Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SERVICIOS DIGITALES E INNOVACIÓN
DEPARTAMENTO CERES

DOCUMENTO DE PERFILES DE LA AUTORIDAD DE CERTIFICACIÓN
AC REPRESENTACIÓN

Referencia:

Documento clasificado como: *Difusión Libre*

Contenido

1. INTRODUCCIÓN

En el presente documento se describe tanto el perfil del certificado de la CA encargada de la emisión de certificados de representante de persona jurídica, así como los perfiles de los certificados emitidos por dicha CA.

2. PERFILES

2.1. CA SUBORDINADA REPRESENTACIÓN

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.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organizational Unit	OU=AC RAIZ FNMT-RCM	Sí		UTF8 String.
5. Validity		Hasta 31/12/2029	Sí		
6. Subject			Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.

Campo		Contenido	Oblig.	Crit.	Especificaciones
	6.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String.
	6.3. Organizational Unit	OU=CERES	Sí		UTF8 String.
	6.4. CommonName	CN=AC Representación	Sí		UTF8 String.
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 CA para firmar el certificado de esta CA 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 CA Subordinada de Representación codificada según el estándar PKCS#1 de RSA.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits
9. Subject Key Identifier		Identificador de la clave pública de la CA 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	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. Certificate Policies		Política de certificación	Sí		

Campo			Contenido	Oblig.	Crit.	Especificaciones
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí		Atendiendo a la rfc5280: " *PolicyInformation SHOULD only contain an OID.* *In a CA certificate,these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }*"
	11.2. Policy Qualifier Id			Sí		
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí		UTF8 String.
12. CRL Distribution Point				Sí		
	12.1. Distribution Point 1		Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1).
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Authority Info Access				Sí	No	
	13.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	13.2. Access Location 1		http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	Sí		URL del servicio de OCSP.
	13.3. 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		Certificado de la CA emisora: De la rfc 5280: "the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."

Campo		Contenido	Oblig.	Crit.	Especificaciones
	13.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA raíz de la FNMT-RCM.
14. Basic Constraints			Sí	Sí	
	14.1. cA	Valor TRUE (CA)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."
	14.2. pathLenConstraint	0	Sí		Un pathLenConstraint de cero indica que no pueden existir más certificados de CA intermedios en la ruta de certificación.

2.2. PERFILES DE CERTIFICADOS DE ENTIDADES FINALES

2.2.1. Certificado de Sello de Entidad

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.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	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,
	4.3. Organization Unit	OU=CERES	Sí		UTF8 String,
	4.4. CommonName	CN=AC Representación			UTF8 String.
5. Validity		Variable	Sí		La duración será variable (1, 2 ó 3 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA

Campo		Contenido	Oblig.	Crit.	Especificaciones
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8 String, tamaño máximo 64 (rfc5280) OU=Departamento de Informática
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo:SN= Q0000000J
	6.6. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VATES-Q0000000J
	6.7. Common Name	Denominación del componente	Sí		UTF8String (rfc5280) tamaño máximo 64 caracteres. Por ejemplo:CN=Servicio de Registro
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	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 CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	No	Campo que contiene la clave pública del certificado.
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	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
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment	1	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	0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature	0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.

Campo			Contenido	Oblig.	Crit.	Especificaciones
	11.2. Document Signing		1.3.6.1.4.1.311.10.3.12	Sí		
	11.3. Adobe Authentic Documents Trust		1.2.840.113583.1.1.5	Sí		
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance (0.4.0.1862.1.1)		Certificado cualificado	Sí		Indicación de certificado cualificado
	12.2. 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. Certificate for electronic seals as defined in Regulation (EU) No 910/2014
	12.3. QcPDS(0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_es.pdf,es},{https://www.cert.fnmt.es/pds/PDS_en.pdf,en}	Sí		Lugar donde se encuentra la declaración PDS
	12.4. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		Número de años a partir de la caducidad del certificado 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
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.4	Sí		Identificador de la política
	13.2. Policy Qualifier Id			Sí		
		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 según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de FNMT-RCM con NIF: Q2826004J (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-organizatio(4) etsi(0) qualifed-certificate-policies(194112) policy-identifiers(1) qcp-legal(1)
14. Subject Alternative Names				Sí	No	

