Certification Policy for

RA Operators Certificates. Certificate Profile

Paseo de la Castellana, 79 – 28046 - Madrid (Spain)
Teléfono: 902 902 172 (Calls from Spain)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es/en

Security Level

Public Document

Important Notice

Address: Paseo de la Castellana, 79 - 28046 - Madrid (Spain)

Telephone: 902 902 172 (calls from Spain) International (+34) 933 935 946

Fax: (+34) 933 031 611. Web: www.anf.es/en

RA Operator 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)	*e.g. ANF Assured ID CA1*		YES
	SERIALNUMBER	G63287510		YES
	Organisation Identifier	*This is the VAT number.* *At present ANF AC does not include it*		
	EmailAddress (E)	info@anf.es		
	Organisational Unit (OU)	Organizational unit within the Certification Services Provider responsible for the certificate issuance		YES
	Organisation (O)	*e.g. ANF Autoridad de Certificacion*		YES
	Locality (L)	*e.g. Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*		
	State (ST)	*e.g. Barcelona*		
	Country (C)	*e.g. ES*		YES
AuthorityCertIssuer				
AuthorityCertSerial Number				
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			

Subject *(all fields encoded using UTF-8)*	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.: IDCES-00000000G. 3 characters to indicate the document number (IDC= national identity document) + 2 characters to identify the country (ES) + ID number*			YES
	OrganizationIdentifier	*The certificate must include at least= Serial Number or OrganizationIdentifier (VAT number), e.g.* *VATES-B0085974Z*			
	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**	*RA Operator Certificate (AUTHENTICATION)*		YES
		SIGNATURE	*RA Operator Certificate (SIGNATURE)*		
		ENCRYPTION	*RA Operator Certificate (ENCRYPTION)*		
	Organisation (O)	*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.*			
	Title (T)	*Subject's title*			
	Description				
SubjectAlternativeName	SubjectAlternativeName - 2.5.29.17				
	email e.g.: pedro@cial.com				YES
	DNSName *Directory Name*				
	1.3.6.1.4.1.18332.11	*Full name of a natural or legal person, who grants a representation to the subscriber*			

	1.3.6.1.4.1.18332.12	*First name of the natural person granting a representation to the subscriber*		
	1.3.6.1.4.1.18332.13	*Surnames of the natural person granting a representation to the subscriber*		
	1.3.6.1.4.1.18332.14	*VAT number* / National / Foreign Citizens ID Card *of the legal entity or natural person that grants a representation to the subscriber*		
	1.3.6.1.4.1.18332.20.3	*Subscriber's name*		
	1.3.6.1.4.1.18332.20.4	*Subscriber's Surname 1*		
	1.3.6.1.4.1.18332.20.5	*Subscriber's Surname 2*		
	1.3.6.1.4.1.18332.20.8	*e.g.: National / Foreign Citizen ID Card*		
	1.3.6.1.4.1.18332.20.13	*e.g.: Spanish*		
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*		
	1.3.6.1.4.1.18332.10.10	*e.g.: SHA256-gsq33wq/udldyk5ZN84paMeYx*		
	1.3.6.1.4.1.18332.10.10.1	*e.g.: https://www.anf.es/app/ + (RA locator =OID1.3.6.1.4.1.18332.19)*		
	2.5.4.2	*knowldgeinformation*		
	2.5.4.65	*Pseudonym* *(chosen by the subscriber)*		
	1.3.6.1.4.1.18332.30.1	*Full name of the country to which the issuance corresponds*		
	1.3.6.1.4.1.18332.40.1	*e.g. Qualified certificate*		
	1.3.6.1.4.1.18332.41.1	*1000*		
	1.3.6.1.4.1.18332.41.2	*e.g. Purchase contracts signing*		
	1.3.6.1.4.1.18332.41.3	*e.g. 10.000*		
	1.3.6.1.4.1.18332.41.4	*e.g. euros*		
	1.3.6.1.4.1.18332.42.1	*e.g. BCN - 345*		
	1.3.6.1.4.1.18332.42.2	Level 1 Recognized Registration Authority		
	1.3.6.1.4.1.18332.42.4	Level 2 Recognized Registration Authority		
	1.3.6.1.4.1.18332.42.11	*e.g. Consultancy Harbinger*		
	1.3.6.1.4.1.18332.42.13	*e.g. legal department*		

	1.3.6.1.4.1.18332.47.1	*e.g.= 8&1EB4F96F*			
	1.3.6.1.4.1.18332.47.3	*HSM Token Model*			
	1.3.6.1.4.1.18332.600	*e.g.: AR Manager desktop v.3.6*			
1.3.6.1.4.1.18332.19	*e.g. 33993893-503677*				
1.3.6.1.4.1.18332.19.1	*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 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://anf.es/en/*		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		**(AUTHENTICATION)**	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.22.1.1.22		YES
			(SIGNATURE)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.22.1.3.22		
			(ENCRYPTION)	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.22.1.2.22		
	PolicyCPSLocation		[1,1] Policy certifier information: Policy certifier ID =CPS Certifier: http://www.anf.es/en			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 **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)		
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