



Certification Policy for Legal Representatives of Legal Persons. 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 2016

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

Telephone: (+356) 2299 3100

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



**Legal Representative of
Legal Person Certificate**
(AUTHENTICATION) (SIGNATURE) (ENCRYPTION)
TOKEN BY SOFTWARE - HSM TOKEN

Field	Value		Crit	Mandatory
Version	2 = (V3)			YES
Serial number				YES
<i>SignatureAlgorithm</i>	sha256WithRSAEncryption			YES
<i>SignatureHashAlgorithm</i>	sha256			YES
Issuer	Common Name (CN)	<i>e.g. ANF Trusted ID CA1</i>		YES
	SERIALNUMBER	MT23399415		YES
	Organisation Identifier	<i>This is the VAT number. At present ANF AC does not include it.</i>		
	EmailAddress (E)	info@anfacmalta.com		
	Organisational Unit (OU)	Organizational unit within the Certification Services Provider responsible for the certificate issuance		YES
	Organisation (O)	<i>e.g. ANF AC Malta, Ltd</i>		YES
	Locality (L)	<i>e.g. Qormi (see current address at http://www.anfacmalta.com)</i>		
	State (ST)	<i>e.g. Qormi</i>		
	Country (C)	<i>e.g. MT</i>		YES
AuthorityCertIssuer				
AuthorityCertSerial Number				
Identifier of the issuer entity key – <i>Authority KeyIdentifier</i>	Hash with SHA1 of the public key used to sign the certificate			YES
<i>Issuer Alternative Name</i>				
Valid from <i>NotBefore</i>				YES
Valid until				YES



<i>NotAfter</i>				
Subject <i>(all fields encoded using UTF-8)</i>	<i>Subject</i>			
	1.3.6.1.4.1.18838.1.1	<i>Subject's country = subscriber</i>		
	Country (C)	<i>Subject's city</i>		
	Locality (L)	<i>Subject's state</i>		
	State (ST)	<i>Subject's Email</i>		
	EmailAddress (E)	<i>E.g.: IDCMT-000000A. 3 characters to indicate the document number (IDC= national identity document) + 2 characters to identify the country (MT) + ID number</i>		
	SERIAL NUMBER (SN)	<i>The certificate must include at least= Serial Number or OrganizationIdentifier (VAT number), e.g. VATMT-00000000</i>		
	OrganizationIdentifier	<i>e.g. Company name.</i>		
	OrganizationName (O)	<i>First name of the legal representative, according to identity document (National/Foreign Citizens ID Card / Passport)</i>		
	Given Name (G)	<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>		
	SurName (SN)	<i>Subject's country = subscriber</i>		
	Common Name (CN)			
	Organisational Unit (OU)	AUTHENTICATION	Legal Representative of a Legal Person Certificate (AUTHENTICATION)	YES
		SIGNATURE	Legal Representative of a Legal Person Certificate (SIGNATURE).	
ENCRYPTION		Legal Representative of a Legal Person Certificate (ENCRYPTION).		
Description	<i>e.g. Registration Number: XXX / Date of Registration: XXX / Name of Company: XXX / Registered Office: XXX</i>			
Title (T)	<i>e.g. Sole Administrator</i>			
SubjectAlternativeName	SubjectAlternativeName - 2.5.29.17			
	<i>eMail</i>	<i>e.g.: peter@cial.com</i>		
	<i>DNSName</i> <i>Directory Name</i>	<i>e.g.: www.anf.es</i>		

	1.3.6.1.4.1.18339.10.1			
	1.3.6.1.4.1.18339.10.2			
	1.3.6.1.4.1.18339.10.3			
	1.3.6.1.4.1.18339.10.4			
	1.3.6.1.4.1.18339.10.8	<i>e.g.: passport</i>		
	1.3.6.1.4.1.18339.10.9	<i>e.g.: Maltese</i>		
SubjectDirectoryAttributes	<i>SubjectDirectoryAttributes – 2.5.29.9</i>			
	2.5.4.20	<i>TelephoneNumber</i>		
	2.5.4.23	<i>Facsimile</i>		
	2.5.4.9	<i>StreetAddress</i>		
	2.5.4.16	<i>PostalAddress</i>		
	2.5.4.17	<i>PostalCode</i>		
	1.3.6.1.4.1.18339.10.10	<i>e.g.: SHA256-gsq33wq/udldyk5ZN84paMeYx</i>		
	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>		
	1.3.6.1.4.1.18339.30.1	<i>Full name of the country to which the issuance corresponds</i>		
	1.3.6.1.4.1.18339.40.1	<i>e.g. Qualified certificate</i>		
	1.3.6.1.4.1.18339.41.1	<i>1000</i>		
	1.3.6.1.4.1.18339.41.2	<i>e.g. Purchase contracts signing</i>		
	1.3.6.1.4.1.18339.41.3	<i>e.g. 10.000</i>		
	1.3.6.1.4.1.18339.41.4	<i>e.g. euros</i>		
	1.3.6.1.4.1.18339.42.1			
	1.3.6.1.4.1.18339.42.11	<i>Automatically completed by AR Manager</i>		
	1.3.6.1.4.1.18339.42.13	<i>Automatically completed by AR Manager</i>		
	1.3.6.1.4.1.18339.47.1	<i>Automatically completed by AR Manager</i>		
	1.3.6.1.4.1.18339.47.3	<i>Automatically completed by AR Manager</i>		
	1.3.6.1.4.1.18339.90			
	1.3.6.1.4.1.18339.90.1			
	1.3.6.1.4.1.18339.90.2			
	1.3.6.1.4.1.18339.90.3			
	1.3.6.1.4.1.18339.91.2			
	1.3.6.1.4.1.18339.92			
	1.3.6.1.4.1.18339.92.1			

