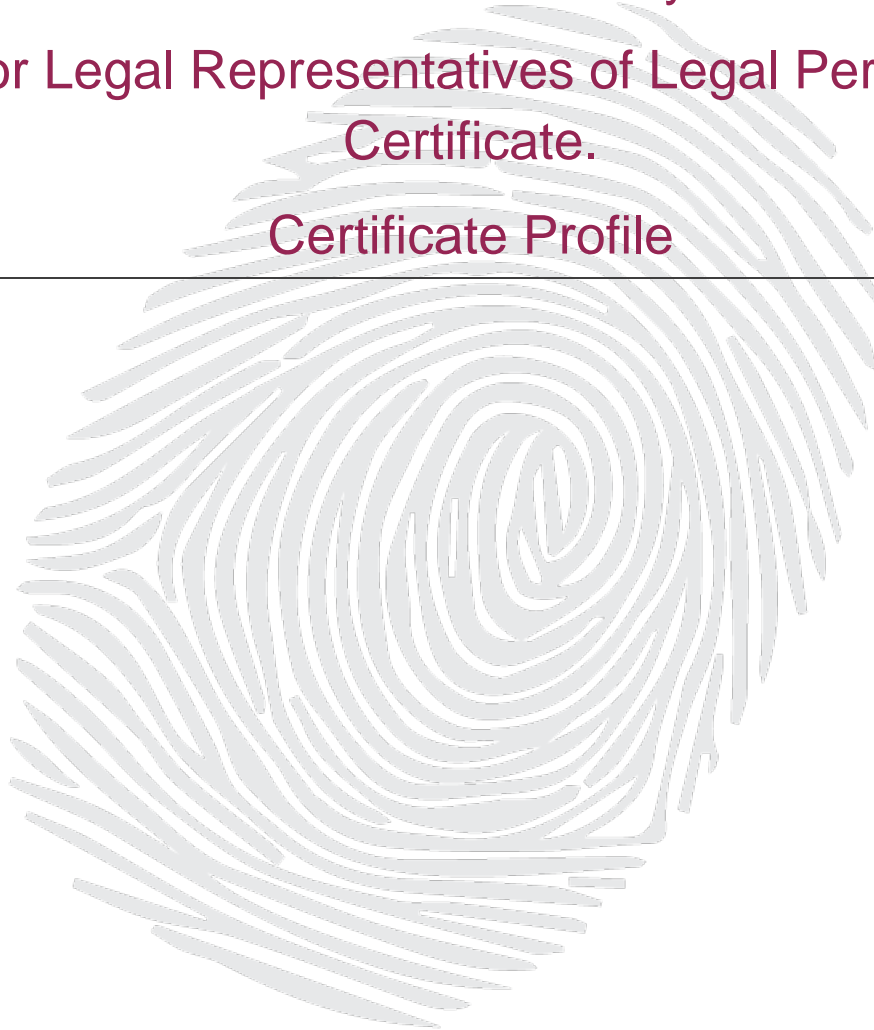




Certification Policy for Legal Representatives of Legal Persons Certificate. Certificate Profile



Security Level

Public Document

Important Notice

This document is property of ANF AC MALTA

Distribution and reproduction prohibited without authorization by ANF AC MALTA

Copyright © ANF AC MALTA 2017

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

Telephone: (+356) 2299 3100

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



Certificate for Legal Representatives of Legal Persons
(AUTHENTICATION) (SIGNATURE) (ENCRYPTION)
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	
<i>SignatureAlgorithm</i>	1.2.840.113549.1.1.11	sha256WithRSAEncryption		RFC 5280	Issuer	String UTF8 (40) Signature Algorithm identifier. Identifying the algorithm type.		YES	
<i>SignatureHashAlgorithm</i>	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)	<i>e.g. ANF Trusted ID CA1</i>		AR Manager	Common name of the CA issuing the certificate		YES	
	2.5.4.5	SERIALNUMBER	MT23399415		AR Manager	ANF AC's VAT number		YES	
	2.5.4.97	Organisation Identifier	<i>This is the VAT number. At present ANF AC does not include it.</i>	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)	Organizational 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)	<i>e.g. ANF AC Malta, Ltd</i>			Issuer	Official name of the Certification Services Provider		YES
		Locality (L)	<i>e.g. Qormi (see current address at http://www.anfacmalta.com)</i>			Issuer	Locality/address of the Certification Services Provider		