Campo			Contenido	Oblig.	Crit.	Especificaciones
	14.1. rfc822 Name		Correo electrónico del *Suscriptor*	Opcional		
	14.2. Directory Name					
		14.2.1 Entidad suscriptora	Nombre de la entidad propietaria del Sello Id Campo/Valor: 1.3.6.1.4.1.5734.1.6=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Ministerio de Economía y Hacienda
		14.2.2 NIF entidad	Número único de identificación de la entidad (NIF) Id Campo/Valor: 1.3.6.1.4.1.5734.1.7=<NIF entidad suscriptora>	Sí		UTF8 String, tamaño 9. Por ejemplo: 1.3.6.1.4.1.5734.1.7=Q2826004J
		14.2.3 Denominación del componente	Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí		
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Access Location 1		http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP
	16.3. 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		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: "*the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path*

Campo		Contenido	Oblig.	Crit.	Especificaciones
					that terminates at a point trusted by the certificate user."
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
17. Basic Contraints		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".	Sí	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.2.2. Certificado de Sello de Entidad con correo electrónico seguro

Perfil de certificado de sello de entidad que contiene la cuenta de correo electrónico del suscriptor y la extensión e-mail protection, habilitando su uso para poder cifrar y/o firmar digitalmente correos electrónicos de forma segura utilizando la tecnología S/MIME. Obsoleto desde el 15 de septiembre de 2024.

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.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	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,
	4.3. Organization Unit	OU=CERES	Sí		UTF8 String,
	4.4. CommonName	CN=AC Representación			UTF8 String.
5. Validity		Variable	Sí		La duración será variable (1, 2 ó 3 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid

Campo		Contenido	Oblig.	Crit.	Especificaciones
	6.3. Organization	Denominación (nombre "oficial" de la organización) del suscriptor	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
	6.4. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo:SN= Q0000000J
	6.5. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VATES-Q0000000J
	6.6. Common Name	Denominación (nombre "oficial" de la organización) del suscriptor	Sí		UTF8 String, tamaño máximo 64 (rfc5280). Por ejemplo: o=MINISTERIO DE ECONOMÍA
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	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 CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	No	Campo que contiene la clave pública del certificado.
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	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
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment	1	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	0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature	0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Email Protection	1.3.6.1.5.5.7.3.4	Sí		Ver X509, RFC 5280 y BRG S/MIME.

Campo			Contenido	Oblig.	Crit.	Especificaciones
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Si		Ver X509 y RFC 5280.
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance (0.4.0.1862.1.1)		Certificado cualificado	Sí		Indicación de certificado cualificado
	12.2. 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. Certificate for electronic seals as defined in Regulation (EU) No 910/2014
	12.3. QcPDS(0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_es.pdf,es},{https://www.cert.fnmt.es/pds/PDS_en.pdf,en}	Sí		Lugar donde se encuentra la declaración PDS
	12.4. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		Número de años a partir de la caducidad del certificado 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
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.5	Sí		Identificador de la política
	13.2. Policy Qualifier Id			Sí		
		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 según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de FNMT-RCM con NIF: Q2826004J (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-organizatio(4) etsi(0) qualifed-certificate-policies(194112) policy-identifiers(1) qcp-legal(1)
	13.4. Policy Identifier		2.23.140.1.5.2.1	Sí		Cumplimiento de BRG de CAB Forum OID de Organization-Validated, Legacy
14. Subject Alternative Names				Sí	No	

Campo			Contenido	Oblig.	Crit.	Especificaciones
	14.1. rfc822 Name		Correo electrónico del *Suscriptor*	Sí		
	14.2. Directory Name					
		14.2.1 Entidad suscriptora	Nombre de la entidad propietaria del Sello Id Campo/Valor: 2.5.4.10=<Entidad Suscriptora>	Sí		UTF8 String. Por ejemplo: 2.5.4.10=Ministerio de Economía y Hacienda
		14.2.2 Identificador con NIF entidad	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Sí		UTF8 String, tamaño 9. Por ejemplo: 2.5.4.97=VATES-Q2826004J
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Access Location 1		http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP
	16.3. 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		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: "*the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Access Location 2		http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la

Campo		Contenido	Oblig.	Crit.	Especificaciones
					ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
17. Basic Contraints		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".	Sí	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.2.3. Perfil de certificado de representante para administradores únicos y solidarios

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.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organizational Unit	OU=CERES	Sí		UTF8 String.
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String.
5. Validity		2 años	Sí		
6. Subject		Identificación/descripción del *Representante* y de la *Entidad representada*	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	6.2. Organization	Razón social de la *Entidad Representada*	Sí		UTF8 String, tamaño máximo 200. Por ejemplo: O=Entidad de pruebas
	6.3. OrganizationIdentifier	NIF de la *Entidad Representada*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. UTF8String (rfc5280). Ejemplo: organizationIdentifier= VATES-Q00000000J

