



Certificate Certification Policy

Class 2 Natural Person. Certificate Profile

CIF: G-63287510



Security level

Public

Important announcement

This document is the property of ANF Certification Authority

Its reproduction and dissemination is prohibited without the express authorization of ANF Certification Authority

Copyright © ANF Certification Authority 2016

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



Class 2 Natural Person Certificate

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

Countryside	Value		Crit	Oblig
Version	2 = (V3)			YES
Serial number				YES
Signature algorithm. <i>SignatureAlgorithm</i>	sha256WithRSAEncryption			YES
Hash algorithm firm <i>SignatureHashAlgorithm</i>	sha256			YES
Transmitter	Common Name (CN)	<i>eg ANF Assured ID CA1</i>		YES
	SERIALNUMBER	G63287510		YES
	Organization Identifier	<i>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</i>		
	EmailAddress (E)	info@anf.es		
	Organizational Unit (OU)	Organizational unit within the Certification Services Provider responsible for issuing the certificate		YES
	Organization (O)	<i>eg ANF Certification Authority</i>		YES
	Locality (L)	<i>eg Barcelona (see current address at http://www.anf.es/es/address-direccion.html)</i>		
	State (ST)	<i>eg Barcelona</i>		
Country (C)	<i>pe ES</i>		YES	
Issuer Alternative <i>Yam</i>				
Valid from <i>NotBefore</i>				YES
Valid until <i>NotAfter</i>				YES
	<i>Subject</i>			
	1.3.6.1.4.1.18838.1.1	<i>Subject ID</i>		YES
	Country (C)	<i>Country of subject = subscriber</i>		YES



Subject <i>(all fields encoded using UTF-8)</i>	Locality (L)	<i>Subject's city</i>		YES	
	State (ST)	<i>Subject province</i>		YES	
	EmailAddress (E)	<i>Subject's email</i>			
	SERIAL NUMBER (SN)	<i>For instance</i> <i>p. eg: IDCES-00000000G. 3 characters to indicate the document number (IDC = national identity document) + 2 characters to identify the country (ES) + Identity number</i>		YES	
	OrganizationIdentifier	<i>The certificate must include at least = Serial Number or OrganizationIdentifier (NIF-VAT), eg</i> <i>VATES-B0085974Z</i>			
	Given Name (G)	<i>Name of the subject.</i> <i>First name, according to identity document (DNI / Passport)</i>		YES	
	SurName (SN)	<i>Surname of the subject.</i> <i>First surname, blank space, second surname of the person responsible for the certificate according to the DNI or in case of foreigner in passport</i>		YES	
	Common Name (CN)	<i>Full name + subject ID</i>		YES	
	Organizational Unit (OU)	AUTHENTICATION	<i>Class 2 Certificate of Natural Person (AUTHENTICATION)</i>		YES
		FIRM	<i>Class 2 Natural Person Certificate (SIGNATURE)</i>		
		Encryption	<i>Class 2 Certificate of Natural Person (CIFRADO)</i>		
	Organization (O)	<i>Example: O = Name of the College / collegiate number.</i> <i>In the case of professional training: you can include the name of the association, union or group to which you belong. Or issuer of the professional training degree. Additionally, the associate or union number can be included as specified in the previous case.</i> <i>In the case of freelancers, it can include: Registered trade name or Trademark registered in the name of the subject.</i>			
	Title (T)	<i>Subject title</i>			
Description					
<i>Alternative name of the subject</i> - 2.5.29.17					
<i>e-mail example: pedro@cial.com</i>					
<i>DNSName</i>				YES	
<i>Directory Name</i>					

Alternative name of the subject - SubjectAlternativeN love	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 proxy to the subscriber		
	1.3.6.1.4.1.18332.13	Surname of the natural person granting a proxy to the subscriber		
	1.3.6.1.4.1.18332.14	NIF / DNI / NIE of the legal entity or natural person that grants a representation to the subscriber		
	1.3.6.1.4.1.18332.20.3	Subscriber name		
	1.3.6.1.4.1.18332.20.4	Surname 1 subscriber		
	1.3.6.1.4.1.18332.20.5	Surname 2 subscriber		
	1.3.6.1.4.1.18332.20.8	eg: DNI		
	1.3.6.1.4.1.18332.20.13	pe: Spanish		
SubjectDirect oryAttributes	<i>SubjectDirectoryAttributes - 2.5.29.9</i>			
	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 / udllyk5ZN84paMeYx		
	1.3.6.1.4.1.18332.10.10.1	Example: https://tomcat2.anf.es/cliente_archivo_ws/poderes/(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		
	1.3.6.1.4.1.18332.41.1	1000		
	1.3.6.1.4.1.18332.41.2	eg signing of purchase contracts		
	1.3.6.1.4.1.18332.41.3	eg 10,000		
	1.3.6.1.4.1.18332.41.4	pe euros		
	1.3.6.1.4.1.18332.42.1			
	1.3.6.1.4.1.18332.42.11	It is filled in automatically by AR Manager		
	1.3.6.1.4.1.18332.42.13	It is filled in automatically by AR Manager		
	1.3.6.1.4.1.18332.47.1	It is filled in automatically by AR Manager		