						(String UTF8) Size [RFC 5280] 128		
		State (ST)	<i>e.g. Qormi</i>		Issuer	State of the Certification Services Provider		
	2.5.4.6	Country (C)	<i>e.g. MT</i>	(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
AuthorityCertificateIssuer				(String UTF8) Size 128	Issuer	Name of the CA to which it corresponds the keyIdentifier		
AuthorityCertificateSerialNumber				(Integer)	Issuer	Serial number of the CA certificate		
Identifier of the issuer entity key - AuthorityKeyIdentifier	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
	2.5.4.6	Country (C)	<i>Subject's country = subscriber</i>	<i>Two-digit country code ISO 3166-1</i>	AR manager	According to ETSI-QC this field must be completed obligatorily See RFC 3739 / ETSI 101862		YES
	2.5.4.7	Locality (L)	<i>Subject's city</i>	(String UTF8) Size [RFC 5280] 128	AR manager			YES
	2.5.4.8	State (ST)	<i>Subject's state</i>		AR manager			YES
	1.2.840.113549.1.9.1	EmailAddress (E)	<i>Subject's Email</i>		AR manager			
	2.5.4.5	SERIAL NUMBER (SN)	<i>E.g.: IDCMT-000000A. 3 characters to indicate the</i>	(Printable String)) Size [RFC 5280] 64	AR manager	Tax Identification number of the subject Preferably the semantics proposed by the standard ETSI		YES



			<i>document number (IDC= national identity document) + 2 characters to identify the country (MT) + ID number</i>			EN 319 412-1 will be used		
2.5.4.97	Organisation Identifier		<i>The certificate must include at least= Serial Number or Organization Identifier (VAT number), e.g. VATMT-00000000</i>	<i>According to the technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity)</i>	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 (DNI), it is the VAT number for the EU		
2.5.4.10	Organization Name (O)		<i>e.g. Company name.</i>	<i>ETSI EN 319 412-1 [i.4], clause 5</i>	AR manager	Corporate name, as stated in official registries.		YES
2.5.4.42	Given Name (G)		<i>First name of the legal representative, according to identity document (National/Foreign Citizens ID Card / Passport)</i>	<i>(String UTF8) Size 40. Mandatory according to ETSI EN 319 412-2</i>	AR manager	Name of legal representative (as it appears on his/her National/Foreign Citizens ID Card / Passport).		YES
2.5.4.4	SurName (SN)		<i>Surname(s) of the legal representative. First surname, blank space, second surname of the person responsible for the certificate in accordance with the National ID Card or in case of a foreigner the passport</i>	<i>(String UTF8) Size 80. Mandatory according to ETSI EN 319 412-2</i>	AR manager	Surname(s) (as it appears on his/her National/Foreign Citizens ID Card / Passport).		YES
2.5.4.3	Common Name (CN)			<i>(String UTF8) Size 132 [RFC 5280]</i>	AR manager	The name and two surnames must be entered in accordance with an identity document (National/Foreign Citizens ID Card / Passport).		YES
2.5.4.11	Organisational Unit (OU)	AUTHENTICATION		Legal Representative of a Legal Person Certificate (AUTHENTICATION)	String UTF8) Size [RFC 5280] 128	AR Manager the concept. ANF CT the suffixes SIGNATURE AUTHENTICATION, and ENCRYPTION	Description of certificate type	YES
		SIGNATURE		Legal Representative of a Legal Person Certificate (SIGNATURE).				
		SIGNATURE	Cryptographic software token	Legal Representative of a Legal Person Certificate (SIGNATURE) SSCD				
		SIGNATURE	SSCD token	Legal Representative of a Legal Person Certificate (SIGNATURE) CS				
		ENCRYPTION	Centralized Service	Legal Representative of a				

				Legal Person Certificate (ENCRYPTION).					
	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 - 2.5.29.17									
SubjectAlternativeName	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		e.g.: www.anfacmalta.com			AR manager	May include web URL		
	1.3.6.1.4.1.18339.10.1			UTF8 String.		AR manager	First name of legal representative		
	1.3.6.1.4.1.18339.10.2			UTF8 String.		AR manager	First surname of legal representative		
	1.3.6.1.4.1.18339.10.3			UTF8 String.		AR manager	Second surname of legal representative		
	1.3.6.1.4.1.18339.10.4			UTF8 String.		AR manager	National/Foreign Citizens ID Card of legal representative		
	1.3.6.1.4.1.18339.10.8		e.g.: passport	UTF8 String.		AR manager	Type of identity document submitted by the legal representative		

