Certification Policy for Public Employees 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

Public Employee Certificate

(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 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)	Organisational unit within the Certification Services Provider responsible for issuing the certificate		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				
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				YES

NotAfter				
Subject *(all fields encoded using UTF-8)*	*Subject*			
	Country (C)	*e.g. = ES*		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-VAT), e.g.* *VATES-B0085974Z*		
	Given Name (G)	*e.g.: "JUAN ANTONIO"*		YES
	SurName (SN)	*e.g.: "DE LA CAMARA ESPAÑOL - National / Foreign Citizen ID Card 00000000G*		YES
	Common Name (CN)	*e.g.: JUAN ANTONIO DE LA CAMARA ESPAÑOL - National (DN) ID Card 00000000G*		YES
	Organisational Unit (OU)	Certificate for Public Employee High Level **(AUTHENTICATION)**		YES
		Certificate for Public Employee High Level **(SIGNATURE)**		
		Certificate for Public Employee High Level (**ENCRYPTION)**		
		Certificate for Public Employee Medium Level		
		e.g.: DATA PROCESSING GENERAL SUBDIRECTION		
		OU = e.g.: E04976701		
		*Certificate subscriber identification number (*Supposedly *univocal). Corresponds to the* PRN *or PIN.*		
	Organisation (O)	*e.g.: MINISTRY OF PUBLIC WORKS AND TRANSPORT.*		
	Title (T)	*e.g.: PROGRAMMER ANALYST. Descriptive name of the position or post held by the person responsible for the certificate*		
	SubjectAlternativeName - 2.5.29.17			
	email e.g.: pedro@cial.com			YES

SubjectAlternativeName	*DNSName* *Directory Name*				
	HIGH level	2.16.724.1.3.5.7.1.1	*High Level Public Employee Certificate (AUTHENTICATION)* *High Level Public Employee Certificate (SIGNATURE)* *High Level Public Employee Certificate (ENCRYPTION)*		YES
	MEDIUM level	2.16.724.1.3.5.7.2.1	*Medium Level Public Employee Certificate*		
	HIGH level	2.16.724.1.3.5.7.1.2	*e.g.: MINISTRY OF PUBLIC WORKS AND TRANSPORT*		YES
	MEDIUM level	2.16.724.1.3.5.7.2.2			
	HIGH level	2.16.724.1.3.5.7.1.3	*e.g.: S2833002*		YES
	MEDIUM level	2.16.724.1.3.5.7.2.3			
	HIGH level	2.16.724.1.3.5.7.1.4	*e.g.: 00000000G*		YES
	MEDIUM level	2.16.724.1.3.5.7.2.4			
	HIGH level	2.16.724.1.3.5.7.1.5	*e.g.: A02APE1056*		YES
	MEDIUM level	2.16.724.1.3.5.7.2.5			
	HIGH level	2.16.724.1.3.5.7.1.6	*e.g.: "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	*e.g.: "DE LA CAMARA"*		YES
	MEDIUM level	2.16.724.1.3.5.7.2.7			
	HIGH level	2.16.724.1.3.5.7.1.8	*e.g.: "ESPAÑOL"*		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	*e.g.: DATA PROCESSING GENERAL SUBDIRECTION*		YES

	MEDIUM level	2.16.724.1.3.5.7.2.10			
	HIGH level	2.16.724.1.3.5.7.1.11	*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	*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*			
	1.3.6.1.4.1.18332.42.1				
	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	*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 to sign the certificate				YES
SubjectPublic KeyInfo	RSA (2048)				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	**(HIGH LEVEL) and** **(MEDIUM LEVEL) SIGNATURE**	***Present*** *if the certificate is issued with the recognized qualification. Annex I eIDAS*		YES
	QcSSCD	**It is ONLY included in the High-level type (SIGNATURE)**	***ONLY if the device is SSCD*** Secure Signature Creation Device (SSCD)		YES
	QcType- esign	**(HIGH LEVEL) and** **(MEDIUM LEVEL) SIGNATURE** *QcType 1*	*QcType 1 is outlined* *ETSI EN 319 412-5*		Y YES
	QcPDS	**(HIGH LEVEL) and** **(MEDIUM LEVEL) SIGNATURE**	*https://anf.es/en/* *URL that allows access to all policies of the PKI in English.* *Https protocol* *ETSI EN 319 412-5*		YES
	QcLimitValue	**(HIGH LEVEL) and** **(MEDIUM LEVEL) SIGNATURE**	*Limit amount of liability assumed by the issuer expressed in EUROS*		YES
	QcEuRetentionPeriod	**(HIGH LEVEL) and** **(MEDIUM LEVEL) SIGNATURE**	*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		**(HIGH LEVEL) and (MEDIUM LEVEL) SIGNATURE**	To indicate the semantics of a natural person defined by the EN 319 412-1		
Certificate Policies	PolicyIdentifier	**HIGH Level**	**(AUTHENTICATIO)**	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.4.1.1.22		YES
		HIGH Level	**(SIGNATURE)**	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.4.1.3.22		
		HIGH Level	**(ENCRYPTION)**	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.4.1.4.22		
		MEDIUM Level		[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.4.1.2.22		YES
	PolicyIdentifier	HIGH Level	[2] Certificates policy: Policy identifier =2.16.724.1.3.5.7.1			YES
		MEDIUM Level	[2] Certificates policy: Policy identifier =2.16.724.1.3.5.7.2			YES
	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 to electronic signature legislation. Before accepting it check integrity, limitations, validity, and authorized uses.			YES
	PolicyIdentifier	ONLY FOR AUTHENTICATION TYPE AND ONLY FOR	0.4.0.2042.1.2	NCP+ (Normalized Certificate Policy requiring a secure user device)		

		HSM DEVICE				
	PolicyIdentifier	**ONLY FOR SIGNATURE / AUTHENTICATION 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			País		
Basic Constraints	Type of matter = End entity Route length restriction =None CA = FALSE				**SI**	
Key usage	*(HIGH LEVEL)* **SIGNATURE**			No repudiation (c0)	**SI**	
	(HIGH LEVEL) **AUTHENTICATION**			Digital signature		
				KeyEncipherment,		
				dataEncipherment		
	(HIGH LEVEL) **ENCRYPTION**			KeyEncipherment,		
				dataEncipherment		
	MEDIUM Level			Digital Signature		
				No repudiation (c0)		
				Key Encipherment		
				dataEncipherment		
Extended key usage	(HGIH 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		
Identification algorithm	sha1						YES
Signature Value							YES
Digital fingerprint							YES