



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

Definición Perfiles de Certificado Emitidos por AC FNMT Usuarios (CA Personas Físicas)

	NOMBRE	FECHA
Elaborado por:	Soporte Técnico	04/12/14
Revisado por:	Soporte Técnico	04/12/14
Aprobado por:	Soporte Técnico	04/12/14

HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	Descripción	Autor
1.0	04/12/14	Creación del documento	Soporte Técnico
1.1	09/12/14	Revisión del documento	Soporte Técnico
1.2	10/12/2016	Adaptación a eIDAS	Soporte Técnico

Referencia:

Documento clasificado como: *Público*

Índice

Introducción	3
Perfil Certificado Persona Física en Software.....	4
Diferencias entre los nuevos certificados de Persona física y los de la nueva CA.	7
1. 3. Signature Algorithm	7
2. 4. Issuer Distinguish Name	7
3. 5. Validity.....	7
4. 6. Subject.....	7
5. 8. Subject Public Key Info	7
6. 10. Key Usage	8
7. 11. Extended Key Usage	8
8. 12. Qualified Certificate Statements	8
9. 13. Certificate Policies	8
10. 15. CRL Distribution Point	8
11. 16. Authority Info Access	9
Adaptación a eIDAS	10
12. 6. Subject.....	10
13. 12. Qualified Certificate Statements	10
Perfil Final Adaptado a eIDAS.....	11
Formas de Validación	15
CRLs	15
LDAP	15
OCSP	16
Certificados.....	16

Introducción

Este documento recoge los diferentes campos que componen los perfiles de los certificados de políticas de personas físicas y el significado de cada uno de ellos.

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

Los certificados que abarca el documento son:

- Certificado de persona física 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 de Persona Física, 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/10445900/10526749/AC_Raiz_FNMT-RCM_SHA256.cer

Subordinada:

https://www.sede.fnmt.gob.es/documents/10445900/10526749/AC_FNMT_Usuarios.cer

Perfil Certificado Persona Física en Software

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		Object Identifier 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	Denominación de la Unidad Organizativa ou= Ceres	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Common Name	cn= AC FNMT Usuarios	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5.	Validity	4 años	Sí		
6.	Subject	Identificación/descripción del custodio/responsable de las claves certificadas	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. SerialNumber	NIF del titular	Sí		PrintableString (rfc5280) Ejemplo: SN=00000000T
	6.3. Given Name	Nombre de pila, de acuerdo con documento de identidad	Sí		UTF8String (rfc5280). Por ejemplo: gn=Juan
	6.4. Surname	Apellidos de acuerdo con documento de identificación	Sí		UTF8String (rfc5280). Por ejemplo: sn=Español Español
	6.5. Common Name	Apellidos, Nombre y NIF del titular	Sí		UTF8String (rfc5280). Por ejemplo: cn= Español Español Juan – 00000000T
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 titular, 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
9.	Subject Key Identifier	Identificador de la clave pública del titular 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		De la rfc 5280: "The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an

Campo	Contenido	Oblig	Crit	Especificaciones
				entity authentication service, a data origin authentication service, and/or an integrity service."
10.2. Content Commitment	1	Sí		De la rfc 5280: "The contentCommitment bit is asserted when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non-repudiation service that protects against the signing entity falsely denying some action. In the case of later conflict, a reliable third party may determine the authenticity of the signed data."
10.3. Key Encipherment	1	Sí		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
10.4. Data Encipherment	0	Sí		Se utiliza para cifrar datos que no sean claves criptográficas.
10.5. Key Agreement	0	Sí		Para uso en el proceso de acuerdo de claves
10.6. Key Certificate Signature	0	Sí		Se permite usa para firmar certificados. Este uso se utiliza en los certificados de autoridades de certificación.
10.7. CRL Signature	0	Sí		Se permite para firmar listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación.
11. Extended Key Usage	Uso mejorado o extendido de las claves	Sí		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	Opcional		Protección de correo electrónico.
11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente
11.3. AnyExtendedKeyUsage	2.5.29.37.0	Sí		
12. Qualified Certificate Statements	Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
12.1. QcCompliance	Certificado es reconocido.	Sí		Indica que el certificado es reconocido.
12.2. 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. 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."
12.3. QcLimitValue	0 €	Sí		Límite de responsabilidad
13. Certificate Policies	Política de certificación	Sí		
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.10.1	Sí		Identificador de la política
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 reconocido. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
14. Subject Alternative Names	Identificación/descripción del titular	Sí	No	
14.1. rfc822 Name	Correo electrónico del titular	Opcional		
14.2. Directory Name				
14.2.1. Nombre	Nombre de pila del titular del certificado 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 titular del	Sí		UTF8 String. Por ejemplo:

