ANF AUTORIDAD DE CERTIFICACIÓN

Certificate Certification Policy of Public Employee. Certificate Profile

CIF G-63287510

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

Security level

Public

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

Public Employee Certificate

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

Countryside	Value		Crit	Oblig
Version	2 = (V3)			YES
Serial number				YES
Signature algorithm. *SignatureAlgorithm*	sha256WithRSAEncryption			YES
Hash algorithm firm *SignatureHashAlgorithm*	sha256			YES
Transmitter	Common Name (CN)	*eg ANF Assured ID CA1*		YES
	SERIALNUMBER	G63287510		YES
	Organization Identifier	*It is the VAT number, in Spain called NIF-VAT it is not the CIF. It is the NIF for VAT in the EU* *Currently ANF AC does not include it*		
	EmailAddress (E)	info@anf.es		
	Organizational Unit (OU)	Organizational unit within the Certification Services Provider responsible for issuing the certificate		YES
	Organization (O)	*eg ANF Certification Authority*		YES
	Locality (L)	*eg Barcelona (see current address at http:// www.anf.es/es/address-direccion.html*		
	State (ST)	*eg Barcelona*		
	Country (C)	*pe ES*		YES
AuthorityCertIssuer				
AuthorityCertSerial Number				
Identifier of the issuing entity key *Authority KeyIdentifier*	Hash with SHA1 of the public key used to sign the certificate			YES
Issuer Alternative Yam				
Valid from				YES

NotBefore				
Valid until *NotAfter*				YES
Subject *(all fields encoded using UTF-8)*	*Subject*			
	Country (C)	*pe = ES*		YES
	Locality (L)	*Subject's city*		YES
	State (ST)	*Subject province*		YES
	EmailAddress (E)	*Subject's email*		
	SERIAL NUMBER (SN)	*For instance* *p. eg: IDCES-00000000G. 3 characters to indicate the document number (IDC = national identity document) + 2 characters to identify the country (ES) + Identity number*		YES
	OrganizationIdentifier	*The certificate must include at least = Serial Number or OrganizationIdentifier (NIF-VAT), eg* *VATES-B0085974Z*		
	Given Name (G)	*p. eg: "JUAN ANTONIO"*		YES
	SurName (SN)	*p. ex .: "DE LA CAMARA ESPAÑOL - DNI 00000000G*		YES
	Common Name (CN)	*ex .: JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G*		YES
	Organizational Unit (OU)	High Level Public Employee Certificate **(AUTHENTICATION)**		YES
		High Level Public Employee Certificate (**FIRM)**		
		High Level Public Employee Certificate (**ENCRYPTED)**		
		Public Employee Certificate Medium Level		
		p. e.g .: GENERAL SUBDIRECTION OF DATA PROCESSING		
		OU = p. ex .: E04976701		
		Certificate subscriber identification number (supposedly unique). It corresponds to the NRP or PIN. *See NOTE 3*		
	Organization (O)	*p. eg: MINISTRY OF DEVELOPMENT.*		

	Title (T)		*p. eg: PROGRAMMER ANALYST. Descriptive name of the position or position held by the person responsible for the certificate*		
Alternative name of the subject - SubjectAlternativeName	*Alternative name of the subject*		- 2.5.29.17		
	e-mail example: pedro@cial.com				YES
	DNSName *Directory Name*				
	High level	2.16.724.1.3.5.7.1.1	*High Level Public Employee Certificate (AUTHENTICATION)*		YES
			High Level Public Employee Certificate (SIGNATURE)		
			High Level Public Employee Certificate (CIFRADO)		
	Medium level	2.16.724.1.3.5.7.2.1	*Public Employee Certificate Medium Level*		
	High level	2.16.724.1.3.5.7.1.2	*p. eg: MINISTRY OF DEVELOPMENT*		YES
	Medium level	2.16.724.1.3.5.7.2.2			
	High level	2.16.724.1.3.5.7.1.3	*p. eg: S2833002*		YES
	Medium level	2.16.724.1.3.5.7.2.3			
	High level	2.16.724.1.3.5.7.1.4	*p. eg: 00000000G*		YES
	Medium level	2.16.724.1.3.5.7.2.4			
	High level	2.16.724.1.3.5.7.1.5	*p. eg: A02APE1056*		YES
	Medium level	2.16.724.1.3.5.7.2.5			
	High level	2.16.724.1.3.5.7.1.6	*Ex .: "JUAN ANTONIO"*		YES
	Medium level	2.16.724.1.3.5.7.2.6			
	High level	2.16.724.1.3.5.7.1.7	*Ex .: "FROM THE CAMERA"*		YES
	Medium level	2.16.724.1.3.5.7.2.7			
	High level	2.16.724.1.3.5.7.1.8	*Ex .: "SPANISH"*		YES
	Medium level	2.16.724.1.3.5.7.2.8			

