

## Certification Policy of Issuance Reports Manager and PKI Operator Certificates. Certificate Profile

---



### **Security Level**

Public

---

### **Important Notice**

This document is property of ANF Autoridad de Certificación  
Distribution and reproduction is prohibited without written authorization  
from ANF Autoridad de Certificación

### **Copyright © ANF Autoridad de Certificación 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/en](http://www.anf.es/en)

---



# Issuance Reports Manager and PKI Operator Certificates

(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
<b>Issuer</b>	Common Name (CN)	<i>e.g. ANF Assured ID CA1</i>		YES
	SERIALNUMBER	G63287510		YES
	Organisation Identifier	G63287510		
	EmailAddress (E)	<i>This is the VAT number. At present ANF AC does not include it</i>		
	Organisational Unit (OU)	info@anf.es		YES
	Organisation (O)	Organizational unit within the Certification Services Provider responsible for the certificate issuance		YES
	Locality (L)	<i>e.g. ANF Autoridad de Certificacion</i>		
	State (ST)	<i>e.g. Barcelona (see current address at <a href="http://www.anf.es/es/address-direccion.html">http://www.anf.es/es/address-direccion.html</a>)</i>		
	Country (C)	<i>e.g. Barcelona</i>		YES
AuthorityCertIssuer				
AuthorityCertSerial Number				
Identifier of the issuer entity key – <i>Authority KeyIdentifier</i>	Hash with SHA1 of the public key used to sign the certificate			YES
<i>Issuer Alternative Name</i>				
Valid from <i>NotBefore</i>				YES
Valid until <i>NotAfter</i>				YES



<b>Subject</b> (all fields encoded using UTF-8)	<i>Subject</i>				
	1.3.6.1.4.1.18838.1.1	<i>Subject's National / Foreign Citizen ID Card</i>		YES	
	Country (C)	<i>Subject's country = subscriber</i>		YES	
	Locality (L)	<i>Subject's city</i>		YES	
	State (ST)	<i>Subject's state</i>		YES	
	EmailAddress (E)	<i>Subject's Email</i>			
	SERIAL NUMBER (SN)	<i>E.g.: IDCES-00000000G. 3 characters to indicate the document number (IDC= national identity document) + 2 characters to identify the country (ES) + ID number</i>		YES	
	OrganizationIdentifier	<i>The certificate must include at least= Serial Number or OrganizationIdentifier (VAT number), e.g.</i>  <i>VATES-B0085974Z</i>			
	Given Name (G)	<i>Name of subject, according to identity document (National/Foreign Citizens ID Card / Passport)</i>		YES	
	SurName (SN)	<i>Surname(s) of the subject.</i>  <i>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</i>		YES	
	Common Name (CN)	<i>Full name + Subject's National/Foreign Citizen ID Card</i>		YES	
	Organisational Unit (OU)	<b>AUTHENTICATION</b>	<i>Issuance Reports Manager Certificate (AUTHENTICATION)</i>		YES
		<b>SIGNATURE</b>	<i>Issuance Reports Manager Certificate (SIGNATURE)</i>		
		<b>ENCRYPTION</b>	<i>Issuance Reports Manager Certificate (ENCRYPTION)</i>		
		<b>AUTHENTICATION</b>	<i>PKI Operator Certificate (AUTHENTICATION)</i>		
		<b>SIGNATURE</b>	<i>PKI Operator Certificate (SIGNATURE)</i>		
		<b>ENCRYPTION</b>	<i>PKI Operator Certificate (ENCRYPTION)</i>		
Organisation (O)	<i>e.g.: O = ANF Autoridad de Certificación</i>				
Title (T)	<i>e.g. lawyer</i>				
Description					
SubjectAlternativeName - 2.5.29.17					
<i>email e.g.: pedro@cial.com</i>			YES		

