



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

DEFINICIÓN DE PERFILES AC REPRESENTACIÓN

	NOMBRE	FECHA
Elaborado por:		
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	Descripción	Autor
1.0			
1.1		Modificación del texto tipo entidad en el perfil de certificado de entidad sin personalidad jurídica	
1.2		Certificados de PJ y ESPJ pasan a ser reconocidos	
1.3		Actualización de perfiles conforme a los estándares ETSI (mandato M460) y directrices de la DTIC.	

Referencia:

Documento clasificado como: *Público*

Índice

Introducción	4
Perfil certificado de representación para administradores únicos y solidarios	5
Diferencias entre los certificados de persona jurídica y los de nuevos de representante para administradores únicos y solidarios	8
1. 3. Signature Algorithm	8
2. 4. Issuer Distinguish Name	8
3. 6. Subject	8
4. 8. Subject Public Key Info	9
5. 10. Key Usage	9
6. 11. Extended Key Usage	9
7. 12. Qualified Certificate Statements	9
8. 13. Certificate Policies	9
9. 14. Subject Alternative Names	10
10. 15. CRL Distribution Point	10
11. 16. Authority Info Access	11
Perfil certificado de representante de persona jurídica	12
Diferencias entre los certificados de persona jurídica y los nuevos certificados de representante de persona jurídica	16
12. 3. Signature Algorithm	16
13. 4. Issuer Distinguish Name	16
14. 6. Subject	16
15. 8. Subject Public Key Info	16
16. 10. Key Usage	16
17. 11. Extended Key Usage	17
18. 12. Qualified Certificate Statements	17
19. 13. Certificate Policies	17
20. 14. Subject Alternative Names	17

21. 15. CRL Distribution Point	17
22. 16. Authority Info Access	18
Perfil certificado de representante de entidad sin personalidad jurídica.....	19
Diferencias entre los certificados de persona jurídica y los nuevos certificados de representante de entidad sin personalidad jurídica	22
23. 3. Signature Algorithm	22
24. 4. Issuer Distinguish Name	22
25. 6. Subject.....	23
26. 8. Subject Public Key Info	23
27. 10. Key Usage	23
28. 11. Extended Key Usage	23
29. 12. Qualified Certificate Statements	23
30. 13. Certificate Policies	23
31. 14. Subject Alternative Name	24
32. 15. CRL Distribution Point	24
33. 16. Authority Info Access	25
Formas de Validación	26
CRLs	26
LDAP	26
URL	27
OCSP	27
Certificados.....	27

Introducción

Este documento recoge los diferentes campos que componen los perfiles de los certificados de políticas de persona jurídica, persona jurídica de representación y entidad sin representación jurídica, y el significado de cada uno de ellos.

Además plasma las diferencias entre los campos de los antiguos certificados de persona jurídica de la CA FNMT Clase 2 CA y los nuevos.

Los certificados que abarca el documento son:

- Certificado de representante de persona jurídica en software.
- Certificado de representante para administradores únicos y solidarios en software.
- Certificados de representante de entidad sin personalidad jurídica en software.

Los campos que se modifican se marcan en azul en las tablas, al final del perfil se explica la diferencia respecto al perfil anterior.

Para el correcto funcionamiento de las aplicaciones en los clientes con los nuevos certificados, es decir, evitar avisos de falta de confianza en los nuevos certificados, es necesario instalar/distribuir el nuevo certificado de la CA intermedia. Lo más conveniente es instalarlo en el servidor web que está ofreciendo el servicio a los usuarios para que lo adquieran en la sesión.