	1.3.6.1.4.1.18339.10.9	<i>e.g.: Maltese</i>	<i>UTF8 String.</i>	AR manager	Nationality of the legal representative		
SubjectDirectoryAttributes	SubjectDirectoryAttributes - 2.5.29.9						
	2.5.4.20	<i>TelephoneNumber</i>		AR manager	Subscriber's telephone		
	2.5.4.23	<i>Facsimile</i>		AR manager	Subscriber's fax		
	2.5.4.9	<i>StreetAddress</i>		AR manager	Subscriber's address		
	2.5.4.16	<i>PostalAddress</i>		AR manager	Subscriber's postal address		
	2.5.4.17	<i>PostalCode</i>		AR manager	Subscriber's postal code		
	1.3.6.1.4.1.18339.10.10	<i>e.g.: SHA256-gsq33wq/udldyk5ZN84paMeYx</i>		AR manager	It is the hash of the document that accredits mandate or power in favor of the subject		
	1.3.6.1.4.1.18339.10.10.1	<i>e.g.: https://tomcat2.anf.es/cliente_archivo_ws/poderes/localizador_AR=OID1.3.6.1.4.1.18332.19</i>		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	<i>e.g. 33993893-503677</i>		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	<i>e.g. 26144-56501328 3643648640</i>		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	<i>Full name of the country to which the issuance corresponds</i>			AR manager	The certificate is subjected to the legislation of that country		
1.3.6.1.4.1.18339.40.1	<i>e.g. Qualified certificate</i>			AR manager	Qualification with which the certificate was issued		
1.3.6.1.4.1.18339.41.1	<i>1000</i>			AR manager	Limitation of liability assumed by the CA		
1.3.6.1.4.1.18339.41.2	<i>e.g. Purchase contracts signing</i>			AR manager	Use of the certificate limited to the concept expressed in this field		
1.3.6.1.4.1.18339.41.3	<i>e.g. 10.000</i>			AR manager	Limitation of use of the certificate by amount		
1.3.6.1.4.1.18339.41.4	<i>e.g. euros</i>			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	<i>Automatically completed by AR Manager</i>			AR manager	RA office holder		
1.3.6.1.4.1.18339.42.13	<i>Automatically completed by AR Manager</i>			AR manager	RA operator department		

1.3.6.1.4.1.18339.47.1	<i>Automatically completed by AR Manager</i>		ANF CT	UUID of the Electronic Signature Device that stores the certificate		
1.3.6.1.4.1.18339.47.3	<i>Automatically completed by AR Manager</i>		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		
1.3.6.1.4.1.18339.91.1			AR manager	Legal form of the subscriber		
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		
	1.3.6.1.4.1.18339.95.2			AR manager	Companies with which it relates suffix 01		
	1.3.6.1.4.1.18339.95.3			AR manager	Companies with which it relates suffix 02		
	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	<i>e.g.: AR Manager desktop v.3.6</i>		AR manager	AR Manager program used for processing and version		
<i>Subject Key Identifier</i>	2.5.29.14	Hash in SHA1 of the public key used to	<i>RFC 5280</i> <i>In accordance with standard</i>	Issuer	Identifier derived from using the hash function on the public key of the subject		YES

		sign the certificate			s RFC2459 & PKCS#1				
SubjectPublicKeyInfo		RSA (2048)			(String UTF8) RSA in accordance with RFC 4055 [10] and ECC algorithm in accordance with the RFC 5639 [11]	Issuer	Field to transport the public key and to identify the algorithm with which the key is used.		YES
Access to issuer entity information	1.3.6.1.5.7.1.1	AccessMethod [1]	[1] Access to authority information Access method = On line certificate status protocol (1.3.6.1.5.7.48.1)	Issuer		Id-ad-ocsp with OID: (OCSP)		YES	
		AccessLocation [1]	Alternative name: URL address=http://	Issuer		OCSP Responder address		YES	
		AccessMethod [2]	1.3.6.1.5.7.48.2	Issuer		id-ad-caIssuers 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 Certificate Statement	1.3.6.1.5.5.7.1.3	0.4.0.1862.1.1	QcCompliance	SIGNATURE / AUTHENTICATION	Present if the certificate is issued with the recognized qualification. Annex I eIDAS	ANF CT	qcStatements in accordance with	YES	



