
# DIRECCIÓN DE SERVICIOS DIGITALES E INNOVACIÓN
# DEPARTAMENTO CERES

## DOCUMENTO DE PERFILES DE LA AUTORIDAD DE CERTIFICACIÓN
## AC COMPONENTES INFORMÁTICOS

**Referencia:**

**Documento clasificado como:** *Público*

# Contenido

# 1. OBJETO

El objeto de este documento es la definición de los perfiles de los certificados emitidos por la autoridad de certificación *AC Componentes Informáticos* de la FNMT-RCM. Así mismo, se incluye la definición del perfil de la propia autoridad.

# 2. PERFILES

## 2.1. CA SUBORDINADA COMPONENTES

| Campo | | Contenido | Obligatoriedad | Criticidad | 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>Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- $2^{159}$). |
| 3. Signature Algorithm | | Sha256withRsaEncryption | Sí | | Identificando el tipo de algoritmo<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>O=FNMT-RCM | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 4.3. Organization Unit | OU=AC RAIZ FNMT-RCM | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| 5. Validity | | 15 años | Sí | | |
| 6. Subject | | Entidad emisora del certificado (CA Subordinada) | Sí | | |
| | 6.1. Country | C=ES | Sí | | Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280) |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | 6.2. Organization | Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado).<br>O=FNMT-RCM. | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 6.3. Organization Unit | OU=AC Componentes Informáticos | 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>Coincide con el campo Subject Key Identifier de la CA raíz. |
| 8. Subject Public Key Info | | Clave pública de la CA de Componentes, codificada según el estándar PKCS#1 de RSA.<br>La longitud de la clave será 2048 bits. | Sí | | Campo que contiene la clave pública del certificado. |
| 9. Subject Key Identifier | | Identificador de la clave pública de la CA de Componentes. | 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 del certificado. | 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 | | Si se activa el bit, permite que el certificado sea utilizado para firmar otros certificados. Este uso se utiliza en los certificados de autoridades de certificación. |
| | 10.7. CRL Signature | 1 | Sí | | Si se activa el bit, permite la firma de listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación. |
| 11. Certificate Policies | | Política de certificación | Sí | No | |

| Campo | | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|---|
| | 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 | | | | | |
| | | 11.2.1 CPS Pointer | http://www.cert.fnmt.es/dpcs/ | Sí | | IA5String String. URL de la declaración de prácticas de certificación. |
| | | 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 | No | |
| | 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 | 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. |
| | 13.1. Subject Type | | CA | | | Tipo de sujeto: Autoridad de Certificación. |
| | 13.2. Path Length | | 0 | | | Un pathLenConstraint de cero indica que esta CA no puede emitir certificados para otras CAs subordinadas, únicamente puede emitir certificados para entidades finales. |
| 14. Authority Info Access | | | | Sí | | |
| | 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) | | | OCSP (1.3.6.1.5.5.7.48.1) |
| | 14.2. Access Location 1 | | http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder | | | URL del servicio de OCSP |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | | | | | |
| | 14.3. Access Method 2 | Identificador de método de acceso a la información de certificados adicionales necesarios para la validación:<br><br>1.3.6.1.5.5.7.48.2 (ca cert) | | | Certificado de la CA emisora:<br><br>De la rfc 5280: "*the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*" |
| | 14.4. Access Location 2 | http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt | | | Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA raíz de la FNMT-RCM. |