La cadena completa de certificados de confianza de los nuevos certificados puede encontrarla en:

Raíz:

https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Raiz_FNMT-RCM_SHA256.cer/b1447e06-9927-45b7-92cc-8690edd7562d

Subordinada:

https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Representacion.cer

Perfil certificado de representación 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 certificado 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, 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 128 (rfc5280)
	4.3. Organizational Unit	OU=CERES	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
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 1er 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	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/Inscripción: 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 suscriptor, 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 suscriptor o poseedor de claves. 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
	Email Protection	1.3.6.1.5.5.7.3.4	Sí		Ver X509 y RFC 5280
	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	1.3.6.1.4.1.5734.3.11.1	Sí		Identificador de la política
	13.1.1. Policy Qualifier Id				
	13.1.2. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
	13.1.3. User Notice	Certificados electrónicos destinados a personas jurídicas en sus relaciones con las AAPP o en la	Sí		UTF8 String.

			contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario			
	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 suscriptor	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	
	15.1.	Distribution Point 1	Punto de distribución 1 de la CRL ldap://ldapprep.cert.fnmt.es/CN=CRL<xxx>,OU=AC%20Representacion,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		UTF8String 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		UTF8String. 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.	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	Sí		Certificado de la CA emisora: De la rfc 5280: "the idad- calssuers OID is used when the additional information lists

		necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)			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 r5280: "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."

Diferencias entre los certificados de persona jurídica y los de nuevos de representante para administradores únicos y solidarios

3. Signature Algorithm

El algoritmo de firma pasa de ser SHA1 a ser SHA256. En nuevo O.I.D. para este campo es 1.2.840.113549.1.1.11

4. Issuer Distinguish Name

Pasa de ser

C=ES, O=FNMT, OU=FNMT CLASE 2 CA

A ser

C = ES, O = FNMT-RCM, OU = Ceres, CN = C Representación

6. Subject

Pasa de ser

CN= ENTIDAD e - CIF 12345678B NOMBRE APELLIDO1PF APELLIDO2PF PRUEBASPF - 00000000T
OU = 500070076
OU = FNMT Clase 2 CA
O = FNMT
C = ES

A ser

Description = Reg:99999 /Hoja:999999 /Tomo:9 /Folio:999 /Fecha:01/01/2000
/Inscripción:99
SERIALNUMBER = IDCES-00000000T
G = PRUEBASPF
SN = APELLIDO1PF APELLIDO2PF
CN = 00000000T PRUEBASPF APELLIDO1PF (R: A999999989)
2.5.4.97 = VATES-A999999989
O = ENTIDAD 1 PRUEBAS
C = ES

8. Subject Public Key Info

Pasa de ser de 1024 a 2048.

10. Key Usage

Firma Digital y Cifrado de Clave y se añade Sin Repudio.

11. Extended Key Usage

Correo Seguro y Autenticación del Cliente.

12. Qualified Certificate Statements

Certificado Reconocido (Cualificado), se añade el tiempo de Retención 15 años, la localización de las PDS y que el certificado esta emitido para realizar firmas electrónicas.

13. Certificate Policies

El OID de las políticas de certificación (Policy Identifier) pasa de 1.3.6.1.4.1.5734.3.7 a 1.3.6.1.4.1.5734.3.11.1

El uso del certificado pasa a ser:

“Certificados electrónicos destinados a personas jurídicas 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”

Además se añaden las políticas 0.4.0.194112.1.0 que indica que es un certificado de persona física cualificado para la UE y 2.16.724.1.3.5.8 que se usa como identificador de política relativo a normativa nacional.

14. Subject Alternative Names

Se añaden un nuevo elemento:

- Cargo/Poder (1.3.6.1.4.1.5734.1.20) que puede tomar dos valores
 - administrador único
 - administrador solidario

Y se modifican dos existentes.

El 1.3.6.1.4.1.5734.1.4 añade un identificador del tipo de documento IDCES-00000000T

El 1.3.6.1.4.1.5734.1.7 añade un identificador del tipo de documento VATES-A99999989

15. CRL Distribution Point

Pasa del formato

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección del directorio:

CN=CRL***

OU=FNMT Clase 2 CA

O=FNMT

C=ES

Al formato

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección URL=

ldap://ldaprep.cert.fnmt.es/CN=CRL***,OU=AC%20Representacion,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

Dirección URL=

http://www.cert.fnmt.es/crlsrep/CRL***.cr

Indicar que el acceso al directorio es abierto, no se requiere de autenticación. Se crea una nueva rama en el LDAP OU=CERES, CN=AC Representacion.