	High level	2.16.724.1.3.5.7.1.9	*E.g.: juanantonio.delacamara.espanol@mfom.es*		YES
	Medium level	2.16.724.1.3.5.7.2.9			
	High level	2.16.724.1.3.5.7.1.10	*p. e.g .: GENERAL SUBDIRECTION OF DATA PROCESSING*		YES
	Medium level	2.16.724.1.3.5.7.2.10			
	High level	2.16.724.1.3.5.7.1.11	*p. e.g .: PROGRAMMER ANALYST (*		YES
	Medium level	2.16.724.1.3.5.7.2.11			
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		*Example: SHA256-gsq33wq / udldyk5ZN84paMeYx*		
	1.3.6.1.4.1.18332.10.10.1		*Example: https://www.anf.es/app/ + (AR locator = OID1.3.6.1.4.1.18332.19)*		
	2.5.4.2		*knowldgeinformation*		
	2.5.4.65		*Pseudonym –Pseudonym* *(chosen by the subscriber)*		
	1.3.6.1.4.1.18332.30.1		*Full name of the country to which the issue corresponds*		
	1.3.6.1.4.1.18332.40.1		*pe Recognized certificate*		
	1.3.6.1.4.1.18332.42.1				
	1.3.6.1.4.1.18332.42.11				
	1.3.6.1.4.1.18332.42.13				
	1.3.6.1.4.1.18332.47.1		*Example = 8 & 1EB4F96F*		
	1.3.6.1.4.1.18332.47.3		*HSM token model*		
	1.3.6.1.4.1.18332.600		*Example: AR Manager desktop v.3.6*		
1.3.6.1.4.1.18332.19	*Example 33993893-503677*				
1.3.6.1.4.1.18332.19.1	*Example 26144-56501328 3643648640*				

Identifier of the subject key - Subject Key Identifier	Hash in SHA1 of the public key used to sign the certificate				YES
SubjectPublic KeyInfo	RSA (2048) NIST P-256				YES
Access to the information of issuing entity	AccessMethod [1]	*[1] Access to authority information* *Access method = Certificate Status Protocol* *online (1.3.6.1.5.5.7.48.1)*			YES
	AccessLocation [1]	*Alternative name: URL = http: //*			YES
	AccessMethod [2]	*1.3.6.1.5.5.7.48.2*			
	AccessLocation [2]	*URL =*			
Points of CRL distribution	cRLDistributionPoint [1]	*[1] CRL distribution point* *Distribution point name:* *Full name:* *Url address*			YES
	DistributionPoint [2]				
	DistributionPoint [3]				
Declarations of certificates recognized *Qualified Certificate Statement*	QcCompliance	**Signature of** **(HIGH LEVEL) and** **(MEDIUM LEVEL)**	***Present** if the certificate is issued with the qualification of recognized. Annex I eIDAS*		YES
	QcSSCD	**ONLY included in the type** **High level (FIRM)**	***ONLY if the device is SSCD*** Secure Signature Creation Device (SSCD)		YES
	QcType- esign	**Signature of** **(HIGH LEVEL) and** **(MEDIUM LEVEL)** *QcType 1*	*QcType 1 reviewed* *ETSI EN 319 412-5*		YES
	QcPDS	**FIRM -** **(HIGH LEVEL)** **(MEDIUM LEVEL)**	https://anf.es/en/ *URL that allows access to all PKI policies in English. Https protocol*		YES

