Política de Certificación de Certificados de Servidor Seguro (OV), Servidor Seguro (DV), Servidor Seguro (EV), Sede Electrónica y Sede Electrónica (EV)

Perfil Técnico

Paseo de la Castellana, 79 – 28046 - Madrid (Spain)
Telephone: 902 902 172 (Calls from Spain)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

Nivel de Seguridad

Publico

AVISO IMPORTANTE

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (Spain)

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

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

Certificado de Servidor Seguro (OV), Servidor Seguro (DV) Servidor Seguro (EV), Sede Electrónica y Sede Electrónica (EV)

TOKEN POR SOFTWARE - TOKEN HSM

Campo	OID	valor		Norma	APP	Aclaración	Crít	Oblig
Versión		2 = (V3)		RFC 5280	Emisor	Integer: =2 ([RFC5280] describe la versión del certificado al usar extensiones es decir v3 su valor debe ser 2)		SI
Número de serie				RFC 5280	Emisor	Establecido automáticamente por ANF AC. [RFC5280] integer positivo, no mayor 20 octetos (1- 2^{159}) Se utiliza para identificar de manera unívoca el certificado		SI
Signature Algorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		RFC 5280	Emisor	Identificador del Algoritmo de firma String UTF8 (40). Identificando el tipo de algoritmo.		SI
Signature HashAlgorithm	2.16.840.1.101.3.4.2.1	sha256			Emisor	Identificador del Algoritmo hash de firma		SI
Emisor	2.5.4.3	Common Name (CN)	*p.ej. ANF Assured ID CA1*		AR Manager	Nombre común de la CA emisora del certificado		SI
	2.5.4.5	SERIALNUMBER	G63287510		AR Manager	CIF de ANF AC		SI
	2.5.4.97	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*	eIDAS	Emisor	Identificación de la organización emisora. Como se especifica en cláusula 5.1.4 de ETSI EN 319 412-1 [7].		
		EmailAddress (E)	info@anf.es		Emisor	Email CA		

	2.5.4.11	Organisational Unit (OU)	Unidad organizativa dentro del Prestador de Servicios de Certificación responsable de la emisión del certificado		AR Manager	Tal y como aparece en el certificado del emisor. (String UTF8) Size [RFC 5280] 128		SI
	2.5.4.10	Organisation (O)	*p.e. ANF Autoridad de Certificacion*		Emisor	Nombre oficial del Prestador de Servicios de Certificación		SI
		Locality (L)	*p.e. Barcelona (see current address at http://www.anf.es/es/address-direccion.html)*		Emisor	Localidad/dirección del Prestador de Servicios de Certificación (String UTF8) Size [RFC 5280] 128		
		State (ST)	*p.e. Barcelona*		Emisor	Provincia del Prestador de Servicios de Certificación		
	2.5.4.6	Country (C)	*p.e. ES*	(2 character ISO 3166 country code [5])	AR Manager	País del Prestador de Servicios de Certificación (PrintableString) Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements" Size 2 [RFC 5280]		SI
AuthorityCertIssuer				(String UTF8) Size 128	Emisor	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier		
AuthorityCertSerialNumber				(Integer)	Emisor	Número de serie del certificado de CA		
Identificador de la clave de la entidad emisora - *Authority* *KeyIdentifier*	2.5.29.35	Hash con SHA1 de la clave pública utilizada para firmar el certificado		RFC 5280 (String UTF8)	Emisor	Identificador derivado de utilizar la función de hash sobre la clave pública del sujeto. Es un medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado		SI
Issuer Alternative Name	2.5.29.18							
Válido desde *NotBefore*					Emisor	Fecha inicio validez		SI
Válido hasta *NotAfter*					Emisor	Fecha fin de validez		SI