## 2.2. CERTIFICADOS DE COMPONENTES

### 2.2.1. Certificado de componente de sello de entidad

| Campo | | Contenido | Obligatoriedad | Criticidad | 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>Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- $2^{159}$).<br>El número de serie se asignará de forma aleatoria. |
| 3. Signature Algorithm | | Sha256withRsaEncryption | Sí | | Identificando el tipo de algoritmo<br>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).<br>O=FNMT-RCM. | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 4.3. Organization Unit | OU=AC Componentes Informáticos | Sí | | UTF8 String, tamaño máximo 128 (rfc5280). |
| 5. Validity | | Variable | Sí | | La duración será variable (1, 2 ó 3 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto. |
| 6. Subject | | Identificación/descripción del suscriptor del certificado y del componente | 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. LocalityName | Nombre de la localidad del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>L=Madrid |
| | 6.3. Organization | Denominación del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>O=Ministerio de Economía |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | 6.4. Organizational Unit | Departamento o área del suscriptor para el que se emite el certificado. | No | | UTF8String (rfc5280). Por ejemplo:<br>OU=Departamento de Informática |
| | 6.5. Serial Number | NIF del suscriptor | Sí | | PrintableString (rfc5280). Por ejemplo:<br>SN= Q0000000J |
| | 6.6. Organization Identifier | Identificador de la organización distinto del nombre<br>Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) | Sí | | Por ejemplo: organizationidentifier=VATES-Q0000000J |
| | 6.7. Common Name | Denominación del componente | Sí | | UTF8String (rfc5280). Por ejemplo:<br>CN=Servicio de Registro |
| 7. Authority Key Identifier | | Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente. | Sí | No | 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>Coincide con el campo Subject Key Identifier de la CA emisora. |
| 8. Subject Public Key Info | | Clave pública del componente, codificada según el estándar PKCS#1 de RSA.<br>La longitud de la clave será 2048 bits. | Sí | No | Campo que contiene la clave pública del certificado. |
| 9. Subject Key Identifier | | Identificador de la clave pública del componente. | Sí | No | 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 | Normalizado en norma X509 |
| | 10.1. Digital Signature | 1 | Sí | | Permite realizar la operación de firma electrónica |
| | 10.2. Content Commitment | 1 | 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 | 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. Se utiliza en los certificados de autoridades de certificación. |

| Campo | | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|---|
| | 10.7. CRL Signature | | 0 | Sí | | Se permite para firmar listas de revocación de certificados. |
| 11. Extended Key Usage | | | Uso mejorado o extendido de las claves | Sí | No | 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. Client Authentication | | 1.3.6.1.5.5.7.3.2 | Sí | | Autenticación de cliente. |
| | 11.2. Document Signing | | 1.3.6.1.4.1.311.10.3.12 | Sí | | Firma de documentos. |
| | 11.3. Adobe Authentic Documents Trust | | 1.2.840.113583.1.1.5 | Sí | | Firma de documentos PDF. |
| 12. Qualified Certificate Statements | | | Extensiones cualificadas. | Sí | No | ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados |
| | 12.1. QcCompliance (0.4.0.1862.1.1) | | Certificado cualificado | Sí | | Indicación de certificado cualificado |
| | 12.2. QcEuRetentionPeriod (0.4.0.1862.1.3) | | 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 (0.4.0.1862.1.6) | | Id-etsi-qct-eseal (0.4.0.1862.1.6.2) | Sí | | Indica que el certificado es de sello.<br><br>Certificate for electronic seals as defined in Regulation (EU) No 910/2014 |
| | 12.4. QcPDS(0.4.0.1862.1.5) | | {https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en} | Sí | | Lugar donde se encuentra la declaración PDS |
| 13. Certificate Policies | | | Política de certificación | Sí | No | |
| | 13.1. Policy Identifier | | 1.3.6.1.4.1.5734.3.9.19 | Sí | | Identificador de la política |
| | 13.1.1 Policy Qualifier Id | | | Sí | | |
| | | 13.1.1.1 CPS Pointer | http://www.cert.fnmt.es/dpcs/ | Sí | | IA5String String. URL de las condiciones de uso. |
| | | 13.1.1.2 User Notice | "Certificado cualificado de sello electrónico según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de FNMT-RCM con | Sí | | UTF8 String. Longitud máxima 200 caracteres. |