Campo		Contenido	Oblig.	Crit.	Especificaciones
	6.4. CommonName	NIF, nombre y primer apellido del *Representante* y (R: NIF de la *Entidad representada).*	Sí		UTF8 String, tamaño máximo 126. Por ejemplo: CN=00000000T Juan Español (R: Q0000000J)
	6.5. Surname	Apellidos del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: SN=Español Español
	6.6. GivenName	Nombre de pila del *Representante*	Sí		UTF8 String, tamaño máximo 50. Por ejemplo: givenName=Juan
	6.7. SerialNumber	NIF del *Representante*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.8. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales.	Sí		UTF8String. Estará compuesto por la concatenación separada por comas de los siguientes datos registrales: - Registro - Hoja - Tomo y Folio o Identificador único Registral (IRUS) - Nº de inscripción - Fecha de inscripción Por ejemplo: 2.5.4.13=”Reg:XXX/Hoja: XXX/ Tomo: XXX/Folio: XXX/Fecha: dd/mm/yyyy/Incripción: XX” ó ”Reg:XXX/Hoja: XXX/ IRUS: XXX/Fecha: dd/mm/yyyy/Incripción: XX”
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 CA para firmar un certificado.	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 emisora.
8. Subject Public Key Info		Clave pública del *Firmante*, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits
9. Subject Key Identifier		Identificador de la clave pública del *Firmante*. 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	Sí	Normalizado en norma X509.
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.

Campo			Contenido	Oblig.	Crit.	Especificaciones
	10.3. Key Encipherment		1	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		0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature		0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
	11.2. Document Signing		1.3.6.1.4.1.311.10.3.12	Sí		
	11.3. Adobe Authentic Documents Trust		1.2.840.113583.1.1.5	Sí		
12. Qualified Certificate Statements			Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance		Certificado es cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcType		Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS		{https://www.cert.fnmt.es/pds/PDS_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_en.pdf (, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.4. QcEuRetentionPeriod		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante.
13. Certificate Policies			Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.1	Sí		Identificador de la política establecido por el Prestador.
	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 representante de p. jurídica (relación con AAPP y contratación). Sujeto a condiciones de uso según DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String.

Campo			Contenido	Oblig.	Crit.	Especificaciones
	13.3. Policy Identifier		0.4.0.194112.1.0			QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.4. Policy Identifier		2.16.724.1.3.5.8	Sí		Identificador de la política según normativa nacional.
14. Subject Alternative Names			Identificación/descripción del *Representante* y de la *Entidad representada*	Sí	No	
	14.1. rfc822 Name		Correo electrónico del *Representante*	Sí		
	14.2. Directory Name					
		14.2.1. Nombre	Nombre de pila del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.1=JUAN
		14.2.2. Apellido1	Primer apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
		14.2.3. Apellido2	Segundo apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.3 =ESPAÑOL
		14.2.4. NIF	NIF del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.4=IDCES-99999999R
		14.2.5. Razón Social	Razón social de la *Entidad Representada* 1.3.6.1.4.1.5734.1.6=Razón social	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Entidad de pruebas
		14.2.6. NIF de la entidad	NIF de la *Entidad Representada* 1.3.6.1.4.1.5734.1.7=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.7= VATES-Q00000000J
		14.2.7. Cargo / Poder	Cargo o poder del *Representante* dentro de la entidad 1.3.6.1.4.1.5734.1.20 =Cargo	Sí		UTF8 String. Dos posibles valores: - administrador único - administrador solidario Por ejemplo: 1.3.6.1.4.1.5734.1.20 =Administrador único

Campo		Contenido	Oblig.	Crit.	Especificaciones
15. CRL Distribution Point			Sí	No	
	15.1. Distribution Point 1	Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2	Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2). <nnn> es el identificador de la CRL particionada concreta donde se halla el certificado.
16. Authority Info Access			Sí	No	
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Access Location 1	http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP
	16.3. 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		Certificado de la CA emisora: De la rfc 5280: "the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de Representación.
17. 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".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. cA	Valor FALSE (entidad final)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

2.2.4. Perfil de representante de persona jurídica

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.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		String UTF8 (40). Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	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 Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organizational Unit	OU=CERES	Sí		UTF8 String.
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String.
5. Validity		2 años	Sí		
6. Subject		Identificación/descripción del *Representante* y de la *Entidad representada*	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	6.2. Organization	Razón social de la *Entidad Representada*	Sí		UTF8 String, tamaño máximo 200. Por ejemplo: O=Entidad de pruebas
	6.3. OrganizationIdentifier	NIF de la *Entidad Representada*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. UTF8String (rfc5280). Ejemplo: organizationIdentifier= VATES-Q00000000J