Campo		Contenido	Oblig	Crit	Especificaciones
		certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =<Apellido 1			1.3.6.1.4.1.5734.1.2=ESPAÑOL
	14.2.3. Apellido2	Segundo apellido del titular del certificado 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	Identificador de identidad del titular / custodio de las claves. (NIF). Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=<NIF	Sí		UTF8 String, tamaño 9. Por ejemplo: 1.3.6.1.4.1.5734.1.4=99999999R
15.	CRL Distribution Point		Sí	No	
	15.1. Distribution Point 1	Punto de distribución 1 de la CRL ldap://ldapsu.cert.fnmt.es/C N=CRL<xxx*>, CN=AC%20FNMT%20Usuarios , OU=CERES, O=FNMT-RCM, C=ES?certificateRevocationList; binary?base?objectclass=cRL DistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx*> es un identificador que identificará 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://ocspusu.cert.fnmt.es/o cspusu/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/cert s/ACUSU.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 persona física
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 rfc5280: "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 nuevos certificados de Persona física y los de la nueva CA.

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 = AC FNMT Usuarios

5. Validity

La validez del certificado pasa de 3 a 4 años.

6. Subject

Pasa de ser

CN = NOMBRE APELLIDO1PF APELLIDO2PF PRUEBASPF - 00000000T

OU = 500070076

OU = FNMT Clase 2 CA

O = FNMT

C = ES

A ser

CN = APELLIDO1PF APELLIDO2PF PRUEBASPF - 00000000T

SN = APELLIDO1PF APELLIDO2PF

G = PRUEBASPF

SERIALNUMBER = 00000000T (No confundir con el Serial Number del certificado)

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, Autenticación del Cliente y se añade Cualquier Propósito.

12. Qualified Certificate Statements

Certificado Reconocido (Cualificado), Límite de uso Monetario 0€ y se añade el tiempo de Retención 15 años.

13. Certificate Policies

El OID de las políticas de certificación (Policy Identifier) pasa de 1.3.6.1.4.1.5734.3.5 a 1.3.6.1.4.1.5734.3.10.1.

15. CRL Distribution Point

Pasa del formato

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección del directorio:

CN=CRL13169

OU=FNMT Clase 2 CA

O=FNMT

C=ES

Al formato URL

[1]Punto de distribución CRL

Nombre del punto de distribución:

Nombre completo:

Dirección

URL=ldap://ldapusu.cert.fnmt.es/cn=CRL1,cn=AC%20FNMT%20Usuarios,ou=CERES,o=FNMT-RCM,c=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

Indicar que el acceso al directorio es el mismo C=ES, O=FNMT-RCM y luego la nueva CA va a la rama OU=CERES, CN=AC FNMT Usuarios. Mientras que la de clase 2 iba a la rama OU=FNMT Clase 2 CA. Esta estructura arbórea permite la convivencia de las dos CAs en un mismo directorio.

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.

Adaptación a eIDAS

En este apartado destacamos los cambios que ha sufrido el certificado de usuario con respecto para adaptarse a la nueva normativa Europea.

6. Subject

Pasa de ser

CN = APELLIDO1PF APELLIDO2PF PRUEBASPF - 00000000T
SN = APELLIDO1PF APELLIDO2PF
G = PRUEBASPF
SERIALNUMBER = 00000000T (No confundir con el Serial Number del certificado)
C = ES

A ser

CN = EIDAS PRUEBAS - 00000000T
G = PRUEBAS
SN = EIDAS
SERIALNUMBER = IDCES-00000000T
C = ES

El serialnumber pasa a ser el identificador del document de identidad más el número del document de identidad.

