1 of the public key used to sign the certificate		RFC 5280 (String UTF8)	Issuer	Identifier derived from using the hash function on the public key of the subject. It is a means to identify the public key corresponding to the private key used to sign a certificate		YES
Issuer Alternative Name	2.5.29.18							
Valid from *NotBefore*					Issuer	Validity start date		YES
Valid until *NotAfter*					Issuer	Validity end date		YES
Subject *(all fields encoded using UTF-8)*	2.5.4.6	Country (C)	*Subject's country = subscriber*	*Two-digit country code* *ISO 3166-1*	AR manager	According to ETSI-QC this field must be completed obligatorily See RFC 3739 / ETSI 101862		YES
	2.5.4.7	Locality (L)	*Subject's city*	*(String UTF8)* *Size [RFC 5280] 128*	AR manager			YES
	2.5.4.8	State (ST)	*Subject's province*		AR manager			YES
	1.2.840.113549.1.9.1	EmailAddress (E)	*Subject's Email*		AR manager			
	2.5.4.5	SERIAL NUMBER (SN)	*E.g.: IDCMT-000000A. 3 characters to indicate the document number (IDC= national identity document) + 2 characters to identify the country (MT) + ID number*	*(Printable String)) Size [RFC 5280] 64*	AR manager	Tax Identification number of the subscriber Preferably the semantics proposed by the standard ETSI EN 319 412-1 will be used		YES

	2.5.4.97	OrganizationIdentifier	*The certificate must include at least= Serial Number or OrganizationIdentifier (VAT number), e.g.* *VATMT-00000000*	*According to the technical standard ETSI EN 319 412-1 (VATES* + VAT number *of the entity)*		AR manager	VAT number. VAT number, as it appears in the official registries. Coded According to the European Standard EN 319 412-1 Do not confuse with the National/Foreign Citizen ID Card, it is the VAT number for the EU		
	2.5.4.10	OrganizationName (O)	*e.g. Company name. LTD.*	*ETSI EN 319 412-1 [i.4], clause 5*		AR manager	Corporate name, as it appears in the official registers		YES
	2.5.4.42	Given Name (G)	*e.g.: "JOSEPH"*	*(String UTF8) Size 40.* *Mandatory according to ETSI EN 319 412-2*		AR manager	First name of the person responsible for the certificate (representative of the entity) according to the National Citizen ID Card or in case of a foreigner to the passport.		YES
	2.5.4.4	SurName (SN)	*e.g.: "SMITH RICHARDSON – 000000A"*	*(String UTF8) Size 80.* *Mandatory according to ETSI EN 319 412-2*		AR manager	First surname, blank space, second surname of the person responsible for the certificate, according to identity document (National/Foreign Citizen ID Card / Passport), dash and National / Foreign Citizen ID Card or passport number		YES
	2.5.4.3	Common Name (CN)	*e.g.: "VALIDATION AND ELECTRONIC SIGNATURE PLATFORM*	*(String UTF8) Size 132 [RFC 5280]*		AR manager	Name of system or application of automatic process.		YES
	2.5.4.11	Organisational Unit (OU)	**Electronic Seal Certificate** **Medium Level Public Administration Electronic Seal** **High Level Public Administration Electronic Seal**	 *Only in HSM devices*		String UTF8) Size [RFC 5280] 128	AR Manager The suffix HIGH level MEDIUM level is included by ANF CT	Description of certificate type	YES
	2.5.4.11	Organisational Unit (OU)	*e.g.: EXPLOITATION SUBDIRECTION*			String UTF8) Size [RFC 5280] 128	AR Manager	Name of the unit within the organisation providing the service	
	2.5.4.11	Organisational Unit (OU)	ONLY in Public Administration certificates	*e.g.: MT00000000*		*String UTF8) Size [RFC 5280] 128*	AR Manager	DIR3code of the unit	