Campo		Contenido	Oblig.	Crit.	Especificaciones
	6.4. CommonName	NIF, nombre y primer apellido del *Representante* y (R: NIF de la *Entidad representada).*	Sí		UTF8 String, tamaño máximo 126. Por ejemplo: CN=00000000T Juan Español (R: Q0000000J)
	6.5. Surname	Apellidos del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: SN=Español Español
	6.6. GivenName	Nombre de pila del *Representante*	Sí		UTF8 String, tamaño máximo 50. Por ejemplo: givenName=Juan
	6.7. SerialNumber	NIF del *Representante*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.8. Description	Identificador de los documentos públicos que acreditan las facultades del *Representante* 2.5.4.13=Id de documentos públicos	Sí		UTF8 String, tamaño máximo 100 caracteres. Por ejemplo: 2.5.4.13= "Ref: XXXXX/YYYYY/ZZZZZ/12345678/20151212120000"
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 CA para firmar un certificado.	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 emisora.
8. Subject Public Key Info		Clave pública del *Firmante*, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits
9. Subject Key Identifier		Identificador de la clave pública del *Firmante*. 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	Sí	Normalizado en norma X509.
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment	1	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	0	Sí		Ver X509 y RFC 5280.

Campo			Contenido	Oblig.	Crit.	Especificaciones
	10.7. CRL Signature		0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
	11.2. Document Signing		1.3.6.1.4.1.311.10.3.12	Sí		
	11.3. Adobe Authentic Documents Trust		1.2.840.113583.1.1.5	Sí		
12. Qualified Certificate Statements			Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance		Certificado es cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcType		Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS		{https://www.cert.fnmt.es/pds/PDS_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.4. QcEuRetentionPeriod		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante.
13. Certificate Policies			Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.2	Sí		Identificador de la política establecido por el Prestador.
	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 representante de p. jurídica en sus relaciones con las AAPP. Sujeto a condiciones de uso según la DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String.
	13.3. Policy Identifier		0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.4. Policy Identifier		2.16.724.1.3.5.8	Sí		Identificador de la política según normativa nacional.
14. Subject Alternative Names			Identificación/descripción del *Representante* y de la *Entidad*	Sí	No	

Campo			Contenido	Oblig.	Crit.	Especificaciones
	14.1. rfc822 Name		Correo electrónico del *Representante*	Sí		
	14.2. Directory Name					
		14.2.1. Nombre	Nombre de pila del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.1=JUAN
		14.2.2. Apellido1	Primer apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
		14.2.3. Apellido2	Segundo apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.3 =ESPAÑOL
		14.2.4. NIF	NIF del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.4=IDCES-99999999R
		14.2.5. Razón Social	Razón social de la *Entidad Representada* 1.3.6.1.4.1.5734.1.6=Razón social	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Entidad de pruebas
		14.2.6. NIF de la entidad	NIF de la *Entidad Representada* 1.3.6.1.4.1.5734.1.7=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.7= VATES-Q00000000J
15. CRL Distribution Point				Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2). <nnn> es el identificador de la CRL particionada concreta donde se halla el certificado.
16. Authority Info Access				Sí	No	

Campo		Contenido	Oblig.	Crit.	Especificaciones
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Access Location 1	http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP.
	16.3. 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		Certificado de la CA emisora: De la rfc 5280: "the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de Representación.
17. 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".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. cA	Valor FALSE (entidad final)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."

2.2.5. Perfil de certificado de representante de entidad sin personalidad jurídica

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.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		String UTF8 (40). Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	4.2. Organization	Denominación (nombre "oficial" de la organización) del *Prestador de Servicios de Confianza* (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String.
	4.3. Organization Unit	OU=CERES	Sí		UTF8 String.
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String.
5. Validity		2 años	Sí		
6. Subject		Identificación/descripción del *Representante* y de la *Entidad representada*	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString.
	6.2. Organization	Razón social de la *Entidad Representada*	Sí		UTF8 String, tamaño máximo 200. Por ejemplo: O=Entidad de pruebas
	6.3. OrganizationIdentifier	NIF de la *Entidad Representada*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. UTF8String (rfc5280). Ejemplo: organizationIdentifier= VATES-Q00000000J
	6.4. CommonName	NIF, nombre y primer apellido del *Representante* y (R: NIF de la *Entidad representada).*	Sí		UTF8 String, tamaño máximo 126. Por ejemplo:

