

Certificate Policy for Natural Person Class 2 Certificates. 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



Natural Person Class 2 Certificate

(AUTHENTICATION) (SIGNATURE) (ENCRYPTION)
TOKEN BY SOFTWARE - HSM TOKEN

Field	Value		Crit	Mandatory
Version	2 = (V3)			YES
Serial number				YES
SignatureAlgorithm	sha256WithRSAEncryption			YES
SignatureHashAlgorithm	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
Issuer Alternative Name				
Valid from NotBefore				YES
Valid until NotAfter				YES
Subject	<i>Subject</i>			
	1.3.6.1.4.1.18838.1.1	<i>Subject's country = subscriber</i>		YES
	Country (C)	<i>Subject's city</i>		YES
	Locality (L)	<i>Subject's state</i>		YES
	State (ST)	<i>Subject's Email</i>		YES



Subject <i>(all fields encoded using UTF-8)</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>			YES	
	OrganizationIdentifier	<i>Name of subject, according to identity document (National/Foreign Citizens ID Card / Passport)</i>				
	Given Name (G)	<i>Surname(s) of the subject. 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>			YES	
	SurName (SN)	<i>Full name + Subject's National/Foreign Citizen ID Card</i>			YES	
	Common Name (CN)	<i>Subject's country = subscriber</i>			YES	
	Organisational Unit (OU)	AUTHENTICATION	<i>Certificate for Natural Person Class 2 (AUTHENTICATION)</i>			YES
		SIGNATURE	<i>Certificate for Natural Person Class 2 (SIGNATURE)</i>			
		ENCRYPTION	<i>Certificate for Natural Person Class 2 (ENCRYPTION)</i>			
	Organisation (O)	<i>E.g.: O = College Name / collegiate number. In the case of professional training: may include the name of the association, guild or grouping to which it belongs. Or issuer of professional training degree. In addition, the number of associate or member may be included as specified in the previous assumption. In case of freelances, may include: Registered trade name or Trademark of the subject.</i>				
Title (T)	<i>Subject's title</i>					
Description						
SubjectAlternativeName	Subject alternative name - 2.5.29.17					
	<i>email e.g.: peter@cial.com</i>					
	DNSName Directory Name				YES	
	1.3.6.1.4.1.18339.11	<i>Full name of a natural or legal person, who grants a representation to the subscriber</i>				
	1.3.6.1.4.1.18339.12	<i>First name of the natural person granting a representation to the subscriber</i>				
	1.3.6.1.4.1.18339.13	<i>Surnames of the natural person granting a representation to the subscriber</i>				
	1.3.6.1.4.1.18339.14	<i>VAT number / National / Foreign Citizens ID Card of the legal entity or natural person that grants a representation to the subscriber</i>				

	1.3.6.1.4.1.18339.20.3	Subscriber's name		
	1.3.6.1.4.1.18339.20.4	Subscriber's Surname 1		
	1.3.6.1.4.1.18339.20.5	Subscriber's Surname 2		
	1.3.6.1.4.1.18339.20.8	e.g.: National / Foreign Citizen ID Card		
	1.3.6.1.4.1.18339.20.13	e.g.: Maltese		
	<i>SubjectDirectoryAttributes – 2.5.29.9</i>			
	2.5.4.20	TelephoneNumber		
	2.5.4.23	Facsimile		
	2.5.4.9	StreetAddress		
	2.5.4.16	PostalAddress		
	2.5.4.17	PostalCode		
	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://www.anfacmalta.com/app/ + (RA locator =OID1.3.6.1.4.1.18339.19)		
	2.5.4.2	knowledgeinformation		
	2.5.4.65	Pseudonym (chosen by the subscriber)		
	1.3.6.1.4.1.18339.30.1	Full name of the country to which the issuance corresponds		
SubjectDirectoryAttributes	1.3.6.1.4.1.18339.40.1	e.g. Qualified certificate		
	1.3.6.1.4.1.18339.41.1	1000		
	1.3.6.1.4.1.18339.41.2	e.g. Purchase contracts signing		
	1.3.6.1.4.1.18339.41.3	e.g. 10.000		
	1.3.6.1.4.1.18339.41.4	e.g. euros		
	1.3.6.1.4.1.18339.42.1			
	1.3.6.1.4.1.18339.42.11	It is filled in automatically by AR Manager		
	1.3.6.1.4.1.18339.42.13	It is filled in automatically by AR Manager		
	1.3.6.1.4.1.18339.47.1	It is filled in automatically by AR Manager		
	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				
1.3.6.1.4.1.18339.600		<i>e.g.: AR Manager desktop v.3.6+Critical+ANF CT</i>		
2.5.4.15	BusinessCategory	PrivateOrganization	PrivateOrganization	
			GovernmentEntity	
			BusinessEntity	
			Non-commercialEntity	
	JurisdictionOfIncorporationLocalityName	Locality		
1.3.6.1.4.1.3 11.60.2.1.2	JurisdictionOfIncorporationStateOrProvinceName	Province		
1.3.6.1.4.1.3 11.60.2.1.3	JurisdictionOfIncorporationCountryName	Country		



1.3.6.1.4.1.18339.19	e.g. 33993893-503677			
1.3.6.1.4.1.18339.19.1	e.g. 26144-56501328 3643648640			
Subject Key Identifier	Hash in SHA1 of the public key used for signing the certificate			YES
SubjectPublic KeyInfo	RSA (2048) NIST P-256			YES
Access to issuer entity information	AccessMethod [1]	[1] Access to authority information Access method = On line certificate status protocol (1.3.6.1.5.5.7.48.1)		YES
	AccessLocation [1]	Alternative name: URL address =http://		YES
	AccessMethod [2]	1.3.6.1.5.5.7.48.2		
	AccessLocation [2]	URL address=		
CRL distribution points	cRLDistributionPoint [1]	[1] CRL distribution point Distribution point name: Full name: URL address		YES
	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 type SIGNATURE	ONLY if the device is SS CD 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	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	YES

			<i>of all information, relevant to the use of a certificate, after its expiration)</i>			
	semanticsId-Natural	SIGNATURE / AUTHENTICATION	To indicate the semantics of a natural person defined by the EN 319 412-1			
Certificate Policies	PolicyIdentifier	(AUTHENTICATION)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.3.4.1.1.22		YES	
		(SIGNATURE)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.3.4.1.2.22			
		(ENCRYPTION)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.3.4.1.3.22			
	PolicyCPSLocation	[1,1] Policy certifier information: Policy certifier ID =CPS Certifier: http://www.anfacmalta.com			YES	
	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 check integrity, limitations, validity, and authorized uses.			YES	
	PolicyIdentifier	ONLY FOR AUTHENTICATION TYPE AND ONLY FOR HSM DEVICE	0.4.0.2042.1.2	NCP+ (Normalized Certificate Policy requiring a secure user device)		
	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)			
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	Digital 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>It is filled in automatically by AR Manager</i>				