SubjectAlternativeName	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	<i>SubjectDirectoryAttributes – 2.5.29.9</i>			
	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	knowledgeinformation		
	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			
	1.3.6.1.4.1.18332.42.3	Issuance Reports Manager			
	1.3.6.1.4.1.18332.42.4	Level 2 Recognized Registration Authority			
	1.3.6.1.4.1.18332.42.8	<i>e.g. 1</i>			
	1.3.6.1.4.1.18332.42.9	Authorized PKI Operator			
	1.3.6.1.4.1.18332.42.11	<i>e.g. Consultancy Harbinger</i>			
	1.3.6.1.4.1.18332.42.13	<i>e.g. legal department</i>			
	1.3.6.1.4.1.18332.47.1	<i>e.g.= 8&amp;1EB4F96F</i>			
	1.3.6.1.4.1.18332.47.3	<i>HSM Token Model</i>			
	1.3.6.1.4.1.18332.600	<i>e.g.: AR Manager desktop v.3.6</i>			
1.3.6.1.4.1.18332.19	<i>e.g. 33993893-503677</i>				
1.3.6.1.4.1.18332.19.1	<i>e.g. 26144-56501328 3643648640</i>				
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]				
	QcCompliance	<b>SIGNATURE / AUTHENTICATION</b>	<b>Present</b> if the certificate is issued with the recognized qualification. Annex I eIDAS	YES	
	QcSSCD	<b>only included in type SIGNATURE</b>	<b>ONLY if the device is SS CD</b> Secure Signature Creation Device (SSCD)	YES	

<p>Qualified Certificate Statement</p> <p>TSI EN 319 412-1, antes ETSI TS 101 862</p>				
	QcType- esign	<b>SIGNATURE</b> <i>QcType 1</i>	<b>ONLY in the profile (SIGNATURE),</b> <i>QcType 1is outlined</i> <i>ETSI EN 319 412-5</i>	YES
	QcPDS	<b>SIGNATURE / AUTHENTICATION</b>	<a href="https://anf.es/en/">https://anf.es/en/</a>	YES
	QcLimitValue	<b>SIGNATURE / AUTHENTICATION</b>	<i>Limit amount of liability assumed by the issuer expressed in EUROS</i>	YES
	QcRetentionPeriod	<b>SIGNATURE / AUTHENTICATION</b>	<i>Integer: =15</i> <i>([ETSI EN 319 412-5])</i> <i>Describes the conservation period of all information, relevant to the use of a certificate, after its expiration)</i>	YES
semnaticslD-Natural	<b>SIGNATURE / AUTHENTICATION</b>	To indicate the semantics of a natural person defined by the EN 319 412-1		
<p>Certificate Policies</p>	PolicyIdentifier	<b>IRM Certificate (AUTHENTICATION)</b>	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.23.1.1.22	YES
		<b>IRM Certificate (SIGNATURE)</b>	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.23.1.4.22	
		<b>IRM Certificate (ENCRYPTION)</b>	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.23.1.3.22	
		<b>PKI Operator Certificate (AUTHENTICATION)</b>	[1] Certificates policy: Policy identifier =1.3.6.1.4.1.18332.23.1.2.22	
		<b>PKI Operator Certificate (SIGNATURE)</b>	[1] Certificates policy: Policy	

			identifier =1.3.6.1.4.1.18332.23.1.6.22		
		<b>PKI Operator Certificate (ENCRYPTION)</b>	[1] Certificates policy:  Policy  identifier =1.3.6.1.4.1.18332.23.1.5.22		
	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	<b>ONLY FOR SIGNATURE TYPE</b>	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				
<i>Basic Constraints</i>	Type of matter =End entity  Route Length Restriction =None  CA = FALSE			YES	
<i>Key usage</i>	Certificate type: <b>SIGNATURE</b>	Non-repudiation (c0) KeyEncipherment, dataEncipherment		YES	
	Certificate type: <b>AUTHENTICATION</b>	Electronic signature, Non-repudiation (c0) KeyEncipherment, dataEncipherment			
	Certificate type: <b>ENCRYPTION</b>	KeyEncipherment,			



		dataEncipherment			
<i>Extended key usage</i>	<b>Signature / Authentication</b>	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