Certificate for Secure Server (OV), Secure Server (DV), Secure Server (EV), Electronic Headquarters and Extended Validation Electronic Headquarters Certificates (EV Headquarters).

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

Certificate for Secure Server (OV), Secure Server (DV), Secure Server (EV), Electronic Headquarters and Extended Validation Electronic Headquarters Certificates (EV Headquarters)

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)	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)	*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	Province 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 the key identified in keyIdentifier corresponds		
AuthorityCertSerialNumber				(Integer)	Issuer	Serial number of the CA certificate		
Identifier of the issuer entity key - *Authority*	2.5.29.35	Hash with SHA1 of the public key used for signing the certificate		RFC 5280 (String UTF8)	Issuer	Identifier derived from using the hash function on the subject's public key. It is a mean to identify the public		YES

KeyIdentifier						key corresponding to the private key used to sign a certificate		
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 state*		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 certificate subscriber Preferably the semantics proposed by the standard ETSI EN 319 412-1 will be used		YES
	2.5.4.97	OrganisationIdentifier	*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 ID Card, it is the VAT number for the EU		
	2.5.4.10	OrganisationName (O)	*e.g. Company name. LTD.*	*(String UTF8) Size [RFC 5280] 128* *ETSI EN 319 412-1 [i.4], clause 5*	AR manager	Name ("official" name of the organization) of the subscriber		YES
	2.5.4.42	Given Name (G)	*Name of legal representative, according to identification document (National/Foreign Citizen ID Card / Passport)*	*(String UTF8) Size 40.* *Mandatory according to ETSI EN 319 412-2*	AR manager	Name of the legal representative (as it appears on his/her National/Foreign Citizens ID Card / Passport).		YES
	2.5.4.4	SurName (SN)	*Surname(s) of the legal representative.*	*(String UTF8) Size 80.* *Mandatory according to*	AR manager	Surname(s) of the legal representative (as it appears on his/her National/Foreign Citizens		YES

			First surname, blank space, second surname of the person responsible for the certificate in accordance with the National ID Card or in *case of foreigner the passport*	*ETSI EN 319 412-2*		ID Card / Passport).			
2.5.4.3	Common Name (CN)		*e.g. anfacmalta.com*	*(String UTF8) Size 132 [RFC 5280]*	AR manager	Domain (DNS) where the certificate will reside.			YES
2.5.4.11	Organisational Unit (OU)		**DV SSL**	*Certificate for DV Secure Server SSL*	String UTF8) Size [RFC 5280] 128	AR Manager	Description of certificate type		YES
			OV SSL	*Certificate for OV Secure Server SSL*					
			EV SSL	*Certificate for EV Secure Server SSL*					
			Medium Level Headquarters	*Certificate for Medium Level Electronic Headquarter*					
			Medium Level EV Headquarters	*Certificate for Medium Level EV Electronic Headquarter*					
			High Level Headquarters	*Certificate for High Level Electronic Headquarter*	Public Administration Profile	ANF CT	Only if the device is HSM		YES
			High Level EV Headquarters	*Certificate for High Level EV Electronic Headquarter*	Public Administration Profile	ANF CT	Only if the device is HSM		YES
2.5.4.11	Organizational Unit (OU)		**Certificate for ELECTRONIC HEADQUARTER**	*e.g.: GENERAL ACCESS POINT*	Public Administration Profile	AR manager	The descriptive name of the headquarter.		
2.5.4.15	businessCategory		PrivateOrganization	*for private organization*	*CAB FORUM*	AR manager	Category of organization (required for EV certificates)		YES
			GovernmentEntity	*for public entity*					
			BusinessEntity	*for company*					
			Non-commercialEntity	*for non-commercial entity*					
1.3.6.1.4.1.311.60.2.1.3	JurisdictionCountryName		EV certificates only	*e.g. MT*	*CAB FORUM*	AR manager	Jurisdiction (required for EV certificates)		YES
1.3.6.1.4.1.3	JurisdictionOfIncorporationL		EV certificates	*e.g. Valletta*					

	11.60.2.1.1	ocalityName	only						
	1.3.6.1.4.1.3 11.60.2.1.2	JurisdictionOfIncorporationStateOrProvinceName	EV certificates only	*e.g. Valletta*					
Subject alternative name – SubjectAlternativeName See NOTE 2	Subject alternative name – SubjectAlternativeName - 2.5.29.17								
	eMail e.g: peter@cial.com			*Nombre RFC822* *(String) Size [RFC 5280] 255*	ANF CT	Email of the person responsible for the certificate			YES
	DNSName *Directory Name*	*e.g. anfacmalta.com* *frater.com*		*(String UTF8) Size = 128*	AR manage	Domain Name DNS **It may contain multiple domains**			
Subject Key Identifier	2.5.29.14	Hash in SHA1 of the public key used for signing the certificate		*RFC 5280* *In accordance with standards RFC2459 & PKCS#1*	Issuer	Identifier derived from using the hash function on the subject public key.			YES
SubjectPublicKeyInfo		RSA (2048)		*(String UTF8)* *RSA. In accordance with the RFC 4055 [1 0] 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	1.3.6.1.5.5.7.1.1	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-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 :* *Complete name in http protocol:* *URL Address*		*Issuer*	Indicates the CRL download point.			YES
Qualified Certificate	1.3.6.1.5.5.7.1.3	0.4.0.1862.1.1	QcCompliance	**ONLY EV**	***Present** if the certificate is issued with the consideration of qualified. Annex I*	ANF CT	**qcStatements** in accordance with		YES

