Política de Certificación de Certificados de Responsable de Dictámenes de Emisión y Operador PKI. Perfil de Certificado

Paseo de la Castellana, 79 – 28046 - Madrid (España)
Teléfono: 902 902 172 (llamadas desde España)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

Nivel de Seguridad

Público

Aviso Importante

Dirección: Paseo de la Castellana, 79. 28046 Madrid (España)

Teléfono: 902 902 172 (llamadas desde España) Internacional (+34) 933 935 946

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

Certificado de Responsable de Dictámenes de Emisión y Operador PKI

(AUTENTICACION) (FIRMA) (CIFRADO)
TOKEN POR SOFTWARE - TOKEN HSM

C	Campo	Valor		Crít	Oblig
	Versión	2 = (V3)			SI
	Número de serie				SI
	Algoritmo de firma. *SignatureAlgorithm*	sha256WithRSAEncryption			SI
	Algoritmo Hash de firma *SignatureHashAlgorithm*	sha256			SI
	Emisor	Common Name (CN)	*p.e. ANF Assured ID CA1*		SI
		SERIALNUMBER	G63287510		SI
		Organisation Identifier	*Se trata del VAT number, en España denominado NIF-IVA no es el CIF. Es el NIF para el IVA en la UE* *En la actualidad ANF AC no lo incluye*		
		EmailAddress (E)	info@anf.es		
		Organisational Unit (OU)	Unidad organizativa dentro del Prestador de Servicios de Certificación responsable de la emisión del certificado		SI
		Organisation (O)	*p.e. ANF Autoridad de Certificacion*		SI
		Locality (L)	*p.e. Barcelona (ver dirección actual en http://www.anf.es/es/address-direccion.html*		
		State (ST)	*p.e. Barcelona*		
		Country (C)	*p.e. ES*		SI
	AuthorityCertIssuer				
	AuthorityCertSerial Number				
	Identificador de la clave de la entidad emisora *Authority KeyIdentifier*	Hash con SHA1 de la clave pública utilizada para firmar el certificado			SI

Issuer Alternative Name					
Válido desde *NotBefore*					SI
Válido hasta *NotAfter*					SI
Sujeto *(todos los campos codificados utilizando UTF-8)*	*Subject*				
	1.3.6.1.4.1.18838.1.1	*DNI sujeto*			SI
	Country (C)	*País del sujeto=suscriptor*			SI
	Locality (L)	*Ciudad del sujeto*			SI
	State (ST)	*Provincia del sujeto*			SI
	EmailAddress (E)	*Email del sujeto*			
	SERIAL NUMBER (SN)	*Por ejemplo* *p. ej.: IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad*			SI
	OrganizationIdentifier	*El certificado debe de incluir al menos = Serial Number o OrganizationIdentifier (NIF-IVA), p.e.* *VATES-B0085974Z*			
	Given Name (G)	*Nombre del sujeto.* *Nombre de pila, de acuerdo con documento de identidad (DNI/ Pasaporte)*			SI
	SurName (SN)	*Apellidos del sujeto.* *Primer apellido, espacio en blanco, segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte*			SI
	Common Name (CN)	*Nombre completo + DNI sujeto*			SI
	Organisational Unit (OU)	**AUTENTICACION**	*Certificado de Responsable de Dictamenes de Emisión (AUTENTICACION)*		SI
		FIRMA	*Certificado de Responsable de Dictamenes de Emisión (FIRMA)*		
		CIFRADO	*Certificado de Responsable de Dictamenes de Emisión (CIFRADO)*		
		AUTENTICACION	*Certificado de Operador PKI (AUTENTICACION)*		

		FIRMA	*Certificado de Operador PKI (FIRMA)*		
		CIFRADO	*Certificado de Operador PKI (CIFRADO)*		
	Organisation (O)	*Ej.: O = ANF Autoridad de certificación*			
	Titulo (T)	*p.e. abogado*			
	Description				
Nombre alternativo del sujeto – SubjectAlternativeName	*Nombre alternativo del sujeto* - 2.5.29.17				
	eMail ejemplo: pedro@cial.com				YES
	DNSName *Directory Name*				
	1.3.6.1.4.1.18332.11	*Nombre completo de una persona física o jurídica, que otorga una representación al suscriptor*			
	1.3.6.1.4.1.18332.12	*Nombre de pila de la persona física que otorga una representación al suscriptor*			
	1.3.6.1.4.1.18332.13	*Apellidos de la persona física que otorga una representación al suscriptor*			
	1.3.6.1.4.1.18332.14	*NIF / DNI / NIE de la entidad jurídica o persona física que otorga una representación al suscriptor*			
	1.3.6.1.4.1.18332.20.3	*Nombre suscriptor*			
	1.3.6.1.4.1.18332.20.4	*Apellido 1 suscriptor*			
	1.3.6.1.4.1.18332.20.5	*Apellido 2 suscriptor*			
	1.3.6.1.4.1.18332.20.8	*Ejemplo= DNI, pasaporte, etc.*			
	1.3.6.1.4.1.18332.20.13	*Nacionalidad*			
SubjectDirect	*SubjectDirectoryAttributes – 2.5.29.9*				