TSI EN 319 412-1, before ETSI TS 101 862						ETSI EN 319 412-5		
	0.4.0.1 862.1.4	QcSSCD	Only included in the SIGNATURE type	ONLY if the device is SSCD Secure Signature Creation Device (SSCD)	ANF CT	It is not included in the ENCRYPTION, nor AUTHENTICATION one. <i>Determines that the private key associated with the public key contained in the electronic certificate is on a secure signature creation device, Regulation (EU) 910/2014 [1.8]</i>		YES
	0.4.0.1 862.1.6 .1	QcType-esign	SIGNATURE QcType 1	ONLY in the profile (SIGNATURE), QcType 1 is outlined ETSI EN 319 412-5	ANF CT	id-etsi-qcsQcType clause 4.2.3 in ETSI EN 319 412-5 Not included in the ENCRYPTION, nor in the AUTHENTICATION one <i>It allows automatic systems to determine that it is a certificate of the type SIGNATURE. It follows the following encoding:</i> 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
	0.4.0.1 862.1.5	QcPDS	SIGNATURE / AUTHENTICATION	https://www.anfacmalta.com URL which allows Access to all the PKI policies in English. Https protocol ETSI EN 319 412-5	ANF CT	It is not included in the ENCRYPTION type		YES
	0.4.0.1 862.1.2	QcLimitValue	SIGNATURE / AUTHENTICATION	Limit amount of liability assumed by the issuer expressed in EUROS	AR Manager	<QcLimitValue> <money>EUR</money> <qcBase>1</qcBase> <qcExp>3</qcExp> </QcLimitValue> Not included in the ENCRYPTION type		YES
	0.4.0.1 862.1.3	QcRetentionPeriod	SIGNATURE / AUTHENTICATION	Integer: =15 ([ETSI EN 319 412-5]) Describes the conservation	ANF CT	Not included in the ENCRYPTION type		YES

					<i>period</i> <i>of all information, relevant to the use of a certificate, after its expiration)</i>					
		0.4.0.1 94121. 1.1	semnaticsd- Natural	SIGNATURE / AUTHENTICAT ION	To indicate the semantics of a natural person defined by the EN 319 412-1	ANF CT	Not included in the ENCRYPTION type			
Certificate Policies	2.5.29.32	PolicyIdentifier		(AUTHENTICATION)	[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.2.5.1.1	AR Manager	ANF AC proprietary OID		YES	
				(SIGNATURE) Cryptographic software token	[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.2.5.1.3					
				(ENCRYPTION)	[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.2.5.1.2					
				(SIGNATURE) HSM token	[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.2.5.1.10					
				(SIGNATURE) Centralized Service	[1] Certificates policy: Policy identifier = 1.3.6.1.4.1.18339.2.5.1.14					
		PolicyIdentifier		(AUTHENTICATION)	2.16.724.1.3.5.8	AR Manager				YES
				(SIGNATURE)	2.16.724.1.3.5.8					
				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 to 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	ONLY FOR SIGNATURE TYPE	HSM TOKEN	qcp-natural-qscd (0.4.0.1941 12.1.2)	ANF CT	Qualified signature certificate, according to Regulation EU 910/2014			
				SOFTWARE TOKEN	qcp-natural (0.4.0.1941 12.1.0)	ANF CT	According to Regulation eIDAS			
Fields conditioned by the use of the	2.5.4.15	BusinessCategory	PrivateOrganization		AR manager	for private organization				
			GovernmentEntity		AR manager	for public entity				



certificate			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	Certificate Type: SIGNATURE		AR manager		YES	
		Non-repudiation (c0)					
		Certificate Type: AUTHENTICATION		AR manager			
		Electronic signature, Non-repudiation (c0)					
Certificate Type: ENCRYPTION		AR manager					
KeyEncipherment,							
dataEncipherment							
Extended key usage	2.5.29.37	Signature / Authentication	1.3.6.1.5.5.7.3.2	AR manager			YES
			1.3.6.1.5.5.7.3.4				
Identification algorithm		sha1		Issuer			YES
Signature Value				Issuer	Signature encoded as bit chain		YES
Digital Fingerprint				Issuer	Certificate digital fingerprint		YES
Descriptive Name		<i>Automatically completed by AR Manager</i>		AR Manager	The name and two surnames must be entered in accordance with an identity document (National/Foreign Citizens ID Card).		

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-semanticId-Natural -> **Natural person semantics** (for natural person certificates – electronic signature)
- 0.4.0.194121.1.2 -> id-etsi-qcs-SemanticId-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*