Campo		Contenido	Oblig.	Crit.	Especificaciones
					CN=00000000T Juan Español (R: Q0000000J)
	6.5. Surname	Apellidos del *Representante*	Sí		UTF8String (rfc5280). Por ejemplo: SN=Español Español
	6.6. GivenName	Nombre de pila del *Representante*	Sí		UTF8 String, tamaño máximo 50. Por ejemplo: givenName=Juan
	6.7. SerialNumber	NIF del *Representante*	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.8. Description	Identificador de los documentos públicos que acreditan las facultades del *Representante* 2.5.4.13=Id de documentos públicos	Sí		UTF8 String, tamaño máximo 100 caracteres. Por ejemplo: 2.5.4.13= "Ref: XXXXX/YYYYY/ZZZZZ/12345678/20151212 120000"
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 CA para firmar un certificado.	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 emisora.
8. Subject Public Key Info		Clave pública del *Firmante*, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits.
9. Subject Key Identifier		Identificador de la clave pública del *Firmante*. 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	Sí	Normalizado en norma X509.
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment	1	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	0	Sí		Ver X509 y RFC 5280.
	10.7. CRL Signature	0	Sí		Ver X509 y RFC 5280.

Campo			Contenido	Oblig.	Crit.	Especificaciones
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
	11.2. Document Signing		1.3.6.1.4.1.311.10.3.12	Sí		
	11.3. Adobe Authentic Documents Trust		1.2.840.113583.1.1.5	Sí		
12. Qualified Certificate Statements			Extensiones cualificadas.		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance		Certificado es cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcType		Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS		{https://www.cert.fnmt.es/pds/PDS_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.4. QcEuRetentionPeriod		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra información relevante.
13. Certificate Policies			Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.3	Sí		Identificador de la política establecido por el Prestador.
	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 representante de entidad sin person. jurídica (relación con AAPP). Sujeto a condiciones de uso según DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String.
	13.3. Policy Identifier		0.4.0.194112.1.0	Si		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.4. Policy Identifier		2.16.724.1.3.5.9	Sí		Identificador de la política según normativa nacional.
14. Subject Alternative Names			Identificación/descripción del *Representante* y de la *Entidad*	Sí	No	
	14.1. rfc822 Name		Correo electrónico del *Representante*	Sí		
	14.2. Directory Name					

Campo			Contenido	Oblig.	Crit.	Especificaciones
		14.2.1. Nombre	Nombre de pila del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.1=JUAN
		14.2.2. Apellido1	Primer apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
		14.2.3. Apellido2	Segundo apellido del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.3 =ESPAÑOL
		14.2.4. NIF	NIF del *Representante* Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.4=IDCES-99999999R
		14.2.5. Razón Social	Nombre de la *Entidad sin personalidad jurídica* representada 1.3.6.1.4.1.5734.1.6=Razón social	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.6=Entidad de pruebas
		14.2.6. NIF de la entidad	NIF de la *Entidad sin personalidad jurídica* 1.3.6.1.4.1.5734.1.7=NIF	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.7= VATES-Q00000000J
		14.2.7. Tipo de ESPJ	Tipo de *Entidad sin personalidad jurídica* 1.3.6.1.4.1.5734.1.22=Tipo de entidad.	Sí		UTF8 String. Valores que puede tomar: RA - Comunidad de bienes RB - Comunidad propietarios propiedad horizontal RC - Comunidad titular montes vecinales RD - Sociedad civil RE - Herencia yacente RF - Fondo de inversión RG - Unión temporal de empresas RH - Fondo de capital-riesgo RI - Fondo de pensiones RJ - Fondo de regulación mercado hipotecario RK - Fondo de titulación hipotecaria RL - Fondo de titulación activos RM - Fondo de garantía de inversiones RN - Otros entes sin personalidad jurídica

Campo			Contenido	Oblig.	Crit.	Especificaciones
						Por ejemplo: 1.3.6.1.4.1.5734.1.22=RA – Comunidad de Bienes
15. CRL Distribution Point				Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx> es el identificador de la CRL particionada concreta donde se halla el certificado.
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2). <nnn> es el identificador de la CRL particionada concreta donde se halla el certificado.
16. Authority Info Access				Sí	No	
	16.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Access Location 1		http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP
	16.3. 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		Certificado de la CA emisora: De la rfc 5280: "the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."
	16.4. Access Location 2		http://www.cert.fnmt.es/certs/ACREP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de Representación.
17. 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".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.

Campo		Contenido	Oblig.	Crit.	Especificaciones
	17.1. cA	Valor FALSE (entidad final)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."