oryAttributes	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	*Ejemplo: SHA256-gsq33wq/udldyk5ZN84paMeYx*		
	1.3.6.1.4.1.18332.10.10.1	*Ejemplo: https://tomcat2.anf.es/cliente_archivo_ws/poderes/(localizador AR=OID1.3.6.1.4.1.18332.19)*		
	2.5.4.2	*knowldgeinformation*		
	2.5.4.65	*Seudónimo –Pseudonym* *(elegido por el suscriptor)*		
	1.3.6.1.4.1.18332.30.1	*Nombre completo del país al que corresponde la emisión*		
	1.3.6.1.4.1.18332.40.1	*p.e. Certificado reconocido*		
	1.3.6.1.4.1.18332.41.1	*1000*		
	1.3.6.1.4.1.18332.41.2	*p.e. firma de contratos compra*		
	1.3.6.1.4.1.18332.41.3	*p.e. 10.000*		
	1.3.6.1.4.1.18332.41.4	*p.e. euros*		
	1.3.6.1.4.1.18332.42.1	*p.e. BCN. -345*		
	1.3.6.1.4.1.18332.42.2	Autoridad de Registro Reconocida Nivel 1		
	1.3.6.1.4.1.18332.42.3	Responsable Dictámenes de Emisión		
	1.3.6.1.4.1.18332.42.4	Autoridad de Registro Reconocida Nivel 2		
	1.3.6.1.4.1.18332.42.8	*p.e. 1*		
	1.3.6.1.4.1.18332.42.9	Operador Autorizado de la PKI		
	1.3.6.1.4.1.18332.42.11	*p.e. Gestoría Raimon*		
	1.3.6.1.4.1.18332.42.13	*p.e. departamento legal*		
	1.3.6.1.4.1.18332.47.1	*Ejemplo= 8&1EB4F96F*		
	1.3.6.1.4.1.18332.47.3	*Modelo del token HSM*		
	1.3.6.1.4.1.18332.600	*Ejemplo: AR Manager desktop v.3.6*		
1.3.6.1.4.1.18332.19	*Ejemplo 33993893-503677*			
1.3.6.1.4.1.18332.19.1	*Ejemplo 26144-56501328 3643648640*			
Identificador de la clave del sujeto - Subject Key Identifier	Hash en SHA1 de la clave pública utilizada para firmar el certificado			SI

SubjectPublic KeyInfo	RSA (2048) NIST P-256				SI
Acceso a la información de entidad emisora	AccessMethod [1]	*[1]Acceso a información de autoridad* *Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)*			SI
	AccessLocation [1]	*Nombre alternativo: Dirección URL=http://*			SI
	AccessMethod [2]	*1.3.6.1.5.5.7.48.2*			
	AccessLocation [2]	*Dirección URL=*			
Puntos de distribución CRL	cRLDistributionPoint [1]	*1]Punto de distribución CRL* *Nombre del punto de distribución:* *Nombre completo:* *Dirección URL*			SI
	DistributionPoint [2]				
	DistributionPoint [3]				
	QcCompliance	**FIRMA /** **AUTENTICACION**	***Presente*** *si el certificado es expedido con la calificación de reconocido. Anexo I eIDAS*		SI

Declaraciones de certificados reconocidos *Qualified Certificate Statement* TSI EN 319 412-1, antes ETSI TS 101 862	QcSSCD	**solo se incluye en el tipo FIRMA**	***SOLO si el dispositivo es SSCD*** Secure Signature Creation Device (SSCD)		SI
	QcType- esign	**FIRMA** *QcType 1*	***SOLO** en el **perfil (FIRMA),*** *se reseña QcType 1* *ETSI EN 319 412-5*		SI
	QcPDS	**FIRMA / AUTENTICACION**	*https://anf.es/en/*		SI
	QcLimitValue	**FIRMA / AUTENTICACION**	*Importe límite de responsabilidad asumido por el emisor expresado en EUROS*		SI
	QcRetentionPeriod	**FIRMA / AUTENTICACION**	*Integer: =15* *([ETSI EN 319 412-5]* *describe el periodo de conservación* *de toda la información relevante para el uso de un certificado, tras la* *caducidad de este)*		SI
	semnaticsId-Natural	**FIRMA / AUTENTICACION**	Para indicar semántica de persona física definida por la EN 319 412-1		
Directivas del certificado – *Certificate Policies*	PolicyIdentifier	**Certificado RDE (AUTENTICACION)**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.23.1.1.22		SI

			Certificado RDE (FIRMA)	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.23.1.4.22		
			Certificado RDE (CIFRADO)	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.23.1.3.22		
			Certificado Operador PKI (AUTENTICACION)	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.23.1.2.22		
			Certificado Operador PKI (FIRMA)	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.23.1.6.22		
			Certificado Operador PKI (CIFRADO)	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.23.1.5.22		
	PolicyCPSLocation		[1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.anf.es/documentos			SI
	User notice		[1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado conforme a la legislación firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.			SI
	PolicyIdentifier	**SOLO PARA TIPO FIRMA**	TOKEN HSM	qcp-natural-qscd (0.4.0.194112.1.2)		
			TOKEN SOFTWARE	qcp-natural (0.4.0.194112.1.0)		
Campos condicionados por el uso del certificado	BusinessCategory		PrivateOrganization			
			GovernmentEntity			
			BusinessEntity			
			Non-commercialEntity			
	JurisdictionOfIncorporationLocalityName		Localidad			

	JurisdictionOfIncorporationStateOrProvinceName	Provincia			
	JurisdictionOfIncorporationCountryName	País			
Restricciones básicas *Basic Constraints*	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno CA = FALSE			**SI**	
Uso de la clave *Key usage*	*Tipo certificado*: **FIRMA**	Sin repudio (c0) KeyEncipherment dataEncipherment		**SI**	
	Tipo certificado: **AUTENTICACION**	Firma digital, Sin repudio (c0) KeyEncipherment, dataEncipherment			
	Tipo certificado: **CIFRADO**	KeyEncipherment, dataEncipherment			
Extended key usage	**Firma / Autenticación**	1.3.6.1.5.5.7.3.2	Autenticación del cliente		SI
		1.3.6.1.5.5.7.3.4	Correo seguro		
Algoritmo de identificación	sha1				SI
Signature Value					SI
Huella digital					SI