TSI EN 319 412-1, formerly ETSI TS 101 862				*ETSI EN 319 412-5*		
	QcLimitValue		**Signature of (HIGH LEVEL) and (MEDIUM LEVEL)**	*Limit amount of liability assumed by the issuer expressed in EUROS*		YES
	QcEuRetentionPeriod		**Signature of (HIGH LEVEL) and (MEDIUM LEVEL)**	*Integer: = 15 ([ETSI EN 319 412-5] describes the retention period of all the relevant information for the use of a certificate, after the expiration of this)*		YES
	semnaticsId-Natural		**Signature of (HIGH LEVEL) and (MEDIUM LEVEL)**	To indicate natural person semantics defined by EN 319 412-1		
Directives of the certificate - *Certificate Policies*	PolicyIdentifier	**High level**	**(AUTHENTICATION)**	[1] Certificate Directive: Identifier of directive = 1.3.6.1.4.1.18332.4.1.1.22		YES
		High level	**(FIRM)**	[1] Certificate Directive: Identifier of directive = 1.3.6.1.4.1.18332.4.1.3.22		
		High level	**(ENCRYPTED)**	[1] Certificate Directive: Identifier of directive = 1.3.6.1.4.1.18332.4.1.4.22		
		Medium level		[1] Certificate Directive: Identifier of directive = 1.3.6.1.4.1.18332.4.1.2.22		YES
	PolicyIdentifier	High level	[2] Certificate Directive: Identifier of directive = 2.16.724.1.3.5.7.1			YES
		Medium level	[2] Certificate Directive: Identifier of directive = 2.16.724.1.3.5.7.2			YES
	PolicyCPSLocation		[1,1] Policy certifier information: Policy certifier ID = CPS Certifier:			YES

			http://www.anf.es/documentos			
	User notice		[1,2] Policy certifier information: Policy certifier ID = User Warning Certifier: Notice text = Certificate in accordance with the electronic signature legislation. Before accepting it, check its integrity, limitations, validity and authorized uses.			YES
	PolicyIdentifier	ONLY FOR KIND **AUTHENTICTION** AND ONLY FOR **DEVICE Or HSM**	0.4.0.2042.1.2	NCP + (Normalized Certificate Policy requiring a secure user device)		
	PolicyIdentifier	**ONLY FOR SIGNATURE TYPE / AUTHENTICTION**	TOKEN HSM	qcp-natural-qscd (0.4.0.194112.1.2)		
			TOKEN SOFTWARE	qcp-natural (0.4.0.194112.1.0)		
Fields conditioned by the use of certificate	BusinessCategory			PrivateOrganization		
				GovernmentEntity		
				BusinessEntity		
				Non-commercialEntity		
	JurisdictionOfIncorporationLocalityName			Location		
	JurisdictionOfIncorporationStateOrProvinceName			Province		
	JurisdictionOfIncorporationCountryName			Country		
Restrictions basic *Basic Constraints*	Type of matter = End entity Path length restriction = None CA = FALSE				**YES**	
Key usage *Key usage*	*(HIGH LEVEL)* FIRM			No repudiation (c0)	**YES**	
	(HIGH LEVEL) AUTHENTICATION			Digital signature		
				KeyEncipherment		
				dataEncipherment		
	(HIGH LEVEL) Encryption			KeyEncipherment,		
				dataEncipherment		
	Medium level			Digital Signature		

		No repudiation (c0)			
		Key Encipherment			
		dataEncipherment			
Improved use of the keys - *Extended key usage*	(High level) **Signature / Authentication / Encryption** (Medium level)	1.3.6.1.5.5.7.3.2	Client authentication		YES
		1.3.6.1.5.5.7.3.4	Secure mail		
Algorithm ID	sha1				YES
Signature Value					YES
Fingerprint					YES