Los nuevos certificados además pueden validarse a través de http.

16. Authority Info Access

Se añade al certificado, no está presente en los certificados de clase 2. Contiene información de validación OCSP de los certificados, así como información de localización del certificado de la CA emisora del certificado.

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 certificado 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 certificación (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organizational Unit	OU=CERES	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
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 1er 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.
8.	Subject Public Key Info	Clave pública del suscriptor, codificada de acuerdo con el algoritmo criptográfico.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave.

9. Subject Key Identifier		En este caso RSA Encryption. Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí		La longitud de la clave será 2048 bits 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
	Email Protection	1.3.6.1.5.5.7.3.4	Opcional		Ver X509 y RFC 5280
	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		1.3.6.1.4.1.5734.3.11.2	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.
		13.1.1.2. User Notice	Certificados electrónicos destinados a personas jurídicas 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 suscriptor	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://ldapprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		UTF8String 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 ep/CRLnnn.crl	Sí		UTF8String. 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://ocspcert.fnmt.es/ocspcert/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 idad- 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	Sí	Sí	De la rfc5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.

		las cadenas de certificación".			
	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."

Diferencias entre los certificados de persona jurídica y los nuevos certificados de representante de persona jurídica

3. Signature Algorithm

El algoritmo de firma pasa de ser SHA1 a ser SHA256. En nuevo O.I.D. para este campo es 1.2.840.113549.1.1.11

4. Issuer Distinguish Name

Pasa de ser

C=ES, O=FNMT, OU=FNMT CLASE 2 CA

A ser

C = ES, O = FNMT-RCM, OU = Ceres, CN = C Representación

6. Subject

Pasa de ser

CN= ENTIDAD e - CIF 12345678B NOMBRE APELLIDO1PF APELLIDO2PF PRUEBASPF - 00000000T

OU = 500070076

OU = FNMT Clase 2 CA

O = FNMT

C = ES

A ser

Description = Ref:MVBZ_CE/MVBZ_CE0001/MVBZ_CE0001_P001/6/12042016140827

SERIALNUMBER = IDCES-00000000T

G = PRUEBASPF

SN = APELLIDO1PF APELLIDO2PF

CN = 00000000T PRUEBASPF APELLIDO1PF (R: A99999989)

2.5.4.97 = VATES-A99999989

O = ENTIDAD 1 PRUEBAS

C = ES

8. Subject Public Key Info

Pasa de ser de 1024 a 2048.

10. Key Usage

Firma Digital, Cifrado de Clave y se añade Sin Repudio.

11. Extended Key Usage

Correo Seguro y Autenticación del Cliente.

12. Qualified Certificate Statements

Se añade al certificado, no está presente en los certificados de clase 2. Certificado Reconocido (Cualificado), se añade el tiempo de Retención 15 años, la localización de las PDS y que el certificado esta emitido para realizar firmas electrónicas.

13. Certificate Policies

El OID de las políticas de certificación (Policy Identifier) pasa de 1.3.6.1.4.1.5734.3.7 a 1.3.6.1.4.1.5734.3.11.2

El uso del certificado pasa a ser:

“Certificados electrónicos destinados a personas jurídicas en sus relaciones con las Administraciones Públicas, Entidades y Organismos Públicos vinculados o dependientes de las mismas”.

Además se añaden las políticas 0.4.0.194112.1.0 que indica que es un certificado de persona física cualificado para la UE y 2.16.724.1.3.5.8 que se usa como identificador de política relativo a normativa nacional.

