Certification Policy of Issuance Reports Manager and PKI Operator Certificates. Certificate Profile

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

Issuance Reports Manager and PKI Operator Certificates

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

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

Subject *(all fields encoded using UTF-8)*	*Subject*				
	1.3.6.1.4.1.18838.1.1	*Subject's National / Foreign Citizen ID Card*			YES
	Country (C)	*Subject's country = subscriber*			YES
	Locality (L)	*Subject's city*			YES
	State (ST)	*Subject's state*			YES
	EmailAddress (E)	*Subject's Email*			
	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*			YES
	OrganizationIdentifier	*The certificate must include at least= Serial Number or OrganizationIdentifier (VAT number), e.g.* *VATMT-00000000*			
	Given Name (G)	*Name of subject, according to identity document (National/Foreign Citizens ID Card / Passport)*			YES
	SurName (SN)	*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*			YES
	Common Name (CN)	*Full name + Subject's National/Foreign Citizen ID Card*			YES
	Organisational Unit (OU)	**AUTHENTICATION**	*Issuance Reports Manager Certificate (AUTENTICATION)*		YES
		SIGNATURE	*Issuance Reports Manager Certificate (SIGNATURE)*		
		ENCRYPTION	*Issuance Reports Manager Certificate (ENCRYPTION)*		
		AUTHENTICATION	*PKI Operator Certificate* *(AUTHENTICATION)*		
		SIGNATURE	*PKI Operator Certificate* *(SIGNATURE)*		
		ENCRYPTION	*PKI Operator Certificate* *(ENCRYPTION)*		
	Organisation (O)	*e.g.: O = ANF Autoridad de Certificación*			
	Title (T)	*e.g. lawyer*			
	Description				
	SubjectAlternativeName - 2.5.29.17				
	email e.g.: peter@cial.com				YES

SubjectAlternativeName	*DNSName* *Directory Name*			
	1.3.6.1.4.1.18339.11	*Full name of a natural or legal person, who grants a representation to the subscriber*		
	1.3.6.1.4.1.18339.12	*First name of the natural person granting a representation to the subscriber*		
	1.3.6.1.4.1.18339.13	*Surnames of the natural person granting a representation to the subscriber*		
	1.3.6.1.4.1.18339.14	*VAT number* / National / Foreign Citizens ID Card *of the legal entity or natural person that grants a representation to the subscriber*		
	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*		
SubjectDirectoryAttributes	*SubjectDirectoryAttributes – 2.5.29.9*			
	2.5.4.13	*Description*		
	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	*knowldgeinformation*		
	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*		
	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	*e.g. QRM - 345*		

	1.3.6.1.4.1.18339.42.2	Level 1 Recognized Registration Authority			
	1.3.6.1.4.1.18339.42.3	Issuance Reports Manager			
	1.3.6.1.4.1.18339.42.4	Level 2 Recognized Registration Authority			
	1.3.6.1.4.1.18339.42.8	*e.g. 1*			
	1.3.6.1.4.1.18339.42.9	Authorized PKI Operator			
	1.3.6.1.4.1.18339.42.11	*e.g. Consultancy Harbinger*			
	1.3.6.1.4.1.18339.42.13	*e.g. legal department*			
	1.3.6.1.4.1.18339.47.1	*e.g.= 8&1EB4F96F*			
	1.3.6.1.4.1.18339.47.3	*HSM Token Model*			
	1.3.6.1.4.1.18339.600	*e.g.: AR Manager desktop v.3.6*			
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]				
	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 SSCD*** Secure Signature Creation Device (SSCD)		YES

Qualified Certificate Statement TSI EN 319 412-1, antes ETSI TS 101 862					
	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* *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		
Certificate Policies	PolicyIdentifier	**IRM Certificate (AUTHENTICATION)**	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.23.1.1.22		YES
		IRM Certificate (SIGNATURE)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.23.1.4.22		
		IRM Certificate (ENCRYPTION)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.23.1.3.22		
		PKI Operator Certificate (AUTHENTICATION)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.23.1.2.22		
		PKI Operator Certificate (SIGNATURE)	[1] Certificates policy: Policy		

				identifier =1.3.6.1.4.1.18339.23.1.6.22		
			PKI Operator Certificate **(ENCRYPTION)**	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18339.23.1.5.22		
	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 with 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) KeyEncipherment, dataEncipherment		**YES**	
	Certificate type: **AUTHENTICATION**		Electronic signature, Non-repudiation (c0) KeyEncipherment, dataEncipherment			
	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