| Campo | | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|---|
| | | | NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)" | | | |
| | 13.2. Policy Identifier | | QCP-l (0.4.0.194112.1.1) | Sí | | Certificado cualificado de sello, acorde al Reglamento UE 910/2014<br>Itu-t(0) Identified-organizatio(4) etsi(0) qualifed-certificate-policies(194112) policy-identifiers(1) qcp-legal(1) |
| 14. Subject Alternative Names | | | | Sí | No | |
| | 14.1. Denominación del componente | | Id Campo / Valor:<br>1.3.6.1.4.1.5734.1.8 = < Denominación del componente> | Sí | | |
| 15. CRL Distribution Point | | | Informa acerca de cómo se obtiene la información de la CRL asociada al certificado. | Sí | No | |
| | 15.1. Distribution Point 1 | | Punto de publicación de la CRL1.<br>ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint<br>*xxx: número entero identificador de la CRL (CRL particionadas) | Sí | | Ruta del servicio LDAP donde reside la CRL (punto de distribución 1). |
| | 15.2. Distribution Point 2 | | Punto de publicación de la CRL2.<br>http://www.cert.fnmt.es/crlscomp/CRLnnn.crl<br>*nnn: número entero identificador de la CRL (CRL particionadas) | Sí | | Ruta donde reside la CRL (punto de distribución 2). |
| 16. Authority Info Access | | | | Sí | No | |
| | 16.1. Access Method 1 | | Identificador de método de acceso a la información de revocación:<br>1.3.6.1.5.5.7.48.1 (ocsp) | Sí | | |
| | 16.2. Access Location 1 | | http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder | Sí | | |
| | 16.3. Access Method 2 | | Identificador de método de acceso a la información de certificados adicionales necesarios para la validación:<br>1.3.6.1.5.5.7.48.2 (ca cert) | Sí | | Entidad emisora de los certificados (CA Subordinada)<br>De la rfc 5280: "*the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that* |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | | | | | *terminates at a point trusted by the certificate user."* |
| | 16.4. Access Location 2 | http://www.cert.fnmt.es/certs/ACCOMP.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 la raíz de la FNMT-RCM. |
| 17. Basic Contraints | | 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. Subject Type | Valor FALSE (entidad final) | | | Con este certificado no se pueden emitir otros certificados. |

### 2.2.2. Certificado de autenticación de sitio web estándar

| Campo | | Contenido | Obligatoriedad | Criticidad | 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>Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- $2^{159}$).<br>El número de serie se asignará de forma aleatoria. |
| 3. Signature Algorithm | | Sha256withRsaEncryption | Sí | | Identificando el tipo de algoritmo<br>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).<br>O=FNMT-RCM. | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 4.3. Organization Unit | OU=AC Componentes Informáticos | Sí | | UTF8 String, tamaño máximo 128 (rfc5280). |
| 5. Validity | | 12 meses | Sí | | La vigencia máxima es de 12 meses. |
| 6. Subject | | Identificación/descripción del suscriptor del certificado y del componente | 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. LocalityName | Nombre de la localidad del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>L=Madrid |
| | 6.3. Organization | Denominación del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>O=Ministerio de Economía |
| | 6.4. Serial Number | NIF del suscriptor | Sí | | PrintableString (rfc5280). Por ejemplo:<br>SN= Q0000000J |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | 6.5. OrganizationIdentifier | Identificador de la Organización<br><br>Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad) | Sí | | Por ejemplo: organizationidentifier=VATES-Q0000000J |
| | 6.6. Common Name | Dominio para el que se expide el certificado | Sí | | UTF8String (rfc5280).<br><br>CN=www.fnmt.es |
| 7. Authority Key Identifier | | Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente. | Sí | No | 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 CA emisora. |
| 8. Subject Public Key Info | | Clave pública del componente, codificada según el estándar PKCS#1 de RSA.<br><br>La longitud de la clave será 2048 bits. | Sí | No | Campo que contiene la clave pública del certificado. |
| 9. Subject Key Identifier | | Identificador de la clave pública del componente. | Sí | No | 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 | | | Permite realizar la operación de firma electrónica |
| | 10.2. Content Commitment | 0 | | | 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 | 1 | | | Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras |
| | 10.4. Data Encipherment | 0 | | | Se utiliza para cifrar datos que no sean claves criptográficas. |
| | 10.5. Key Agreement | 0 | | | Para uso en el proceso de acuerdo de claves |
| | 10.6. Key Certificate Signature | 0 | | | Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación. |
| | 10.7. CRL Signature | 0 | | | Se permite para firmar listas de revocación de certificados. |
| 11. Extended Key Usage | | Uso mejorado o extendido de las claves | Sí | No | 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 |