	2.5.4.13	Description	*e.g.* *Registration Number: XXX / Date of Registration: XXX / Name of Company: XXX / Registered Office: XXX*		AR manager	Codification of the public document that certifies the faculty of the signatory or the registration data		YES
	2.5.4.12	Title (T)	*e.g. Sole Administrator*		AR manager	Type of legal empowerment of the legal representative.		
SubjectAlternativeName	SubjectAlternativeName - 2.5.29.17							
	email e.g.: peter@cial.com		*Name RFC822* *(String) Size [RFC 5280] 255*		ANF CT	Email of the person responsible for the certificate		YES
	DNSName *Directory Name*				AR manager	May include web URL		
	Electronic Seal	*1.3.6.1.4.1.18339.10.1*	*e.g. Peter*		ANF CT	First name of legal representative		YES
	Electronic Seal	*1.3.6.1.4.1.18339.10.2*	*e.g. Williams*		ANF CT	First surname of legal representative		YES
	Electronic Seal	*1.3.6.1.4.1.18339.10.3*	*e.g. Turner*		ANF CT	Second surname of legal representative		YES
	Electronic Seal	*1.3.6.1.4.1.18339.10.4*	*e.g. 000000A*		ANF CT	Tax Identification number of legal representative		YES
	Electronic Seal	*1.3.6.1.4.1.18339.10.7*	*e.g. peterwilliams@anfacmalta.com*		ANF CT	Email address of legal representative		YES
	Electronic Seal	*1.3.6.1.4.1.18339.29.1*	*e.g. John*		ANF CT	Name of the Certificate		YES

						Responsible		
	Electronic Seal	*1.3.6.1.4.1.18339.29.2*	*e.g.: "Campbell"*		ANF CT	First surname of the Certificate Responsible		YES
	Electronic Seal	*1.3.6.1.4.1.18339.29.3*	*e.g.: "Parker"*		ANF CT	Second surname of the Certificate Responsible		YES
	Electronic Seal	*1.3.6.1.4.1.18339.29.4*	*e.g. 000000A*		ANF CT	Tax Identification number of the Certificate Responsible		YES
	Electronic Seal	*1.3.6.1.4.1.18339.29.5*	*e.g. johncampbell@acmalta.com*		ANF CT	E-mail of the Certificate Responsible		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.1	Certificate for Public Administration High Level Electronic Seal	*String UTF8) Size = 31*	ANF CT	Indicates type of certificate It is HIGH if the device is an HSM		YES
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.1	Certificate for Public Administration Medium Level Electronic Seal	*UTF8 String.*	ANF CT			YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.2	*e.g. Company name. LTD.*	*(String UTF8) Size = 80*	ANF CT	Name of the subscriber entity		YES
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.2	*e.g. Company name. LTD.*	*(String UTF8) Size = 80*	ANF CT	Name of the subscriber entity		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.3	*e.g.: MT00000000*	(String UTF8) Size = 9	ANF CT	VAT Number of the subscriber entity		YES
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.3	*e.g.: MT00000000*	(String UTF8) Size = 9	ANF CT	VAT Number of the subscriber entity		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.4	*e.g.: 000000A*	*(String UTF8) Size = 9*	ANF CT	National or Foreign Citizen ID Card of the person responsible		YES

						for the Seal		
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.4	*e.g.: 000000A*	*(String UTF8) Size = 9*	ANF CT	National or Foreign Citizen ID Card of the person responsible for the Seal		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.5	*e.g.: "VALIDATION AND ELECTRONIC SIGNATURE PLATFORM.*	*(String UTF8) Size = 128*	ANF CT	Brief description of the component that holds the seal certificate		YES
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.5	*e.g.: "VALIDATION AND ELECTRONIC SIGNATURE PLATFORM.*	*(String UTF8) Size = 128*	ANF CT	Brief description of the component that holds the seal certificate		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.6	*e.g.: "JOHN"*	*(String UTF8) Size 40*	ANF CT	First name of the certificate responsible		YES
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.6	*e.g.: "JOHN"*	*(String UTF8) Size 40*	ANF CT	First name of the certificate responsible		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.7	*e.g.: "CAMPBELL"*	*String UTF8) Size 40*	ANF CT	First surname of the certificate responsible		YES
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.7	*e.g.: "CAMPBELL"*	*String UTF8) Size 40*	ANF CT	First surname of the certificate responsible		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.8	*e.g.: "PARKER"*	*String UTF8) Size 40*	ANF CT	Second surname of the certificate responsible		YES
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.8	*e.g.: "PARKER"*	*String UTF8) Size 40*	ANF CT	Second surname of the certificate responsible		YES
	Public Administration HIGH level	2.16.724.1.3.5.6.1.9	*e.g. johncampbell@acmalta.com*	*(String) Size [RFC 5280]*	ANF CT	Email		YES

