

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 |
|  |  |  |  |
|  |  |  |  |

**Referencia:**

**Documento clasificado como:** *Público*

**Índice**

[Introducción 3](#_Toc405472205)

[Perfil Certificado Persona Física en Software 4](#_Toc405472206)

[Diferencias entre los nuevos certificados de Persona física y los de la nueva CA. 7](#_Toc405472207)

1. [3. Signature Algorithm 7](#_Toc405472208)
2. [4. Issuer Distinguish Name 7](#_Toc405472209)
3. [5. Validity 7](#_Toc405472210)
4. [6. Subject 7](#_Toc405472211)
5. [8. Subject Public Key Info 7](#_Toc405472212)
6. [10. Key Usage 8](#_Toc405472213)
7. [11. Extended Key Usage 8](#_Toc405472214)
8. [12. Qualified Certificate Statements 8](#_Toc405472215)
9. [13. Certificate Policies 8](#_Toc405472216)
10. [15. CRL Distribution Point 8](#_Toc405472217)
11. [16. Authority Info Access 9](#_Toc405472218)

[Formas de Validación 9](#_Toc405472219)

1. [CRLs 9](#_Toc405472220)

[LDAP 9](#_Toc405472221)

1. [OCSP 10](#_Toc405472222)

[Certificados 10](#_Toc405472223)

# 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/11614/116099/AC_Raiz_FNMT-RCM_SHA256.cer/b1447e06-9927-45b7-92cc-8690edd7562d>

Subordinada:

<https://www.sede.fnmt.gob.es/documents/11614/116099/AC_FNMT_Usuarios.cer/6688f274-5fb0-4fef-b50c-4321aaedb0e3>

# 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 certificados es versión 3 (X509v3) |
| 1. 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- 2159).  El número de serie se asignará de forma aleatoria. |
| 1. Signature Algorithm | | | sha256WithRSAEncryption | Sí |  | Object Identifier  OID: 1.2.840.113549.1.1.11 |
| 1. Issuer Distinguish Name |  | | Entidad emisora del certificado (CA Subordinada) | Sí |  |  |
|  | * 1. Country | | C=ES | Sí |  | Se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”. PrintableString, tamaño 2 (rfc5280) |
| * 1. 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) |
| * 1. Organizational Unit | | Denominación de la Unidad Organizativa  ou= Ceres | Sí |  | UTF8 String, tamaño máximo 128 (rfc5280) |
| * 1. Common Name | | cn= AC FNMT Usuarios | Sí |  | UTF8 String, tamaño máximo 128 (rfc5280) |
| 1. Validity | | | 4 años | Sí |  |  |
| 1. Subject |  | | Identificación/descripción del custodio/responsable de las claves certificadas | Sí |  |  |
|  | * 1. Country | | C=ES | Sí |  | Se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”. PrintableString, tamaño 2 (rfc5280) |
| * 1. SerialNumber | | NIF del titular | Sí |  | PrintableString (rfc5280) Ejemplo:  SN=00000000T |
| * 1. Given Name | | Nombre de pila, de acuerdo con documento de identidad | Sí |  | UTF8String (rfc5280). Por ejemplo:  gn=Juan |
| * 1. Surname | | Apellidos de acuerdo con documento de identificación | Sí |  | UTF8String (rfc5280). Por ejemplo:  sn=Español Español |
| * 1. Common Name | | Apellidos, Nombre y NIF del titular | Sí |  | UTF8String (rfc5280). Por ejemplo:  cn= Español Español Juan – 00000000T |
| 1. 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. |
| 1. 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 |
| 1. 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). |
| 1. Key Usage |  | | Uso permitido de las claves certificadas. | Sí | Sí | Normalizado en norma X509 |
|  | * 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.” |
| * 1. 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, areliable third party may determine the authenticity of the signed data.” |
| * 1. Key Encipherment | | 1 | Sí |  | Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras |
| * 1. Data Encipherment | | 0 | Sí |  | Se utiliza para cifrar datos que no sean claves criptográficas. |
| * 1. Key Agreement | | 0 | Sí |  | Para uso en el proceso de acuerdo de claves |
| * 1. Key Certificate Signature | | 0 | Sí |  | Se permite usa para firmar certificados. Este uso se utiliza en los certificados de autoridades de certificación. |
| * 1. CRL Signature | | 0 | Sí |  | Se permite para firmar listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación. |
| 1. 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. |
|  | * 1. Email Protection | | 1.3.6.1.5.5.7.3.4 | Opcional |  | Protección de correo electrónico. |
| * 1. Client Authentication | | 1.3.6.1.5.5.7.3.2 | Sí |  | Autenticación de cliente |
| * 1. AnyExtendedKeyUsage | | 2.5.29.37.0 | Sí |  |  |
| 1. Qualified Certificate Statements |  | | Extensiones cualificadas. | Sí | No | ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados |
|  | * 1. QcCompliance | | Certificado es reconocido. | Sí |  | Indica que el certificado es reconocido. |
| * 1. 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.”. |
| * 1. QcLimitValue | | 0 € | Sí |  | Límite de responsabilidad |
| 1. Certificate Policies |  | | Política de certificación | Sí |  |  |
|  | * 1. Policy Identifier | | 1.3.6.1.4.1.5734.3.10.1 | Sí |  | Identificador de la política |
| * 1. Policy Qualifier Id |  |  |  |  |  |
|  | * + 1. CPS Pointer | http://www.cert.fnmt.es/dpcs/ | Sí |  | IA5String String. URL de las condiciones de uso. |
| * + 1. 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. |
| 1. Subject Alternative Names |  | | Identificación/descripción del titular | Sí | No |  |
|  | * 1. rfc822 Name | | Correo electrónico del titular | Opcional |  |  |
| * 1. Directory Name |  |  |  |  |  |
|  | * + 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 |
| * + 1. 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 |
| * + 1. 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 |
| * + 1. 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 |
| 1. CRL Distribution Point |  | |  | Sí | No |  |
|  | * 1. Distribution Point 1 | | Punto de distribución 1 de la CRL  ldap://ldapusu.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. |
| 1. Authority Info Access |  | |  | Sí | No |  |
|  | * 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) |
| * 1. Acces Location 1 | | http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder | Sí |  | URL del servicio de  OCSP |
| * 1. 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- caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension.  The referenced CA issuers description is  intended to aid certificate users in the  selection of a certification path that  terminates at a point trusted by the  certificate user.” |
| * 1. 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 físical |
| 1. 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. |
|  | * 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.

# 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 AP se encuentra:

* Hots: ldapusu.cert.fnmt.es (193.104.0.184)
* 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 AP se realiza mediante petición firmada. Estas peticiones deberán ir firmadas por un certificado de Sello de la CA de AP o por un certificado de Sello de entidad de la CA de componentes informáticos.

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/11614/116107/OCSP_AC_FNMT_Usuarios.cer/6ae8a04c-90d9-46cb-b9e4-195025663782>

* 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_FNMT_Usuarios.cer/6688f274-5fb0-4fef-b50c-4321aaedb0e3>