Política de Certificación de Certificados de Empleado Público. 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 Empleado Público

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

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				SI

NotBefore				
Válido hasta *NotAfter*				SI
Sujeto *(todos los campos codificados utilizando UTF-8)*	*Subject*			
	Country (C)	*p.e.= ES*		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)	*p. ej.: "JUAN ANTONIO"*		SI
	SurName (SN)	*p. ej.: "DE LA CAMARA ESPAÑOL - DNI 00000000G*		SI
	Common Name (CN)	*ej.: JUAN ANTONIO DE LA CAMARA ESPAÑOL - DNI 00000000G*		SI
	Organisational Unit (OU)	Certificado de Empleado Publico Nivel Alto **(AUTENTICACION)**		SI
		Certificado de Empleado Publico Nivel Alto **(FIRMA)**		
		Certificado de Empleado Publico Nivel Alto **(CIFRADO)**		
		Certificado de Empleado Publico Nivel Medio		
		p. ej.: SUBDIRECCION GENERAL DE PROCESO DE DATOS		
		OU = p. ej.: E04976701		
		Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. *Ver NOTA 3*		
	Organisation (O)	*p. ej.: MINISTERIO DE FOMENTO.*		

	Titulo (T)		*p. ej.: ANALISTA PROGRAMADOR. Nombre descriptivo del puesto o cargo que ostenta el responsable del certificado*		
Nombre alternativo del sujeto – SubjectAlternativeName	*Nombre alternativo del sujeto* - 2.5.29.17				
	eMail ejemplo: pedro@cial.com				SI
	DNSName *Directory Name*				
	Nivel ALTO	2.16.724.1.3.5.7.1.1	*Certificado de Empleado Público Nivel Alto (AUTENTICACIÓN)*		SI
			Certificado de Empleado Público Nivel Alto (FIRMA)		
			Certificado de Empleado Público Nivel Alto (CIFRADO)		
	Nivel MEDIO	2.16.724.1.3.5.7.2.1	*Certificado de Empleado Público Nivel Medio*		
	Nivel ALTO	2.16.724.1.3.5.7.1.2	*p. ej.: MINISTERIO DE FOMENTO*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.2			
	Nivel ALTO	2.16.724.1.3.5.7.1.3	*p. ej.: S2833002*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.3			
	Nivel ALTO	2.16.724.1.3.5.7.1.4	*p. ej.: 00000000G*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.4			
	Nivel ALTO	2.16.724.1.3.5.7.1.5	*p. ej.: A02APE1056*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.5			
	Nivel ALTO	2.16.724.1.3.5.7.1.6	*Ej.: "JUAN ANTONIO"*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.6			
	Nivel ALTO	2.16.724.1.3.5.7.1.7	*Ej.: "DE LA CAMARA"*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.7			
	Nivel ALTO	2.16.724.1.3.5.7.1.8	*Ej.: "ESPAÑOL"*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.8			

	Nivel ALTO	2.16.724.1.3.5.7.1.9	*P. ej.: juanantonio.delacamara.espanol@mfom.es*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.9			
	Nivel ALTO	2.16.724.1.3.5.7.1.10	*p. ej.: SUBDIRECCION GENERAL DE PROCESO DE DATOS*		SI
	Nivel MEDIO	2.16.724.1.3.5.7.2.10			
	Nivel ALTO	2.16.724.1.3.5.7.1.11	*p. ej.: ANALISTA PROGRAMADOR (*		SI
	Nivel MEDIO	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		*Ejemplo: SHA256-gsq33wq/udldyk5ZN84paMeYx*		
	1.3.6.1.4.1.18332.10.10.1		*Ejemplo: https://www.anf.es/app/ + (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*		
	1.3.6.1.4.1.18332.42.1				
	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		*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]				
Declaraciones de certificados reconocidos *Qualified Certificate Statement*	QcCompliance	**FIRMA de** **(NIVEL ALTO) y** **(NIVEL MEDIO)**	***Presente*** *si el certificado es expedido con la calificación de reconocido. Anexo I eIDAS*		SI
	QcSSCD	**SOLO se incluye en el tipo** **Nivel ALTO (FIRMA)**	***SOLO si el dispositivo es SSCD*** Secure Signature Creation Device (SSCD)		SI
	QcType- esign	**FIRMA de** **(NIVEL ALTO) y** **(NIVEL MEDIO)** *QcType 1*	*se reseña QcType 1* *ETSI EN 319 412-5*		SI
	QcPDS	**FIRMA -** **(NIVEL ALTO)** **(NIVEL MEDIO)**	https://anf.es/en/ *URL que permite acceder a todas las políticas de la PKI en inglés. Protocolo https*		SI

TSI EN 319 412-1, antes ETSI TS 101 862				*ETSI EN 319 412-5*		
	QcLimitValue		**FIRMA de (NIVEL ALTO) y (NIVEL MEDIO)**	*Importe límite de responsabilidad asumido por el emisor expresado en EUROS*		SI
	QcEuRetentionPeriod		**FIRMA de (NIVEL ALTO) y (NIVEL MEDIO)**	*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 de (NIVEL ALTO) y (NIVEL MEDIO)**	Para indicar semántica de persona física definida por la EN 319 412-1		
Directivas del certificado – *Certificate Policies*	PolicyIdentifier	**Nivel ALTO**	**(AUTENTICACION)**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.1.22		SI
		Nivel ALTO	**(FIRMA)**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.3.22		
		Nivel ALTO	**(CIFRADO)**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.4.22		
		Nivel MEDIO		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.4.1.2.22		SI
	PolicyIdentifier	Nivel ALTO	[2]Directiva de certificados: Identificador de directiva=2.16.724.1.3.5.7.1			SI
		Nivel MEDIO	[2]Directiva de certificados: Identificador de directiva=2.16.724.1.3.5.7.2			SI
	PolicyCPSLocation		[1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador:			SI

			http://www.anf.es/documentos			
	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 **AUTENTICACION** Y SOLO PARA **DISPOSITIVO HSM**	0.4.0.2042.1.2	NCP+ (Normalized Certificate Policy requiring a secure user device)		
	PolicyIdentifier	**SOLO PARA TIPO FIRMA /AUTENTICACION**	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*	*(NIVEL ALTO)* FIRMA			Sin repudio (c0)	**SI**	
	(NIVEL ALTO) AUTENTICACION			Firma digital		
				KeyEncipherment		
				dataEncipherment		
	(NIVEL ALTO) CIFRADO			KeyEncipherment,		
				dataEncipherment		
	Nivel MEDIO			Digital Signature		

		Sin repudio (c0)			
		Key Encipherment			
		dataEncipherment			
Uso mejorado de las claves - *Extended key usage*	(Nivel ALTO) **Firma / Autenticación / Cifrado** (Nivel MEDIO)	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