Statement TSI EN 319 412-1, before ETSI TS 101 862					*eIDAS*		ETSI EN 319 412-5		
		0.4.0.1862.1.4	**QcSSCD**	**ONLY EV with HSM**	***ONLY if the device is SSCD*** Secure Signature Creation Device (SSCD)	ANF CT	*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 [I.8]*		YES
		0.4.0.1862.1.6.3	QcType-web	**ONLY EV** *QcType 3*	*QcType 3 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	**ONLY EV**	*https://anfacmalta.com* *URL that allows access to all policies of the PKI in English. Https protocol* *ETSI EN 319 412-5*	ANF CT	Not included in ENCRYPTION type		YES
		0.4.0.1862.1.2	QcLimitValue	**ONLY EV**	*Responsibility limit amount assumed by the issuer expressed in EUROS*	ANF CT	<QcLimitValue> <money>EUR</money> <qcBase>1</qcBase> <qcExp>3</qcExp> </QcLimitValue> Not included in ENCRYPTION type		YES
		0.4.0.1862.1.3	QcRetentionPeriod	**ONLY EV**	*Integer: =15* *([ETSI EN 319 412-5]* *describes the conservation period of all information relevant to the use of a certificate, after its*	ANF CT	Not included in ENCRYPTION type		YES

					expiration)				
		0.4.0.194121.1.2	semnaticsId-Legal	**ONLY EV**	To indicate the semantics of a natural person defined by EN 319 412-1	AR Manager	To indicate the semantics of a legal person defined by EN 319 412-1		
Certificate Policies	2.5.29.32	PolicyIdentifier	**DV SSL**		[1] Certificates policy: Policy identifier= 1.3.6.1.4.1.18339.55.1.1.22	AR Manager	ANF AC proprietary OID		YES
			OV SSL		[1] Certificates directive: Policy identifier= 1.3.6.1.4.1.18339.55.1.7.22				
			EV SSL		[1] Certificates directive: Policy identifier= 1.3.6.1.4.1.18339.55.1.2.22				
			Medium Level Electronic Headquarter		[1] Certificates directive: Policy identifier= 1.3.6.1.4.1.18339.55.1.1.3.22				
			Medium Level EV Electronic Headquarter		[1] Certificates directive: Policy identifier= 1.3.6.1.4.1.18339.55.1.1.5.22				
			High Level Electronic Headquarter		[1] Certificates directive: Policy identifier= 1.3.6.1.4.1.18339.55.1.1.4.22				
			High Level EV Electronic Headquarter		[1] Certificates directive: Policy identifier= 1.3.6.1.4.1.18339.55.1.1.6.22				
		PolicyIdentifier	**DV SSL**		2.23.140.1.2.1	AR Manager	CA/B FORUM and Public Administration profile		YES
			OV SSL		2.23.140.1.2.2				
			EV SSL		2.23.140.1.1				
			If the subscriber is a natural person		2.23.140.1.2.3				
			HIGH LEVEL Electronic headquarter		2.16.724.1.3.5.5.1				
			MEDIUM LEVEL Electronic headquarter		2.16.724.1.3.5.5.2				
		PolicyIdentifier	**DV SSL**		0.4.0.2042.1.6	AR Manager	Standard ETSI TS 102 042 and ETSI 101 456		YES
			OV SSL		0.4.0.2042.1.7				
			EV SSL		0.4.0.2042.1.4				
			EV Headquarter		0.4.0.2042.1.4				
			Issued as qualified + HSM		0.4.0.1456.1.1				
		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 check 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	**EV SSL** **EV Headquarter**	0.4.0.194112.1.4 (qcp-web)	AR Manager	All certificates are issued as qualified. Web site qualified certificate according to Regulation EU 910/2014		YES
Basic Constraints	2.5.29.19	Matter type = 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	Used when the authentication function is performed		AR manager		**YES**	
		Key Encipherment	Used for management and transport of keys					
Extended key usage	2.5.29.37	Server authentication	web Server TSL authentication 1.3.6.1.5.5.7.3.1		AR manager			YES
		Client authentication	web Client TSL authentication 1.3.6.1.5.5.7.3.2					
Identification algorithm		sha1			Issuer			YES
Signature Value					Issuer	Signature encoded as bit string		YES
Digital fingerprint					Issuer	Certificate digital fingerprint		YES