| Campo | | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|---|
| | | | | | | básicos que se indican en la extensión KeyUsage. |
| | 11.1. Server Authentication | | 1.3.6.1.5.5.7.3.1 | Sí | | Autenticación de servidor |
| | 11.2. Client Authentication | | 1.3.6.1.5.5.7.3.2 | Si | | Autenticación de cliente |
| 12. Qualified Certificate Statements | | | Extensiones cualificadas. | Sí | No | ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados |
| | QcEuRetentionPeriod (0.4.0.1862.1.3) | | 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.". |
| | QcType (0.4.0.1862.1.6) | | qct-web ( 0.4.0.1862.1.6.3) | | | Certificado de autenticación web |
| | QcPDS (0.4.0.1862.1.5) | | {https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en} | Sí | | Lugar donde se encuentra la declaración PDS, así como el idioma del documento. |
| 13. Certificate Policies | | | Política de certificación | Sí | No | |
| | 13.1. Policy Identifier | | 2.23.140.1.2.2 (organization-validated) | Sí | | {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2) |
| | 13.2. Policy Identifier | | 1.3.6.1.4.1.5734.3.9.16 | Sí | | Identificador de la política asociado a la DPC o PC |
| | 13.2.1 Policy Qualifier Id | | | Sí | | |
| | | 13.2.1.1 CPS Pointer | http://www.cert.fnmt.es/dpcs/ | Sí | | IA5String String. URL de las condiciones de uso. |
| | 13.3. Policy Identifier | | OVCP (0.4.0.2042.1.7) | Sí | | Política de certificación OV para certificados de sitio web acorde al Reglamento UE 910/2014<br><br>itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7) |
| 14. Subject Alternative Names | | | | Sí | No | |
| | 14.1. DNSName | | Id Campo / Valor: | Sí | | Dominio para el que se emite el certificado |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | | NombreDNS = Dominio | | | |
| 15. CRL Distribution Point | | Informa acerca de cómo se obtiene la información de la CRL asociada al certificado. | Sí | No | |
| | 15.1. Distribution Point 1 | Punto de publicación de la CRL1.<br>ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint<br>*xxx: número entero identificador de la CRL (CRL particionadas) | Sí | | Ruta del servicio LDAP donde reside la CRL (punto de distribución 1). |
| | 15.2. Distribution Point 2 | Punto de publicación de la CRL2.<br>http://www.cert.fnmt.es/crlscomp/CRLnnn.crl<br>*nnn: número entero identificador de la CRL (CRL particionadas) | Sí | | Ruta donde reside la CRL (punto de distribución 2). |
| 16. Authority Info Access | | | Sí | No | |
| | 16.1. Access Method 1 | Identificador de método de acceso a la información de revocación:<br>1.3.6.1.5.5.7.48.1 (ocsp) | Sí | | |
| | 16.2. Access Location 1 | http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder | Sí | | |
| | 16.3. Access Method 2 | Identificador de método de acceso a la información de certificados adicionales necesarios para la validación:<br>1.3.6.1.5.5.7.48.2 (ca cert) | Sí | | Entidad emisora de los certificados (CA Subordinada)<br>De la rfc 5280: "*the id-ad-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.*" |
| | 16.4. Access Location 2 | http://www.cert.fnmt.es/certs/ACCOMP.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 la raíz de la FNMT-RCM. |
| 17. Basic Contraints | | 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. Subject Type | Valor FALSE (entidad final) | | | Con este certificado no se pueden emitir otros certificados. |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| 18. Extension SCTs para certificate transparency | | Se incluiran 3 SCTs de diversos servidores de logs de transparencia | Sí | No | OID 1.3.6.1.4.1.11129.2.4.2<br>Especificada en RFC 6962 |