14. Subject Alternative Names

El 1.3.6.1.4.1.5734.1.4 añade un identificador del tipo de documento IDCES-00000000T

El 1.3.6.1.4.1.5734.1.7 añade un identificador del tipo de documento VATES-A99999989

15. CRL Distribution Point

Pasa del formato

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección del directorio:

CN=CRL***

OU=FNMT Clase 2 CA

O=FNMT

C=ES

Al formato

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección URL=

ldap://ldaprep.cert.fnmt.es/CN=CRL***,OU=AC%20Representacion,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

Dirección URL=

http://www.cert.fnmt.es/crlsrep/CRL***.cr

Indicar que el acceso al directorio es abierto, no se requiere de autenticación. Se crea una nueva rama en el LDAP OU=CERES, CN=AC Representacion.

Los nuevos certificados además pueden validarse a través de http.

16. Authority Info Access

Se añade al certificado, no está presente en los certificados de clase 2. Contiene información de validación OCSP de los certificados, así como información de localización del certificado de la CA emisora del certificado.

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 certificado 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 certificación (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organization Unit	OU=CERES	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. CommonName	CN=AC Representación	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
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 1er apellido del Representante y NIF de la Entidad representada.	Sí		UTF8String Por ejemplo: CN=00000000T Juan Español (R: Q00000000J)
	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/ZZZZ/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	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).

		para firmar un certificado.			Coincide con el campo Subject Key Identifier de la AC emisora.
8.	Subject Public Key Info	Clave pública del suscriptor, 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 suscriptor o poseedor de claves. 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
	Email Protection	1.3.6.1.5.5.7.3.4	Opcional		Ver X509 y RFC 5280
	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.
	17.1.1. Policy Qualifier Id				17.1.2. Policy Qualifier Id
	13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		
	13.1.1.1. 13.1.1.2. User Notice	Certificados electrónicos destinados a personas jurídicas 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		
	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

			Identificación/descripción del suscriptor	Sí	No	normativa nacional.
14. Subject Alternative Names						
	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
	14.2.8. Id de documentos públicos		Identificador de los documentos públicos que acreditan las facultades del Representante 1.3.6.1.4.1.5734.1.46=Id de documentos públicos	Sí		UTF8 String, tamaño máximo 100 caracteres. Por ejemplo: 1.3.6.1.4.1.5734.1.46=XXXXX/YYYYY/ZZZZZ/12345678/20151212120000
15. CRL Distribution Point						
	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?objectclasses=cRLDistributionPoint	Sí		UTF8String 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/crlsrp/CRLnnn.crl	Sí		UTF8String. 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. Access Location 1	http://ocspcert.fnmnt.es/ocspcert/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 idad- 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.fnmnt.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 rfc 5280: "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."

Diferencias entre los certificados de persona jurídica y los nuevos certificados de representante de entidad sin personalidad jurídica

3. Signature Algorithm

El algoritmo de firma pasa de ser SHA1 a ser SHA256. En nuevo O.I.D. para este campo es 1.2.840.113549.1.1.11

4. Issuer Distinguish Name

Pasa de ser

C=ES, O=FNMT, OU=FNMT CLASE 2 CA

A ser

C = ES, O = FNMT-RCM, OU = Ceres, CN = C Representación

6. Subject

Pasa de ser

CN= ENTIDAD e - CIF 12345678B NOMBRE APELLIDO1PF APELLIDO2PF PRUEBASPF -
00000000T
OU = 500070076
OU = FNMT Clase 2 CA
O = FNMT
C = ES

A ser

Description = Ref:MVBZ_CE/MVBZ_CE0001/MVBZ_CE0001_P001/6/12042016140827
SERIALNUMBER = IDCES-00000000T
G = PRUEBASPF
SN = APELLIDO1PF APELLIDO2PF
CN = 00000000T PRUEBASPF APELLIDO1PF (R: A999999989)
2.5.4.97 = VATES-A999999989
O = ENTIDAD 1 PRUEBAS
C = ES

8. Subject Public Key Info

Pasa de ser de 1024 a 2048.

10. Key Usage

Firma Digital, Cifrado de Clave y se añade Sin Repudio.

11. Extended Key Usage

Correo Seguro y Autenticación del Cliente.

12. Qualified Certificate Statements

Se añade al certificado, no está presente en los certificados de clase 2. Certificado Reconocido (Cualificado), se añade el tiempo de Retención 15 años, la localización de las PDS y que el certificado esta emitido para realizar firmas electrónicas.

