Política de Certificación de Sello Electrónico.

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 Sello Electrónico

(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)	*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*		
	OrganizationName (O)	*p. ej.: Nombre empresa. S.L.*		SI
	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)	**Certificado de Sello Electrónico**		SI
		Certificado de Sello Electrónico AA.PP. Nivel Medio		
		Certificado de Sello Electrónico AA.PP. Nivel Alto	*Solo en dispositivos HSM*	
	Organisational Unit (OU)	*p. ej: SUBDIRECCION DE EXPLOTACION*		
		SOLO en certificados AA.PP.	*p. ej: E04976701*	
	Description	*p.e.* *Reg: XXX /Hoja: XXX /Tomo: XXX /Sección: XXX /Libro: XXX /Folio: XXX /Fecha: dd-mm-aaaa /Inscripción: XXX* *Notario: Nombre Apellido1 Apellido2 /Núm. Protocolo: XXX*		SI

		/Fecha Otorgamiento: dd-mm-aaaa *En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa* */Numero resolución: XXX*			
	Titulo (T)	*p.e. Administrador Único*			
Nombre alternativo del sujeto – SubjectAlternativeName	*Nombre alternativo del sujeto* - 2.5.29.17				
	eMail ejemplo: pedro@cial.com *DNSName* *Directory Name*				SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.1*	*p.e. Pedro*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.2*	*p.e. López*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.3*	*p.e. García*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.4*	*p.e. 8907234W*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.10.7*	*p.e. pedrolopez@anf.es*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.1*	*p.e. Juan Antonio*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.2*	*Ej: "DE LA CAMARA"*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.3*	*Ej: "ESPAÑOL"*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.4*	*p.e. 896789234J*		SI
	Sello Electrónico	*1.3.6.1.4.1.18332.29.5*	*p.e. juanesp@anf.es*		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.1	Certificado de Sello Electrónico AA.PP. Nivel Alto		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.1	Certificado de Sello Electrónico AA.PP. Nivel Medio		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.2	*p.e. Nombre empresa. S.L.*		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.2	*p.e. Nombre empresa. S.L.*		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.3	*p. ej: S2833002*		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.3	*p. ej: S2833002*		SI
	AA.PP.	2.16.724.1.3.5.6.1.4	*p. ej: 00000000G*		SI

	Nivel ALTO				
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.4	*p. ej: 00000000G*		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.5	*p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA.*		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.5	*p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA.*		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.6	*Ej: "JUAN ANTONIO"*		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.6	*Ej: "JUAN ANTONIO"*		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.7	*Ej: "DE LA CAMARA"*		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.7	*Ej: "DE LA CAMARA"*		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.8	*Ej: "ESPAÑOL"*		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.8	*Ej: "ESPAÑOL"*		SI
	AA.PP. Nivel ALTO	2.16.724.1.3.5.6.1.9	*p.e. juanesp@anf.es*		SI
	AA.PP. Nivel MEDIO	2.16.724.1.3.5.6.2.9	*p.e. juanesp@anf.es*		SI
SubjectDirectoryAttributes	*SubjectDirectoryAttributes – 2.5.29.9*				
	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)*			
	1.3.6.1.4.1.18332.19	*Ejemplo 33993893-503677*			
	1.3.6.1.4.1.18332.19.1	*Ejemplo 26144-56501328 3643648640*			
	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			
	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*		
	1.3.6.1.4.1.18332.90			
	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	*Ejemplo: AR Manager desktop v.3.6+Critocal+ANF CT*		

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		***Presente** si el certificado es expedido con la calificación de reconocido. Anexo I eIDAS*		SI
	QcSSCD	**solo se incluye con dispositivo HSM**	***Presente si el dispositivo es SSCD*** Secure Signature Creation Device (SSCD)		SI
	QcType- esign	***QcType 2***	*se reseña QcType 2* *ETSI EN 319 412-5*		SI
	QcPDS	https://anf.es/en/	*Se proporciona la URL que permite acceder a todas las políticas de la PKI en inglés. Protocolo https* *ETSI EN 319 412-5*		SI
	QcLimitValue		*Importe límite de responsabilidad asumido por el emisor expresado en EUROS*		SI
	QcRetentionPeriod		*Integer: = 15* *([ETSI EN 319 412-5]* *describe el periodo de conservación*		SI

TSI EN 319 412-1, antes ETSI TS 101 862			*de toda la información relevante para el uso de un certificado, tras la caducidad de este)*		
	semnaticsId-Natural		Para indicar semántica de persona fisica definida por la EN 319 412-1		
Directivas del certificado – *Certificate Policies*	PolicyIdentifier	**Sello Electrónico**	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.25.1.1.1		SI
		Sello Electrónico AA.PP. Nivel Alto	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.25.1.1.2		
		Sello Electrónico AA.PP. Nivel Medio	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.25.1.1.3		
	PolicyIdentifier	**Sello Electrónico AA.PP. Nivel Alto**	2.16.724.1.3.5.6.1		SI
		Sello Electrónico AA.PP. Nivel Medio	2.16.724.1.3.5.6.2		
	PolicyCPSLocation	[1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: 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	TOKEN HSM	qcp-natural-qscd (0.4.0.194112.1.3)		SI
		TOKEN SOFTWARE	qcp-natural (0.4.0.194112.1.1)		
Restricciones básicas *Basic Constraints*	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno CA = FALSE			**SI**	
Uso de la clave	*Digital Signature*	Se utiliza cuando se realiza la función de autenticación de activo digital de la persona jurídica		**SI**	

Key usage	*Content Commitment*	Se utiliza cuando se realiza la función de sello electrónico de documento expedido por persona jurídica		
	Key Encipherment	Se utiliza para gestión y transporte de claves		
	Data Encipherment	Se utiliza para el cifrado de datos.		
Uso mejorado de las claves - *Extended key usage*	Client Authentication	1.3.6.1.5.5.7.3.2		SI
	Email Protection	1.3.6.1.5.5.7.3.4		
	Server Authentication	1.3.6.1.5.5.7.3.1		
	codeSigning	1.3.6.1.5.5.7.3.3		
Algoritmo de identificación	sha1			SI
Signature Value				SI
Huella digital				SI