	1.3.6.1.4.1.18339.92.2			
	1.3.6.1.4.1.18339.92.3			
	1.3.6.1.4.1.18339.93			
	1.3.6.1.4.1.18339.94			
	1.3.6.1.4.1.18339.94.1			
	1.3.6.1.4.1.18339.94.2			
	1.3.6.1.4.1.18339.94.3			
	1.3.6.1.4.1.18339.95			
	1.3.6.1.4.1.18339.95.1			
	1.3.6.1.4.1.18339.95.2			
	1.3.6.1.4.1.18339.95.3			
	1.3.6.1.4.1.18339.96			
	1.3.6.1.4.1.18339.96.1			
	1.3.6.1.4.1.18339.97			
	1.3.6.1.4.1.18339.97.1			
	1.3.6.1.4.1.18339.97.2			
	1.3.6.1.4.1.18339.97.3			
	1.3.6.1.4.1.18339.98			
	1.3.6.1.4.1.18339.600	<i>e.g.: AR Manager desktop v.3.6</i>		
1.3.6.1.4.1.18339.19	<i>e.g. 33993893-503677</i>			
1.3.6.1.4.1.18339.19.1	<i>e.g. 26144-56501328 3643648640</i>			
Subject Key Identifier	Hash in SHA1 of the public key used to sign the certificate			YES
SubjectPublic KeyInfo	RSA (2048)			YES
Access to issuer entity information	AccessMethod [1]	<i>[1] Access to authority information Access method = On line certificate status protocol (1.3.6.1.5.5.7.48.1)</i>		YES
	AccessLocation [1]	<i>Alternative name: URL address=http://</i>		YES
	AccessMethod [2]	<i>1.3.6.1.5.5.7.48.2</i>		
	AccessLocation [2]	<i>URL address=</i>		
	cRLDistributionPoint [1]	<i>[1] CRL distribution point</i>		YES

CRL distribution points		<i>Distribution point name:</i>			
		<i>Full name:</i>			
		<i>URL address</i>			
	DistributionPoint [2]				
	DistributionPoint [3]				
Qualified Certificate Statement TSI EN 319 412-1, antes ETSI TS 101 862	QcCompliance	SIGNATURE / AUTHENTICATION	Present if the certificate is issued with the recognized qualification. Annex I eIDAS		YES
	QcSSCD	Only included in the SIGNATURE type	ONLY if the device is SSCD Secure Signature Creation Device (SSCD)		YES
	QcType- esign	SIGNATURE QcType 1	ONLY in the profile (SIGNATURE), QcType 1is outlined ETSI EN 319 412-5		YES
	QcPDS	SIGNATURE / AUTHENTICATION	https://anfacmalta.com URL which allows Access to all the PKI policies in English. Https protocol ETSI EN 319 412-5		YES
	QcLimitValue	SIGNATURE / AUTHENTICATION	Limit amount of liability assumed by the issuer expressed in EUROS		YES
	QcRetentionPeriod	SIGNATURE / AUTHENTICATION	Integer: =15 ([ETSI EN 319 412-5] Describes the conservation period of all information, relevant to the use of a certificate, after its expiration)		YES
	semnaticsId-Natural	SIGNATURE / AUTHENTICATION	To indicate the semantics of a natural person defined by the EN 319 412-1		
PolicyIdentifier		(AUTHENTICATION)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.2.5.1.1		YES
		(SIGNATURE)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.2.5.1.3		
		(ENCRYPTION)	[1] Certificates policy:		

Certificate Policies			Policy identifier =1.3.6.1.4.1.18339.2.5.1.2			
	PolicyIdentifier		(AUTHENTICATION)	2.16.724.1.3.5.8	YES	
			(SIGNATURE)	2.16.724.1.3.5.8		
	PolicyCPSLocation	[1,1] Policy certifier information: Policy certifier ID =CPS Certifier: http://www.anfacmalta.com				
	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.				YES
PolicyIdentifier	ONLY FOR SIGNATURE TYPE	HSM TOKEN	qcp-natural-qscd (0.4.0.194112.1.2)			
		SOFTWARE TOKEN	qcp-natural (0.4.0.194112.1.0)			
Fields conditioned by the use of the certificate	BusinessCategory	PrivateOrganization				
		GovernmentEntity				
		BusinessEntity				
		Non-commercialEntity				
	JurisdictionOfIncorporationLocalityName	Locality				
	JurisdictionOfIncorporationStateOrProvinceName	Province				
JurisdictionOfIncorporationCountryName	Country					
Basic Constraints	Type of matter =End entity Route Length Restriction =None CA = FALSE			YES		
Key usage	Certificate Type: SIGNATURE	Non-repudiation (c0)			YES	
	Certificate Type: AUTHENTICATION	Electronic signature, Non-repudiation (c0)				
	Certificate Type: ENCRYPTION	KeyEncipherment, dataEncipherment				
Extended key usage	Signature / Authentication	1.3.6.1.5.5.7.3.2	Client Authentication			YES
		1.3.6.1.5.5.7.3.4	Secure mail			



Identification algorithm	sha1		YES
Signature Value			YES
Digital Fingerprint			YES
Descriptive Name	<i>Automatically completed by AR Manager</i>		