13. Certificate Policies

El OID de las políticas de certificación (Policy Identifier) pasa de 1.3.6.1.4.1.5734.3.7 a 1.3.6.1.4.1.5734.3.11.3

El uso del certificado pasa a ser:

“Certificados electrónicos destinados a entidades sin personalidad jurídica en sus relaciones con las Administraciones Públicas, Entidades y Organismos Públicos vinculados o dependientes de las mismas”.

Además se añaden las políticas 0.4.0.194112.1.0 que indica que es un certificado de persona física cualificado para la UE y 2.16.724.1.3.5.8 que se usa como identificador de política relativo a normativa nacional.

14. Subject Alternative Name

Tipo de entidad de personalidad Jurídica (1.3.6.4.1.5734.1.22)

El 1.3.6.1.4.1.5734.1.4 añade un identificador del tipo de documento IDCES-00000000T

El 1.3.6.1.4.1.5734.1.7 añade un identificador del tipo de documento VATES-A99999989

15. CRL Distribution Point

Pasa del formato

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección del directorio:

CN=CRL***

OU=FNMT Clase 2 CA

O=FNMT

C=ES

Al formato

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección URL=

ldap://ldaprep.cert.fnmt.es/CN=CRL***,OU=AC%20Representacion,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

Dirección URL=

http://www.cert.fnmt.es/crlsrep/CRLxxx.cr

Indicar que el acceso al directorio es abierto, no se requiere de autenticación. Se crea una nueva rama en el LDAP OU=CERES, CN=AC Representacion.

Los nuevos certificados además pueden validarse a través de http.

16. Authority Info Access

Se añade al certificado, no está presente en los certificados de clase 2. Contiene información de validación OCSP de los certificados, así como información de localización del certificado de la CA emisora del certificado.

Formas de Validación

A continuación se enumeran los mecanismos de validación de los certificados de la AC Representación.

Estos mecanismos son abiertos no requieren de permiso/autorización para ser accedidos.

La validación de estos certificados puede realizarse a través de:

- CRLs
 - LDAP
 - URL
- OCSP

Al final del documento vienen las URLs de los certificados necesarios para validar tanto las CRLs como las respuestas OCSP.

CRLs

Para los certificados AC Representación se utilizan CRLs fraccionadas, por cada 750 certificados se genera una nueva CRL.

Por ejemplo, al emitir el certificado 1 se genera la CRL1. En ella se reserva espacio para incluir la información de revocación de los 750 primeros certificados. Al emitir el certificado 751 se crea la CRL2 donde se almacenará el estado de revocación de los siguientes 750 certificados.

Las CRLs son publicadas en un directorio LDAP.

La información relativa a estas CRLs se encuentra en el CRLDistributionPoint (Punto de Distribución de CRL)

LDAP

El LDAP de la CA de Representación se encuentra:

- Hosts: ldarep.cert.fnmt.es
- Puerto: 389.
- SearchBase: CN=AC Representacion, OU=CERES, O=FNMT-RCM, C=ES

La estructura completa de acceso a la CRL a través del LDAP es:

ldap://ldapusu.cert.fnmt.es/cn=CRL***,cn=AC%20Representacion,ou=CERES,o=FNMT-RCM,c=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

*** es el número de la CRL.

URL

Las CRLs también son accesibles a través de la web, la dirección es:

http://www.cert.fnmt.es/crlsrep/CRL***.crl

*** es el número de la CRL.

OCSP

El acceso al servidor de la AC Representación se realiza mediante petición sin firma.

La URL de acceso al OCSP es <http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder>

Certificados

Para validar las CRLs se necesitan los siguientes certificados:

- Validar Respuestas OCSP:
- Validar firmas de CRLs y certificados de firma de OCSP:

Raíz:

https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Raiz_FNMT-RCM_SHA256.cer/b1447e06-9927-45b7-92cc-8690edd7562d

Subordinada:

https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Representacion.cer