1.3.6.1.4.1.18332.90				
1.3.6.1.4.1.18332.90.1				
1.3.6.1.4.1.18332.90.2				
1.3.6.1.4.1.18332.90.3				
1.3.6.1.4.1.18332.91.2				
1.3.6.1.4.1.18332.92				
1.3.6.1.4.1.18332.92.1				
1.3.6.1.4.1.18332.92.2				
1.3.6.1.4.1.18332.92.3				
1.3.6.1.4.1.18332.93				
1.3.6.1.4.1.18332.94				
1.3.6.1.4.1.18332.94.1				
1.3.6.1.4.1.18332.94.2				
1.3.6.1.4.1.18332.94.3				
1.3.6.1.4.1.18332.95				
1.3.6.1.4.1.18332.95.1				
1.3.6.1.4.1.18332.95.2				
1.3.6.1.4.1.18332.95.3				
1.3.6.1.4.1.18332.96				
1.3.6.1.4.1.18332.96.1				
1.3.6.1.4.1.18332.97				
1.3.6.1.4.1.18332.97.1				
1.3.6.1.4.1.18332.97.2				
1.3.6.1.4.1.18332.97.3				
1.3.6.1.4.1.18332.98				
1.3.6.1.4.1.18332.600		<i>Example: AR Manager desktop v.3.6 + Critocal + ANF CT</i>		
2.5.4.15	BusinessCategory	PrivateOrganization	PrivateOrganization	
			GovernmentEntity	
			BusinessEntity	
			Non-commercialEntity	
	JurisdictionOfIncorporationLocalityName			



	1.3.6.1.4.1.3 11.60.2.1.2	JurisdictionOfIncorporationStateOrProvinceYam		
	1.3.6.1.4.1.3 11.60.2.1.3	JurisdictionOfIncorporationCountryName		
1.3.6.1.4.1.18332.19	<i>Example 33993893-503677</i>			
1.3.6.1.4.1.18332.19.1	<i>Example 26144-56501328 3643648640</i>			
Identifier of the subject key - Subject Key Identifier	Hash in SHA1 of the public key used to sign the certificate			YES
SubjectPublicKeyInfo	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]			
QcCompliance	QcCompliance	FIRM / AUTHENTICATION	Present if the certificate is issued with the qualification of recognized. Annex I eIDAS	YES
	QcSSCD	only included in the SIGNATURE type	ONLY if the device is SSCD Secure Signature Creation Device (SSCD)	YES
	QcType- esign	FIRM QcType 1	ONLY at profile (SIGNATURE), QcType 1 reviewed	YES

Declarations of certificates recognized <i>Qualified Certificate Statement</i> TSI EN 319 412-1, formerly ETSI TS 101 862			ETSI EN 319 412-5		
	QcPDS	FIRM / AUTHENTICATION	https://anf.es/en/		YES
	QcLimitValue	FIRM / AUTHENTICATION	Limit amount of liability assumed by the issuer expressed in EUROS		YES
	QcRetentionPeriod	FIRM / AUTHENTICATION	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	FIRM / AUTHENTICATION	To indicate natural person semantics defined by EN 319 412-1		
Directives of the certificate - <i>Certificate Policies</i>	PolicyIdentifier	(AUTHENTICATION)	[1] Certificate Directive: Identifier of directive = 1.3.6.1.4.1.18332.3.4.1.1.22		YES
		(FIRM)	[1] Certificate Directive: Identifier of directive = 1.3.6.1.4.1.18332.3.4.1.2.22		
		(ENCRYPTED)	[1] Certificate Directive: Identifier of directive = 1.3.6.1.4.1.18332.3.4.1.3.22		
	PolicyCPSLocation		[1,1] Policy certifier information: Policy certifier ID = CPS Certifier: http://www.anf.es/documentos		YES
	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
	ONLY FOR KIND AUTHENTICATION AND	0.4.0.2042.1.2	NCP + (Normalized Certificate Policy requiring a secure user device)		

	PolicyIdentifier	ONLY FOR DEVICE Or HSM				
	PolicyIdentifier	ONLY FOR SIGNATURE TYPE	TOKEN HSM	qcp-natural-qscd (0.4.0.194112.1.2)		
			TOKEN SOFTWARE	qcp-natural (0.4.0.194112.1.0)		
Restrictions basic <i>Basic Constraints</i>	Type of matter = End entity Path length restriction = None CA = FALSE				YES	
Key usage <i>Key usage</i>	<i>Certified type: FIRM</i>		No repudiation (c0)		YES	
	<i>Certified type: AUTHENTICATION</i>		Digital signature, No repudiation (c0)			
	<i>Certified type: Encryption</i>		KeyEncipherment, dataEncipherment			
<i>Extended key usage</i>	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		
Algorithm ID	sha1					YES
Signature Value						YES
Fingerprint						YES
Descriptive name	<i>It is filled in automatically by AR Manager</i>					