				255				
	Public Administration MEDIUM level	2.16.724.1.3.5.6.2.9	*e.g. johncampbell@acmalta.com*	*(String) Size [RFC 5280] 255*	ANF CT	Email		YES
SubjectDirectoryAttributes	SubjectDirectoryAttributes - 2.5.29.9							
	1.3.6.1.4.1.18339.10.10	*e.g.: SHA256-gsq33wq/udldyk5ZN84paMeYx*						
	1.3.6.1.4.1.18339.10.10.1	*e.g.: https://tomcat2.anf.es/cliente_archivo_ws/poderes/(localizador AR=OID1.3.6.1.4.1.18332.19)*			AR manager	It is the link that allows to download the document that accredits mandate or power in favor of the representative		
	1.3.6.1.4.1.18339.19	*e.g. 33993893-503677*			AR manager	Request locator (Sequential of process-identifier of RA or IRM Operator that processed it)		
	1.3.6.1.4.1.18339.19.1	*e.g. 26144-56501328 3643648640*			AR manager	Identifier of RA Operator who processed the request. NOTE: In the case of RA, IRM or PKI Operator certificates, this OID corresponds to the identifier of the operator holding the certificate, outlined in the first part of the code		
	1.3.6.1.4.1.18339.30.1	*Full name of the country to which the issuance corresponds*			AR manager	The certificate is subjected to the		

					legislation of that country		
	1.3.6.1.4.1.18339.40.1	*e.g. Qualified certificate*		AR manager	Qualification with which the certificate was issued		
	1.3.6.1.4.1.18339.41.1	*1000*		AR manager	Limitation of liability assumed by the CA		
	1.3.6.1.4.1.18339.41.2	*e.g. Purchase contracts signing*		AR manager	Use of the certificate limited to the concept expressed in this field		
	1.3.6.1.4.1.18339.41.3	*e.g. 10.000*		AR manager	Limitation of use of the certificate by amount		
	1.3.6.1.4.1.18339.41.4	*e.g. euros*		AR manager	Currency in which values are expressed 1.3.6.1.4.1.18339.41.1 1.3.6.1.4.1.18339.41.3		
	1.3.6.1.4.1.18339.42.1			AR manager	Identifier of the Recognized Registration Authority to which the RA operator belongs		
	1.3.6.1.4.1.18339.42.11			AR manager	RA office holder		
	1.3.6.1.4.1.18339.42.13			AR manager	RA operator department		
	1.3.6.1.4.1.18339.47.1	*e.g. = 8&1EB4F96F*		ANF CT	UUID of the Electronic Signature Device that stores the certificate		
	1.3.6.1.4.1.18339.47.3	*HSM token model*		AR manager	ONLY if it is a HSM token		
	1.3.6.1.4.1.18339.90			AR manager	Descriptive		

					business or professional aspects of the activity		
	1.3.6.1.4.1.18339.90.1			AR manager	professional aspects of interest suffix 01		
	1.3.6.1.4.1.18339.90.2			AR manager	professional aspects of interest suffix 02		
	1.3.6.1.4.1.18339.90.3			AR manager	professional aspects of interest suffix 03		
	1.3.6.1.4.1.18339.91.2			AR manager	Year of origin of the activity		
	1.3.6.1.4.1.18339.92			AR manager	Own trademarks or tradenames		
	1.3.6.1.4.1.18339.92.1			AR manager	Trademarks it distributes suffix 1		
	1.3.6.1.4.1.18339.92.2			AR manager	Trademarks it distributes suffix 2		
	1.3.6.1.4.1.18339.92.3			AR manager	Trademarks it distributes suffix 3		
	1.3.6.1.4.1.18339.93			AR manager	Geographical scope in which it carries out its activity		
	1.3.6.1.4.1.18339.94			AR manager	Addresses places headquarters		
	1.3.6.1.4.1.18339.94.1			AR manager	Offices suffix 01		
	1.3.6.1.4.1.18339.94.2			AR manager	Offices suffix 02		
	1.3.6.1.4.1.18339.94.3			AR manager	Offices suffix 03		
	1.3.6.1.4.1.18339.95			AR manager	Companies with which it relates		

	1.3.6.1.4.1.18339.95.1			AR manager	Companies with which it relates suffix 01		
	1.3.6.1.4.1.18339.95.2			AR manager	Companies with which it relates suffix 02		
	1.3.6.1.4.1.18339.95.3			AR manager	Companies with which it relates suffix 03		
	1.3.6.1.4.1.18339.96			AR manager	Banking entities with which it has relationships		
	1.3.6.1.4.1.18339.96.1			AR manager	Current accounts, SWIFT		
	1.3.6.1.4.1.18339.97			AR manager	economic information		
	1.3.6.1.4.1.18339.97.1			AR manager	economic information suffix 01		
	1.3.6.1.4.1.18339.97.2			AR manager	economic information suffix 02		
	1.3.6.1.4.1.18339.97.3			AR manager	economic information suffix 03		
	1.3.6.1.4.1.18339.98			AR manager	Number of employees		
	1.3.6.1.4.1.18339.600	*e.g.: AR Manager desktop v.3.6*		AR manager	AR Manager program used for processing and version		
Subject Key Identifier	2.5.29.14	Hash in SHA1 of the public key used to sign the certificate	*RFC 5280* *In accordance with standards RFC2459 & PKCS#1*	Issuer	Identifier derived from using the hash function on the public key of the subject		YES
SubjectPublicKeyInfo		RSA (2048)	*(String UTF8)* *RSA in*	Issuer	Field to transport the public key and to		YES

