DIRECCIÓN DE SISTEMAS DE INFORMACIÓN

DEPARTAMENTO CERES

DEFINICIÓN DE PERFILES AC REPRESENTACIÓN

	NOMBRE	FECHA
Elaborado por:	Área Técnica	08/03/2016
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	08/03/2016	Creación del documento	Área Técnica
2.0	09/03/2016	Corrección erratas en la columna “especificaciones”.	Área Técnica
3.0	10/03/2016	Corrección erratas en la columna “especificaciones”.	Área Técnica
4.0	30/03/2016	Alineación con borrador de perfiles de la DTIC (OID políticas).	Área Técnica
5.0	01/04/2016	Modificación del campo User notice del certificado de representante de ESPJ.	Área Técnica

6.0	04/04/2016	Adaptación a propuesta perfil de la DTIC	Área Técnica
7.0	11/04/2016	Corrección enlaces a PDS y eliminación de anyEKU	Área Técnica
8.0	14/04/2016	Modificado UserNotice	Área Técnica

Referencia:
Documento clasificado como: *Público*

Índice

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 de certificado

1.1. Perfil certificado AC 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.
	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.

Campo			Contenido	Oblig	Crit	Especificaciones
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		
	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	

Campo		Contenido	Oblig	Crit	Especificaciones
	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. Acces 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."
	13.4. Acces 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.

1.2. Perfil 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		UTF8String (rfc5280). 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 NIF de la *Entidad representada*.	Sí		UTF8StringPor 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		UTF8String (rfc5280). 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

Campo		Contenido	Oblig	Crit	Especificaciones
	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 - Folio - 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"
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.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Email Protection	1.3.6.1.5.5.7.3.4	Sí		Ver X509 y RFC 5280.
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
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.

Campo			Contenido	Oblig	Crit	Especificaciones
	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.
	13.1.1. Policy Qualifier Id					
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2. User Notice	Certificado electrónico de representante de persona jurídica en sus relaciones con las AAPP o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario	Sí		UTF8 String.
	13.2. Policy Identifier		0.4.0.194112.1.0			QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.3. 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
15. CRL Distribution Point				Sí	No	

Campo		Contenido	Oblig	Crit	Especificaciones
	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 del servicio LDAP 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. Acces 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. Acces 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."

1.3. Perfil certificado 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		UTF8String (rfc5280). 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-Q0000000J
	6.4. CommonName	NIF, nombre y primer apellido del *Representante* y NIF de la *Entidad representada*.	Sí		UTF8StringPor 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		UTF8String (rfc5280). 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.

Campo			Contenido	Oblig	Crit	Especificaciones
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.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí		Ver X509 y RFC 5280.
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
	11.3.					
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.
	13.1.1. Policy Qualifier Id					
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.

Campo			Contenido	Oblig	Crit	Especificaciones
		13.1.1.2. User Notice	Certificado electrónico de representante de persona jurídica en sus relaciones con las AAPP, Entidades y Organismos Públicos vinculados o dependientes de las mismas	Sí		UTF8 String.
	13.2. Policy Identifier		0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.3. 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	
	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 (ARL) http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí		Ruta del servicio LDAP 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. Acces Location 1		http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí		URL del servicio de OCSP.

Campo		Contenido	Oblig	Crit	Especificaciones
	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. Acces 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."

1.4.Perfil 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		UTF8String (rfc5280). 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 NIF de la *Entidad representada*	Sí		UTF8StringPor 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		UTF8String (rfc5280). 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	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

			privada utilizada por la CA para firmar un certificado.			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.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí		Ver X509 y RFC 5280.
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí		Ver X509 y RFC 5280.
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
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.
	13.1.1. Policy Qualifier Id					
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2. Use	Certificado electrónico de representante de entidad sin personalidad jurídica para el	Sí		UTF8 String.

		r Notice	ámbito tributario y cualquier otro previsto por la legislación vigente			
	13.2. Policy Identifier		0.4.0.194112.1.0			QCP-n: certificate policy for EU qualified certificates issued to natural persons.
	13.3. 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					
		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 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 (ARL) http://www.cert.fnmt.es/crlsr	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2). <nnn> es el identificador de la CRL

		ep/CRLnnn.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. Acces 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. Acces 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."

Anexo. Propuesta DTIC de los perfiles de certificados de representante de abril 2016

- *Codificación del atributo Common Name*

Se propone una codificación del campo Common Name que permite al usuario identificar el certificado como uno de representación, distinguiéndolo de uno de Persona Física básico, a través del literal 'R: '. Así mismo se permite identificar la Persona Jurídica representada para facilitar la selección de certificado en caso de una Persona Física que represente a varias Personas Jurídicas.
El campo tiene un tamaño máximo de 64 caracteres según la RFC 5280.

Campo	***Contenido***	***Ejemplo***	***tamaño ****
NIF	*número DNI/NIE*	*12345678Z*	*10*
Nombre	*Tal y como figura en el DNI/NIE*	*Pedro Antonio*	
Apellido 1	*Tal y como figura en el DNI/NIE*	*López*	
Literal	*(R:*		*4*
NIF de la empresa	*NIF de la empresa, tal como figura en los registros oficiales.*	*B0085974Z*	*9*
Literal	*)*		*2*
Literal	***AUTENTIC, FIRMA o CIFRADO***		*8*

**(contando espacio en blanco posterior)*