Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SERVICIOS DIGITALES E INNOVACIÓN
DEPARTAMENTO CERES

DEFINICIÓN PERFILES DE CERTIFICADOS TSU DE LA FNMT

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	03/10/2025
Revisado por:	FNMT-RCM	03/10/2025
Aprobado por:	FNMT-RCM	07/10/2025

Referencia:

Documento clasificado como: *Difusión pública*

1. INTRODUCCIÓN

En el presente documento se describe tanto el perfil del certificado de la autoridad de certificación (AC) encargada de la emisión de certificados de sello electrónico para firma digital de sellos de tiempo (TSUs), así como los perfiles de los certificados emitidos por dicha AC.

2. PERFIL DE CERTIFICADO DE AC TSA CLIENTES

Campo		Contenido	Obligatoriedad	Especificaciones
1. Version		2	Sí	Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		ecdsa-with-SHA384	Sí	String. OID: 1.2.840.10045.4.3.3
4. Issuer Distinguish Name		Entidad emisora del certificado	Sí	
	4.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 64 (rfc5280)
	4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J	Sí	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9 caracteres Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) - 3 caracteres para indicar el tipo legal de identificador (VAT= documento de identificación fiscal)

Campo		Contenido	Obligatoriedad	Especificaciones
				- 2 caracteres para identificar el país ISO 3166-1 [2] - 1 carácter "-" 0x2D (ASCII), U+002D (UTF-8)
	4.4. Common Name	AC del prestador de servicios de confianza bajo la cual se generar el certificado electrónico cn= AC RAIZ FNMT-RCM TSA	Si	UTF8 String, tamaño máximo 64 (rfc5280)
5. Validity		15 años	Sí	
6. Subject			Sí	Identificación del titular asociado a la clave pública
	6.1. Country	C=ES	Sí	Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí	UTF8 String, tamaño máximo 64 (rfc5280)
	6.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J	Sí	PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	6.4. Common Name	AC del prestador de servicios de confianza bajo la cual se generar el certificado electrónico cn= AC TSA CLIENTES	Sí	UTF8 String, tamaño máximo 64 (rfc5280)
7. Authority Key Identifier		Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la AC para firmar el certificado de esta AC Subordinada	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC raíz.
8. Subject Public Key Info		Clave pública de la AC Subordinada para la	Sí	Campo para transportar la clave pública y para

Campo		Contenido	Obligatoriedad	Especificaciones
		Administración Pública, codificada de acuerdo con el algoritmo criptográfico. En este caso Secp384r1.		identificar el algoritmo con el cual se utiliza la clave. ECC P-384 bits
9. Subject Key Identifier		Identificador de la clave pública de la AC Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	0	Sí	Ver X509 y RFC 5280
	10.2. Content Commitment	0	Sí	Ver X509 y RFC 5280
	10.3. Key Encipherment	0	Sí	Ver X509 y RFC 5280
	10.4. Data Encipherment	0	Sí	Ver X509 y RFC 5280
	10.5. Key Agreement	0	Sí	Ver X509 y RFC 5280
	10.6. Key Certificate Signature	1	Sí	Ver X509 y RFC 5280
	10.7. CRL Signature	1	Sí	Ver X509 y RFC 5280
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
	11.1. id_kp_timeStamping	1.3.6.1.5.5.7.3.8	Sí	
12. Certificate Policies		Política de certificación	Sí	
	12.1. Policy Identifier	2.5.29.32.0 (anyPolicy)	Sí	Identificador de la política de identificación.
13. CRL Distribution Point			Sí	
	13.1. Distribution Point 1	Punto de distribución 1 de la CRL (ARL) http://www.cert.fnmt.es/crls/ACRAIZFNMTTSA.crl	Sí	

Campo		Contenido	Obligatoriedad	Especificaciones
14. Authorit y Info Access				
	1.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí	
	1.2. Acces Location 1	http://ocspraiztsa.cert.fnmt.es/ocspraiztsa/OcspResponder	Sí	
	1.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí	
	1.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTTSA.crt	Sí	
15. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".		
	15.1. Subject Type	CA		Tipo de sujeto: Autoridad de Certificación.
	15.2. Path Length	0		Un pathLenConstraint de cero indica que ningún no pueden existir más certificados de AC intermedios en la ruta de certificación.