					accordance with RFC 4055 [10] and ECC algorithm in accordance with the RFC 5639 [11]		identify the algorithm with which the key is used.		
Access to issuer entity information	1.3.6.1.5.5.7.1.1	AccessMethod [1]	*[1] Access to authority information* *Access method = On line certificate status protocol (1.3.6.1.5.5.7.48.1)*		*Issuer*	Id-ad-ocsp with OID: (OCSP)			YES
		AccessLocation [1]	*Alternative name:* *URL address=http://*		*Issuer*	OCSP Responder address			YES
		AccessMethod [2]	*1.3.6.1.5.5.7.48.2*		*Issuer*	id-ad-calssuers with OID			
		AccessLocation [2]	*URL address=*		*Issuer*	Location of CA certificate			
CRL distribution points	2.5.29.31	cRLDistributionPoint [1]	*[1] CRL distribution point* *Distribution point name:* *Full name:* *URL address*		*Issuer*	Indicates CRL download point.			YES
		DistributionPoint [2]				Distribution point of the web where the CRL resides (HTTP or LDAP) number 2			
		DistributionPoint [3]				Distribution point of the web where the CRL resides (HTTP or LDAP) number 3			
Qualified Certificates Statements TSI EN 319 412-1, before ETSI TS 101 862	1.3.6.1.5.5.7.1.3	0.4.0.1862.1.1	QcCompliance		***Present*** *if the certificate is issued with the recognized qualification. Annex I eIDAS*	ANF CT	**qcStatements** in accordance with ETSI EN 319 412-5		YES
		0.4.0.1862.1.4	**QcSSCD**	**only included with HSM device**	***Present if the device is SSCD*** Secure Signature Creation	ANF CT	*Determines that the private key associated with the public key contained in the electronic certificate is on a secure signature creation device,*		YES

					Device (SSCD)		*Regulation (EU) 910/2014 [I.8]*		
		0.4.0.1862.1.6.2	QcType-eseal	***QcType 2***	*QcType 2 is outlined* *ETSI EN 319 412-5*	ANF CT	**id-etsi-qcsQcType** clause 4.2.3 in ETSI EN 319 412-5 *Follows the following encoding:* 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)		YES
		0.4.0.1862.1.5	QcPDS	*https://www.anfacmalta.com*	It is provided the URL that allows access to all policies of the PKI in English. Https protocol *ETSI EN 319 412-5*	ANF CT			YES
		0.4.0.1862.1.2	QcLimitValue		*Limit amount of liability assumed by the issuer expressed in EUROS*	ANF CT	<QcLimitValue> <money>EUR</money> <qcBase>1</qcBase> <qcExp>3</qcExp> </QcLimitValue>		YES
		0.4.0.1862.1.3	QcRetentionPeriod		*Integer: =15* *([ETSI EN 319 412-5]* *Describes the conservation period* *of all information, relevant to the use of a certificate, after its* *expiration)*	ANF CT			YES
		0.4.0.194121.1.2	semnaticsId-Legal		To indicate the semantics of a legal person defined by the EN 319 412-1	ANF CT			
Certificate Policies	2.5.29.32	PolicyIdentifier	**Electronic Seal** Token software criptográfico		[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.25.1.1.1	AR manager	ANF AC proprietary OID		YES
			Electronic Seal Token SSCD		[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.25.1.1.4				
			Public Administration		[1] Certificates policy:				