Sujeto *(todos los campos codificados utilizando UTF-8)*	2.5.4.6	Country (C)	*País del sujeto=suscriptor*	*Código de país dos dígitos* *ISO 3166-1*	AR manager	Según ETSI-QC este campo se debe cumplimentar obligatoriamente Ver RFC 3739 / ETSI 101862		SI
	2.5.4.7	Locality (L)	*Ciudad del sujeto*	*(String UTF8)* *Size [RFC 5280] 128*	AR manager			SI
	2.5.4.8	State (ST)	*Provincia del sujeto*		AR manager			SI
	1.2.840.113549.1.9.1	EmailAddress (E)	*Email del sujeto*		AR manager			
	2.5.4.5	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*	*(Printable String))* *Size [RFC 5280] 64*	AR manager	NIF del suscriptor del certificado Preferiblemente se utilizará la semántica propuesta por la norma ETSI EN 319 412-1		SI
	2.5.4.97	Organization Identifier	*El certificado debe de incluir al menos = Serial Number o OrganizationIdentifier (NIF-IVA), p.e.* *VATES-B0085974Z*	*Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)*	AR manager	VAT number. NIF, tal como figura en los registros oficiales. Codificado Según la Norma Europea EN 319 412-1 No confundir con el DNI, se trata del NIF de IVA para la UE		
	2.5.4.10	Organization Name (O)	*p.e. Nombre empresa. S.L.*	*(String UTF8) Size [RFC 5280] 128* *ETSI EN 319 412-1 [i.4], clause 5*	AR manager	Denominación (nombre "oficial" de la organización) del suscriptor		SI
	2.5.4.42	Given Name (G)	*Nombre de pila del representante legal, de acuerdo con documento de identidad (DNI/Pasaporte)*	*(String UTF8) Size 40.* *Obligatorio según ETSI EN 319 412-2*	AR manager	Nombre del representante legal (tal como consta en su DNI/NIE/pasaporte).		SI
	2.5.4.4	SurName (SN)	*Apellidos del representante legal.* *Primer apellido, espacio en blanco, segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte*	*(String UTF8) Size 80.* *Obligatorio según ETSI EN 319 412-2*	AR manager	Apellido(s) del representante legal (tal como consta en su DNI/NIE/pasaporte).		SI

	2.5.4.3	Common Name (CN)	***p.e.*** *anf.es*		*(String UTF8) Size 132 [RFC 5280]*	AR manager	Dominio (DNS) donde residirá el certificado.		SI
	2.5.4.11	Organisational Unit (OU)	SSL DV		*Certificado de Servidor Seguro SSL DV*	String UTF8) Size [RFC 5280] 128	AR Manager	Descripción del tipo de certificado	SI
			SSL OV		*Certificado de Servidor Seguro SSL OV*				
			SSL EV		*Certificado de Servidor Seguro SSL EV*				
			Sede Nivel Medio		*Certificado de Sede Electronica Nivel Medio*				
			Sede EV Nivel Medio		Certificado de Sede Electronica EV Nivel Medio				
			Sede Nivel Alto		Certificado de Sede Electronica Nivel Alto	Perfil AAPP	ANF CT	Solo si el dispositivo es HSM	SI
			Sede EV Nivel Alto		Certificado de Sede Electronica EV Nivel Alto	Perfil AAPP	ANF CT	Solo si el dispositivo es HSM	SI
	2.5.4.11	Organisational Unit (OU)	Certificado de SEDE ELECTRONICA		*p. ej.: PUNTO DE ACCESO GENERAL*	*Perfil AAPP*	AR manager	El nombre descriptivo de la sede.	
	2.5.4.15	businessCategory	PrivateOrganization		*para organización privada*	*CAB FORUM*	AR manager	Categoría de organización (requerido para certificados EV)	SI
			GovernmentEntity		*para entidad pública*				
			BusinessEntity		*para empresa*				
			Non-commercialEntity		*para entidad no comercial*				
	1.3.6.1.4.1.31 1.60.2.1.3	JurisdictionCountryName	Solo certificados EV		*p.e. ES*	*CAB FORUM*	AR manager	Jurisdicción (requerido para certificados EV)	SI
	1.3.6.1.4.1.31 1.60.2.1.1	JurisdictionOfIncorporationLocalityName	Solo certificados EV		*p.e. Badalona*				
	1.3.6.1.4.1.31 1.60.2.1.2	JurisdictionOfIncorporationStateOrProvinceName	Solo certificados EV		*P.e. Barcelona*				
Nombre	Nombre alternativo del sujeto – SubjectAlternativeName - 2.5.29.17								

