# ANEXO I: IDENTIFICACIÓN DEL CERTIFICADO DE LA AUTORIDAD DE CERTIFICACIÓN AC FNMT USUARIOS

La Autoridad de Certificación AC FNMT Usuarios utiliza para la firma de certificados y CRLs el certificado identificado a continuación:

**Certificado de la Autoridad de Certificación "AC FNMT Usuarios"**

- Nombre distintivo: CN = AC FNMT Usuarios, OU = Ceres, O = FNMT-RCM, C = ES
- Número de serie: 45 5f 3a e1 5c 21 cd ba 54 4f 82 aa 47 51 eb db
- Período de validez desde: martes, 28 de octubre de 2014 12:48:58
- Período de validez hasta: domingo, 28 de octubre de 2029 12:48:58
- Huella digital (sha1): 80 8B 72 E43B 57 4C F5 87 7C B8 41 A8 DF 88 39 6D 38 AB 94
- Huella digital (sha256): 60 12 93 CA 20 B0 9A 03 29 5D 19 62 56 C6 95 3F F9 EB A8 11 DB 8E 3C E1 40 41 3C 1B FF E9 A8 69

# ANEXO II: PERFILES DE CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

## CERTIFICADO RAÍZ DE LA FNMT-RCM

| CERTIFICADO RAÍZ DE LA FNMT-RCM | | | |
|---|---|---|---|
| **CAMPO** | **CONTENIDO** | **CRÍTICA** | **OBSERVACIONES** |
| **Campos de X509v1** | | | |
| **1. Versión** | V3 | | |
| **2. Serial Number** | Número identificativo único del certificado. | | *[RFC3280]: the serial number MUST be a positive integer, not longer than 20 octets ( 1 < SN < $2^{159}$). Processing components MUST be able to interpret such long numbers.* |
| **3. Signature Algorithm** | Sha1withRsaEncryption<br><br>Sha256withRsaEncryption<br><br>Sha512withRsaEncryption | | OID: 1.2.840.113549.1.1.5<br><br>OID: 1.2.840.113549.1.1.11<br><br>OID: 1.2.840.113549.1.1.13<br><br>Norma PKCS#1 v2.1 y RFC 3447. |
| **4. Issuer Distinguished Name** | OU=AC RAIZ FNMT -RCM<br><br>O=FNMT-RCM<br><br>C=ES | | Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements"*, en *PrintableString*. |
| **5. Validez** | Hasta 01/01/2030 | | El programa de inclusión de certificados raíz de Microsoft requiere que la fecha de validez sea posterior al 1/1/2010.<br><br>*[RFC3280]: Validity dates before and through 2049 MUST be encoded by CAs as UTCTime, dates in 2050 and later as GeneralizedTime. Date values MUST be given in the format YYMMDDhhmmssZ resp. YYYYMMDDhhmmssZ, i.e. always including seconds and expressed as Zulu time (Universal Coordinated Time).* |
| **6. Subject** | OU=AC RAIZ FNMT -RCM<br><br>O=FNMT-RCM<br><br>C=ES | | Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements"*, en *PrintableString*.<br><br>Coincidirá con el campo emisor del certificado de las AC subordinada.<br><br>*[RFC3280]: The issuer name MUST be a non-empty DName. Processing components MUST be prepared to receive the following attributes: countryName,*<br><br>*organizationName, organizationalUnitName, distinguishedNameQualifier, stateOrProvinceName, commonName, serialNumber, and domainComponent. Processing components SHOULD be prepared for attributes: localityName, title, surname, givenName, initials, pseudonym, and generationQualifier*<br><br>*[ETSI-QC]: the issuer name MUST contain the countryName attribute. The specified country MUST be the country where the issuer CA is established.*<br><br>*[ETSI-CPN]: the issuer name MUST contain the countryName and the organizationName attributes.* |

| CERTIFICADO RAÍZ DE LA FNMT-RCM | | | |
|---|---|---|---|
| **CAMPO** | **CONTENIDO** | **CRÍTICA** | **OBSERVACIONES** |
| **7. Subject Public Key Info** | Algoritmo: RSA Encryption<br><br>Longitud: 4096 bits | | |
| **Campos de X509v2** | | | |
| **1. issuerUniqueIdentifier** | No se utilizará | | |
| **2. subjectUniqueIdentifier** | No se utilizará | | |
| **Extensiones de X509v3** | | | |
| **1. Subject Key Identifier** | Función hash SHA-1 sobre la clave pública del sujeto (AC raíz). | NO (RFC 3280) | RFC 3280: 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). |
| **2. Authority Key Identifier** | No procede | | |
| **3. KeyUsage** | | SI (RFCs 3280 y 3739) | |
| **Digital Signature** | 0 | | |
| **Non Repudiation** | 0 | | |
| **Key Encipherment** | 0 | | |
| **Data Encipherment** | 0 | | |
| **Key Agreement** | 0 | | |
| **Key Certificate Signature** | 1 | | |
| **CRL Signature** | 1 | | |
| **4.extKeyUsage** | No se utilizará | | |
| **5. privateKeyUsagePeriod** | No se utilizará | | |