			High Level Electronic Seal	Policy identifier = 1.3.6.1.4.1.18339.25.1.1.2				
			Public Administration Medium Level Electronic Seal	[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.25.1.1.3				
		PolicyIdentifier	**Public Administration High Level Electronic Seal**	2.16.724.1.3.5.6.1	AR manager			YES
			Public Administration Medium Level Electronic Seal	2.16.724.1.3.5.6.2				
		PolicyCPSLocation	[1,1] Policy certifier information: Policy certifier ID =CPS Certifier: http://www.anfacmalta.com		AR manager			
		User notice	[1,2] Policy certifier information: Policy certifier ID = User notice Certifier: Notice text = Certificate in compliance with electronic signature legislation. Before accepting it verify integrity, limitations, validity, and authorized uses.		AR manager	Maximum 200 characters. A statement is made by the issuing CA, which refers to certain legal norms.		YES
		PolicyIdentifier	**HSM TOKEN**	qcp-legal-qscd (0.4.0.194112.1.3)	ANF CT	Qualified signature certificate, per Regulation EU 910/2014 eIDAS		YES
			SOFTWARE TOKEN	qcp-legal (0.4.0.194112.1.1)	ANF CT			
Fields conditioned by the use of the certificate	2.5.4.15	BusinessCategory	PrivateOrganization		AR manager	for private organization		
			GovernmentEntity		AR manager	for public entity		
			BusinessEntity		AR manager	for company		
			Non-commercialEntity		AR manager	for non-commercial entity		
	1.3.6.1.4.1.31 1.60.2.1.1	JurisdictionOfIncorporationLocalityName	Locality		AR manager	locality in which the company is registered		
	1.3.6.1.4.1.31 1.60.2.1.2	JurisdictionOfIncorporationStateOrProvinceName	Province		AR manager	province in which the company is registered		
	1.3.6.1.4.1.31 1.60.2.1.3	JurisdictionOfIncorporationCountryName	Country		AR manager	country in which the company is registered		
Basic Constraints	2.5.29.19	Type of matter =End entity Route Length Restriction =None CA = FALSE			Issuer	determines that it is an end-user certificate	**YES**	
Key usage	2.5.29.15	*Digital Signature*	It is used when performing the digital asset authentication function of the legal person		AR manager		**YES**	

		Content Commitment	It is used when performing the function of electronic seal of document issued by legal person				
		Key Encipherment	It is used for management and transport of keys				
		Data Encipherment	It is used for data encryption.				
Extended key usage	2.5.29.37	Client Authentication	1.3.6.1.5.5.7.3.2	AR manager			YES
		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				
Identification algorithm		sha1		Issuer			YES
Signature Value				Issuer	Signature encoded as bit chain		YES
Digital fingerprint				Issuer	Certificate digital fingerprint		YES

ETSI EN **319 412-2 v2.1.1** (Part 2: *Certificate profile for certificates issued to natural persons*) defines the content requirements of certificates issued to natural persons.

The profile is based on the IETF RFC 5280 recommendations and the ITU-T X.509 standard. The information used to define the identity and attributes of the natural person certificate signatory, without pseudonyms, is broken down into the following fields:

- *Field "Subject", using the attributes commonName, surname (or givenName) and countryName. In the attribute SerialNumber, can be include the National / Foreign Citizen ID Card of the signatory.*
- *Extension "Subject Alternative Names". No restrictions are included.*
- *Extension "Subject Directory attributes". The attributes of the Subject field should not be included.*

OIDs for qualified certificates

The coding of certain features of the qualified certificates are outlined by specific OIDs (Object Identifier).

The technical standard that indicated them was the **ETSI TS 101 862**, that reflected with the following OID (now obsolete):

- 1.3.6.1.5.5.7.0.11

And defining the information of the qualified certificate statement (QC-Statement) with the OID:

- 0.4.0.1862

At present, the standard of application is the **ETSI EN 319 412-1** which has resulted in the information on qualified certificates, not included in the previous standard, be reflected with a new OID:

- 0.4.0.194121

Therefore, qualified certificates will be able to indicate certain features of the certificates with OIDs that begin with **0.4.0.1862** (Originally designed for electronic signature of natural persons according to the Directive 1999/93, but nowadays also suitable for legal persons due to the extension of concepts such as the electronic seal of Regulation EU 910/2014 EIDAS) and others with OID that begin with **0.4.0.194121** (specifically to differentiate the certificates of natural and legal person as the Regulation EU 910/2014 EIDAS does).

These are the main OIDs:

- 0.4.0.1862.1.1 – qcStatement – QcCompliance (**Mandatory**)
- 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 (**Mandatory**)
- 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** (for natural person certificates – electronic signature)
- 0.4.0.194121.1.2 -> id-etsi-qcs-SemanticsId-Legal -> **Legal person semantics** (for legal person certificates – electronic seal)
- 0.4.0.1862.1.5 – qcStatement – QcPDS (**Mandatory**).

It will provide at least one URL to a PDS (PKI Disclosure Statements) in English. Other PDS documents can be referenced in other languages with this QCStatement provided they are equivalent to the PDS in English.
No reference should be made to more than one PDS per language.

- 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*