alternativo del sujeto – SubjectAlternativeName	*eMail ejemplo: pedro@cial.com*		*Nombre RFC822* *(String) Size [RFC 5280] 255*	ANF CT	Correo electrónico de la persona responsable del certificado		
	DNSName *Directory Name*	*p.e. anf.es* *frater.es*	*(String UTF8) Size = 128*	AR manage	Nombre de Dominio DNS **Puede contener varios dominios**		
SubjectDirectoryAttributes	SubjectDirectoryAttributes - 2.5.29.9						
	2.5.4.20	*TelephoneNumber*		AR manager	Teléfono del suscriptor		
	2.5.4.23	*Facsimile*		AR manager	Fax del suscriptor		
	2.5.4.9	*StreetAddress*		AR manager	Dirección del suscriptor		
	2.5.4.16	*PostalAddress*		AR manager	Dirección postal del suscriptor		
	2.5.4.17	*PostalCode*		AR manager	Código postal del suscriptor		
Identificador de la clave del sujeto - *Subject Key Identifier*	2.5.29.14	Hash en SHA1 de la clave pública utilizada para firmar el certificado	*RFC 5280* *Conforme con estándares RFC2459 & PKCS#1*	Emisor	Identificador derivado de utilizar la función de hash sobre la clave pública del sujeto.		SI
SubjectPublicKeyInfo		RSA (2048)	*(String UTF8)* *RSA en conformidad con la RFC 4055 [1 0] y ECC algoritmo en conformidad con la RFC 5639 [11]*	Emisor	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave.		SI
Acceso a la información de entidad emisora	1.3.6.1.5.5.7.1.1	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)*	*Emisor*	Id-ad-ocsp con OID: (OCSP)		SI
		AccessLocation [1]	*Nombre alternativo:* *Dirección URL=http://*	*Emisor*	Dirección Respondedor OCSP		SI
		AccessMethod	*1.3.6.1.5.5.7.48.2*	*Emisor*	id-ad-caIssuers con OID		

		[2]						
		AccessLocation [2]	*Dirección URL=*		*Emisor*	localización del certificado de la CA		
Puntos de distribución CRL	2.5.29.31	cRLDistributionPoint [1]	*[1]Punto de distribución CRL* *Nombre del punto de distribución:* *Nombre completo:* *Dirección URL*		*Emisor*	Indica punto de descarga de la CRL.		SI
Declaraciones de certificados cualificados *Qualified Certificate Statement* TSI EN 319 412-1, antes ETSI TS 101 862	1.3.6.1.5.5.7.1.3	0.4.0.1862.1.1	QcCompliance	**SOLO EV**	***Presente*** *si el certificado es expedido con la calificación de cualificado. Anexo I eIDAS*	ANF CT	**qcStatements** en conformidad con ETSI EN 319 412-5		SI
		0.4.0.1862.1.4	QcSSCD	**SOLO EV con HSM**	***SOLO si el dispositivo es SSCD*** Secure Signature Creation Device (SSCD)	ANF CT	*Determina que la clave privada asociada a la clave pública contenida en el certificado electrónico, está en un dispositivo seguro de creación de firma, Reglamento (UE) 910/2014 [I.8]*		SI
		0.4.0.1862.1.6.3	QcType-web	**SOLO EV** *QcType 3*	*se reseña QcType 3* *ETSI EN 319 412-5*	ANF CT	**id-etsi-qcsQcType** clausula 4.2.3 en ETSI EN 319 412-5 *Sigue la codificación siguiente:* id-etsi-qct-esign (id-etsi-qcs-QcType 1) id-etsi-qct-eseal (id-etsi-qcs-QcType 2) id-etsi-qct-web (id-etsi-qcs-QcType 3)		SI
		0.4.0.1862.1.5	QcPDS	**SOLO EV**	*https://anf.es/en/* *URL que permite acceder a todas las políticas de la PKI en inglés. Protocolo https* *ETSI EN 319 412-5*	ANF CT	No se incluye en el tipo CIFRADO		SI
		0.4.0.1862.1.2	QcLimitValue	**SOLO EV**	*Importe límite de responsabilidad asumido por el emisor expresado en EUROS*	ANF CT	<QcLimitValue> <money>EUR</money> <qcBase>1</qcBase> <qcExp>3</qcExp>		SI