12. Qualified Certificate Statements

Se elimina el QcLimitValue y se añade:

- QcType, que indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
- QcPDS, enlace al PKI Disclosure Statements

Perfil Final Adaptado a eIDAS

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		Object Identifier 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	Denominación de la Unidad Organizativa ou= Ceres	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Common Name	cn= AC FNMT Usuarios	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5.	Validity	4 años	Sí		
6.	Subject	Identificación/descripción del custodio/responsable de las claves certificadas	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. SerialNumber	NIF del titular	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.3. Given Name	Nombre de pila, de acuerdo con documento de identidad	Sí		UTF8String (rfc5280). Por ejemplo: givenName=Juan
	6.4. Surname	Apellidos de acuerdo con documento de identificación	Sí		UTF8String (rfc5280). Por ejemplo: sn=Español Español
	6.5. Common Name	Apellidos, Nombre y NIF del titular	Sí		UTF8String (rfc5280). Por ejemplo: cn= Español Español Juan – 00000000T
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 titular, 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
9.	Subject Key Identifier	Identificador de la clave pública del titular 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		De la rfc 5280: "The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service."
	10.2. Content Commitment	1	Sí		De la rfc 5280: "The contentCommitment bit is asserted when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non-repudiation service that protects against the signing entity falsely denying some action. In the case of later conflict, a reliable third party may determine the authenticity of the signed data."
	10.3. Key Encipherment	1	Sí		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0	Sí		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0	Sí		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0	Sí		Se permite usa para firmar certificados. Este uso se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0	Sí		Se permite para firmar listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí		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	Opcional		Protección de correo electrónico.
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance	Certificado es reconocido.	Sí		Indica que el certificado es reconocido.
	12.2. 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. 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."
	12.3. QcType	Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.4. QcPDS	{ https://www.cert.fnmt.es/pds/PDSACUuarios_es.pdf , es}, { https://www.cert.fnmt.es/pds/PDSACUuarios_en.pdf , en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
13. Certificate Policies		Política de certificación	Sí		
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.10.1	Sí		Identificador de la política
	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 reconocido. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.2.3. Policy Identifier		0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
14. Subject Alternative Names			Identificación/descripción del titular	Sí	No	
	14.1. rfc822 Name		Correo electrónico del titular	Opcional		
	14.2. Directory Name					
		14.2.1. Nombre	Nombre de pila del titular del certificado 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 titular del certificado 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 titular del certificado 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	Identificador de identidad del titular custodio de las claves. (NIF). Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=<NIF	Sí		UTF8 String, tamaño 9. Por ejemplo: 1.3.6.1.4.1.5734.1.4=99999999R
15. CRL Distribution Point				Sí	No	
	15.1. Distribution Point 1		Punto de distribución 1 de la CRL Idap://ldapsu.cert.fnmt.es/CN=CRL<xxx*>, CN=AC%20FNMT%20Usuarios, OU=CERES, O=FNMT-RCM, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). <xxx*> es un identificador que identificará 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://ocspusu.cert.fnmt.es/ocspusu/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/ACUSU.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 persona física

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."

Formas de Validación

A continuación se enumeran los mecanismos de validación de los certificados de la AC FNMT Usuarios o Persona Física.

Estos mecanismos son cerrados se requieren de permiso/autorización para ser accedidos.

La validación de estos certificados puede realizarse a través de:

- CRLs
 - LDAP
- 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 FNMT Usuarios 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 Usuarios se encuentra:

- Hosts: ldapusu.cert.fnmt.es
- Puerto: 389.
- SearchBase: CN=AC FNMT Usuarios, 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%20FNMT%20Usuarios,ou=CERES,o=FNMT-RCM,c=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint`

El acceso al LDAP es mediante usuario y password. Es el mismo que se utiliza para acceder al directorio de Clase 2.

*** es el número de la CRL.

OCSP

El acceso al servidor de la AC FNMT Usuarios abierto.

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

Certificados

Para validar las CRLs se necesitan los siguientes certificados:

- Validar Respuestas OCSP:

https://www.sede.fnmt.gob.es/documents/10445900/10532302/OCSP_AC_FNMT_Usuarios

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

Raíz:

https://www.sede.fnmt.gob.es/documents/10445900/10526749/AC_Raiz_FNMT-RCM_SHA256.cer

Subordinada:

https://www.sede.fnmt.gob.es/documents/10445900/10526749/AC_FNMT_Usuarios.cer