3. PERFIL DE CERTIFICADO DE TSU BAJO AC TSA CLIENTES

Campo	Contenido	Oblig.	Crit.	Especificaciones
1. Version	2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2159).
3. Signature Algorithm	ecdsa-with-SHA384	Si	No	String. OID: 1.2.840.10045.4.3.3
4. Issuer Distinguish Name	Entidad emisora del Sello	Sí	No	
4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J	Sí		PrintableString, tamaño 64 (X520).
4.4. Common Name	AC del prestador de servicios de confianza bajo la cual se generar el certificado electrónico cn= AC TSA CLIENTES	Sí		UTF8 String, tamaño máximo 64 (rfc5280)
5. Validity	5 años	Sí	No	

Campo		Contenido	Oblig.	Crit.	Especificaciones
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Sí	No	
	6.1. Country	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas. C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Locality	Nombre de la localidad del suscriptor (organización)	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del creador del Sello	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Organization Identifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Sí		OrganizationIdentifier p. ej: VATES-S2833002.
	6.5. Common Name	Denominación de la unidad de sellado de tiempo (TSU)	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo: cn= TSU 2025
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la AC para firmar un certificado.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la AC emisora.
8. Subject Public Key Info		Clave pública del sello, codificada de acuerdo con el algoritmo criptográfico.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. En RSA la longitud de la clave será 3072 bits. En ECC (Secp256r1) la longitud de la clave ECC P-256 bits
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto

Campo		Contenido	Oblig.	Crit.	Especificaciones
		contienen una clave pública particular y facilita la construcción de rutas de certificación.			(excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage			Sí	Sí	Normalizado en norma X509 y RFC 5280
	10.1. Digital Signature	1			Ver X509 y RFC 5280
	10.2. Content Commitment	1			Ver X509 y RFC 5280
	10.3. Key Encipherment	0			Ver X509 y RFC 5280
	10.4. Data Encipherment	0			Ver X509 y RFC 5280
	10.5. Key Agreement	0			Ver X509 y RFC 5280
	10.6. Key Certificate Signature	0			Ver X509 y RFC 5280
	10.7. CRL Signature	0			Ver X509 y RFC 5280
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	Si	Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
	11.1. id_kp_timeStamping	1.3.6.1.5.5.7.3.8	Sí		Sellado de tiempo
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	ETSI 319422 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance (0.4.0.1862.1.1)	Sello cualificado	Sí		Indica que el Sello es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente.
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del sello que se dispone de los datos de registro y otra información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".

Campo			Contenido	Oblig.	Crit.	Especificaciones
	12.3. QcType (0.4.0.1862.1.6)		Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		Indica que el certificado es de sello electrónico. Certificate for electronic seals as defined in Regulation (EU) No 910/2014
	12.4. QcPDS(0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_TSAFNMTG2_es.pdf,es},{https://www.cert.fnmt.es/pds/PDS_TSAFNMTG2_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS
	12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)		semanticsId-Legal (0.4.0.194121.1.2)	Sí		Indica que el campo subject sigue la semántica propuesta por la EN 319 412-1
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.27.1.0	Sí		Identificador de la política asociado a la DPC o PC
	13.2. Policy Qualifier Id					
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.2.2 User Notice	"Certificado cualificado de sello electrónico para TSU. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106–28009–Madrid–España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.3. Policy Identifier		QCP-l (0.4.0.194112.1.1)	Sí		Certificado cualificado de sello, acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al Sello.	Sí	No	
	14.1. Distribution Point 1		Punto de publicación de la CRL	Sí		Ruta donde reside la CRL

Campo		Contenido	Oblig.	Crit.	Especificaciones
		http://www.cert.fnmt.es/crlsactsafnmtclig2/CRL.crl			
15. Authority Info Access			Sí	No	
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		Acceso al servicio OCSP
	15.2. Acces Location 1	http://ocsptsaclig2.cert.fnmt.es/ocsptsacliG2/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
	15.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí		Emisor de la entidad emisora de certificados (AC Raíz)
	15.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACTSACLIG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
16. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	16.1. Subject Type	Entidad final (valor FALSE)			Con este Sello no se pueden emitir otros certificados
17. PrivateKey UsagePeriod				No	
	17.1. notBefore	Fecha inicial de validez de la clave privada	Si		
	17.2. notAfter	Fecha desde la cual el certificado no podrá emplearse para la emisión de nuevos sellos y será válido solo para validar sellos existentes.	Si		Cuatro años desde fecha de emisión