							</QcLimitValue> No se incluye en el tipo CIFRADO		
		0.4.0.1862.1.3	QcRetentionPeriod	**SOLO EV**	*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)*	ANF CT	No se incluye en el tipo CIFRADO		SI
		0.4.0.194121.1.2	semnaticsId-Legal	**SOLO EV**	Para indicar semántica de persona física definida por la EN 319 412-1	AR Manager	Para indicar semántica de persona jurídica definida por la EN 319 412-1		
Directivas del certificado – *Certificate Policies*	2.5.29.32	PolicyIdentifier	SSL DV		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.1.22	AR Manager	OID propietario de ANF AC		SI
			SSL OV		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.7.22				
			SSL EV		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.2.22				
			Sede Nivel Medio		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.3.22				
			Sede Nivel Medio EV		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.5.22				
			Sede Nivel Alto		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.4.22				
			Sede Nivel Alto EV		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.6.22				
		PolicyIdentifier	SSL DV		2.23.140.1.2.1	AR Manager	CA/B FORUM y perfil AAPP		SI
			SSL OV		2.23.140.1.2.2				
			SSL EV		2.23.140.1.1				
			Si el suscriptor es una persona física		2.23.140.1.2.3				
			Sede electrónica NIVEL ALTO		2.16.724.1.3.5.5.1				
			Sede electrónica NIVEL MEDIO		2.16.724.1.3.5.5.2				
		PolicyIdentifier	SSL DV		0.4.0.2042.1.6	AR Manager	Norma ETSI TS 102 042 y ETSI 101 456		SI
			SSL OV		0.4.0.2042.1.7				
			SSL EV		0.4.0.2042.1.4				
			Sede EV		0.4.0.2042.1.4				
			Emitido como		0.4.0.1456.1.1				

			cualificado + HSM					
		PolicyCPSLocation	[1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.anf.es/documentos		AR Manager			
		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.		AR Manager	Máximo 200 caracteres. Se expresa una declaración realizada por la CA emisora, en la que se hace referencia a determinadas normas legales.		SI
		PolicyIdentifier	**SSL EV**	0.4.0.194112.1.4 (qcp-web)	AR Manager	Todos los certificados que son emitidos como cualificados. Certificado cualificado de sitio web acorde al Reglamento UE 910/2014		SI
			Sede EV					
Restricciones básicas *Basic Constraints*	2.5.29.19	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno CA = FALSE			Emisor	Determina que se trata de un certificado de usuario final	**SI**	
Uso de la clave *Key usage*	2.5.29.15	Digital Signature		Se utiliza cuando se realiza la función de autenticación	AR manager		**SI**	
		Key Encipherment		Se utiliza para gestión y transporte de claves				
Uso mejorado de las claves - *Extended key usage*	2.5.29.37	Autenticación servidor		Autenticación TSL web Server 1.3.6.1.5.5.7.3.1	AR manager			SI
		Autenticación del cliente		Autenticación TSL web Cliente 1.3.6.1.5.5.7.3.2				
Algoritmo de identificación		sha1			Emisor			SI
Huella digital					Emisor	Huella digital del certificado		SI