| CERTIFICADO RAÍZ DE LA FNMT-RCM | | | |
|---|---|---|---|
| **CAMPO** | **CONTENIDO** | **CRÍTICA** | **OBSERVACIONES** |
| **6. Certificate Policies** | | NO | [RFC 3739] obliga la existencia de al menos un valor.<br><br>La Ley de Firma Electrónica dice para los certificados reconocidos: "*La identificación del prestador de servicios de certificación que expide el certificado y su domicilio*". Se incluirá en la DPC.<br><br>*[RFC3280]: PolicyInformation SHOULD only contain an OID*<br><br>*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 }.*<br><br>*To promote interoperability, this profile RECOMMENDS that policy information terms consist of only an OID. Where an OID alone is insufficient, this profile strongly recommends that use of qualifiers* |
| **Policy Identifier** | anyPolicy 2 5 29 32 0 | | |
| **URL CPS** | http://www.cert.fnmt.es/dpcs/ | | |
| **Notice Reference** | NO para los certificados de AC, según RFC 5280 (sustituta de RFC 3280). | | |
| **7. Policy Mappings** | No se utilizará | | |
| **8. Subject Alternate Names** | No se utilizará | NO | |
| **9. Issuer Alternate Names** | No se utilizará | | |
| **10. Subject Directory Attributes** | No se utilizará | | |
| **11. Basic Constraints** | | SI (RFC 3280) | RFC 3280. Puede especificarse el número máximo de niveles en "Path Length Constraint". Para la AC Raíz no se establecerá ningún límite de niveles de AC subordinadas.<br><br>[*RFC3280] This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates.* |
| **Subject Type** | CA | | |
| **Path Length Constraint** | Ninguno | | |
| **12. Policy Constraints** | No utilizado | | |
| **13. CRLDistributionPoints** | No utilizado | | La revocación del certificado Raíz se publicitará por otros mecanismos. |
| **14. Auth. Information Access** | No procede | NO (RFC 3280) | |
| **15.netscapeCertType** | No procede | | |

| CERTIFICADO RAÍZ DE LA FNMT-RCM | | | |
|---|---|---|---|
| **CAMPO** | **CONTENIDO** | **CRÍTICA** | **OBSERVACIONES** |
| **16. netscapeRevocationURL** | No procede | | |
| **17. netscapeCAPolicyURL** | No procede | | |
| **18. netscapeComment** | No procede | | |

**Tabla 1 - Certificado raíz de la FNMT-RCM**

## CERTIFICADO AUTORIDAD DE CERTIFICACIÓN "AC FNMT USUARIOS"

| 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.<br><br>Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- $2^{159}$).<br><br>El número de serie se asignará de forma aleatoria. |
| **3. Signature Algorithm** | | Sha256withRsaEncryption | Sí | | Object Identifier<br><br>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, tamaño 2 (rfc5280) |
| | 4.2. Organization | Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado).<br><br>o=FNMT-RCM | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 4.3. Organizational Unit | Denominación de la Unidad Organizativa<br><br>ou = AC RAIZ FNMT-RCM | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| **5. Validity** | | 15 años | Sí | | |
| **6. Subject** | | | 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. Organization | Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado).<br><br>o=FNMT-RCM | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 6.3. Organizational Unit | Denominación de la Unidad Organizativa | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |

| Campo | | Contenido | Oblig | Crit | Especificaciones |
|---|---|---|---|---|---|
| | | ou= Ceres | | | |
| | 6.4. Common Name | cn= AC FNMT Usuarios | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| **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).<br><br>Coincide con el campo Subject Key Identifier de la AC raíz. |
| **8. Subject Public Key Info** | | Clave pública de la CA Subordinada para la Administración Pública, codificada de acuerdo con el algoritmo criptográfico.<br><br>En este caso RSA Encryption. | Sí | | Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave.<br><br>La longitud de la clave será 2048 |
| **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 |
| | 10.1. Digital Signature | 0 | Sí | | Permite realizar la operación de firma electrónica. |
| | 10.2. Content Commitment | 0 | Sí | | Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma. |
| | 10.3. Key Encipherment | 0 | 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 | 1 | Sí | | Se permite usa para firmar certificados. Este uso se utiliza en los certificados de autoridades de certificación. |
| | 10.7. CRL Signature | 1 | Sí | | Se permite para firmar listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación. |

| Campo | | | Contenido | Oblig | Crit | Especificaciones |
|---|---|---|---|---|---|---|
| **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.*<br><br>*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. Longitud máxima 200 caracteres. |
| **12. CRL Distribution Point** | | | | Sí | | |
| | 12.1. Distribution Point 1 | | Punto de distribución 1 de la CRL (ARL)<br><br>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)<br><br>http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl | Sí | | Ruta del servicio LDAP donde reside la CRL (punto de distribución 2). |
| **13. Basic Constraints** | | | | Sí | Sí | |
| | 13.1. 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." |
| | 13.2. pathLenConstraint | | 0 | Sí | | Un pathLenConstraint de cero indica que ningún no pueden existir más certificados de CA intermedios en la ruta de certificación. |
| **14. Authority Info Access** | | | | Sí | No | |

| Campo | | Contenido | Oblig | Crit | Especificaciones |
|---|---|---|---|---|---|
| | 14.1. Access Method 1 | Identificador de método de acceso a la información de revocación:<br><br>1.3.6.1.5.5.7.48.1 (ocsp) | Sí | | OCSP<br><br>(1.3.6.1.5.5.7.48.1) |
| | 14.2. Acces Location 1 | http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder | Sí | | URL del servicio de<br><br>OCSP |
| | 14.3. Access Method 2 | Identificador de método de acceso a la información de certificados adicionales<br><br>necesarios para la validación:<br><br>1.3.6.1.5.5.7.48.2 (ca cert) | Sí | | Certificado de la CA emisora:<br><br>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.<br><br>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." |
| | 14.4. 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 FNMTRCM. |

**Tabla 2 - Certificado Autoridad de Certificación "AC FNMT Usuarios"**

# ANEXO III: PERFIL DEL CERTIFICADO DE PERSONA FÍSICA

| 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 | | 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, areliable 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 |