### 2.2.3. Certificado de autenticación de sitio web wildcard

| Campo | | Contenido | Obligatoriedad | Criticidad | 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>Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- $2^{159}$).<br>El número de serie se asignará de forma aleatoria. |
| 3. Signature Algorithm | | Sha256withRsaEncryption | Sí | | Identificando el tipo de algoritmo<br>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).<br>O=FNMT-RCM. | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 4.3. Organization Unit | OU=AC Componentes Informáticos | Sí | | UTF8 String, tamaño máximo 128 (rfc5280). |
| 5. Validity | | 12 meses | Sí | | La vigencia máxima es de 12 meses. |
| 6. Subject | | Identificación/descripción del suscriptor del certificado y del componente | 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. LocalityName | Nombre de la localidad del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>L=Madrid |
| | 6.3. Organization | Denominación del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>O=Ministerio de Economía |
| | 6.4. Serial Number | NIF del suscriptor | Sí | | PrintableString (rfc5280). Por ejemplo:<br>SN= Q0000000J |
| | 6.5. OrganizationIdentifier | Identificador de la Organización | Sí | | Por ejemplo: organizationidentifier=VATES-Q0000000J |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | | Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad) | | | |
| | 6.6. Common Name | Dominio wildcard para el que se expide el certificado. | Sí | | UTF8String (rfc5280). Por ejemplo: CN=*.cert.fnmt.es |
| 7. Authority Key Identifier | | Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente. | Sí | No | 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>Coincide con el campo Subject Key Identifier de la CA emisora. |
| 8. Subject Public Key Info | | Clave pública del componente, codificada según el estándar PKCS#1 de RSA.<br>La longitud de la clave será 2048 bits. | Sí | No | Campo que contiene la clave pública del certificado. |
| 9. Subject Key Identifier | | Identificador de la clave pública del componente. | Sí | No | 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 | | | Permite realizar la operación de firma electrónica |
| | 10.2. Content Commitment | 0 | | | 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 | 1 | | | Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras |
| | 10.4. Data Encipherment | 0 | | | Se utiliza para cifrar datos que no sean claves criptográficas. |
| | 10.5. Key Agreement | 0 | | | Para uso en el proceso de acuerdo de claves |
| | 10.6. Key Certificate Signature | 0 | | | Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación. |
| | 10.7. CRL Signature | 0 | | | Se permite para firmar listas de revocación de certificados. |
| 11. Extended Key Usage | | Uso mejorado o extendido de las claves | Sí | No | 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. Server Authentication | 1.3.6.1.5.5.7.3.1 | Sí | | Autenticación de servidor |

| Campo | | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|---|
| | 11.2. Client Authentication | | 1.3.6.1.5.5.7.3.2 | Si | | 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. QcEuRetentionPeriod (0.4.0.1862.1.3) | | 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.". |
| | 12.2. QcType (0.4.0.1862.1.6) | | qct-web (0.4.0.1862.1.6.3) | | | Certificado de autenticación web |
| | 12.3. QcPDS (0.4.0.1862.1.5) | | {https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en} | Sí | | Lugar donde se encuentra la declaración PDS, así como el idioma del documento. |
| 13. Certificate Policies | | | Política de certificación | Sí | No | |
| | 13.1. Policy Identifier | | 2.23.140.1.2.2 (organization-validated) | Sí | | {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2), |
| | 13.2. Policy Identifier | | 1.3.6.1.4.1.5734.3.9.17 | Sí | | Identificador de la política asociado a la DPC o PC |
| | 13.2.1 Policy Qualifier Id | | | Sí | | |
| | | 13.2.1.1 CPS Pointer | http://www.cert.fnmt.es/dpcs/ | Sí | | IA5String String. URL de las condiciones de uso. |
| | 13.3. Policy Identifier | | OVCP (0.4.0.2042.1.7) | Sí | | Política de certificación OV para certificados de sitio web acorde al Reglamento UE 910/2014<br>itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7) |
| 14. Subject Alternative Names | | | | Sí | No | |
| | 14.1. DNSName | | Id Campo / Valor:<br>NombreDNS = Dominio wildcard | Sí | | Dominio para el que se emite el certificado |
| | 14.2. DNSName | | Nombre de dominio base | Sí | | UTF8 String, tamaño máximo 128.<br>Por ejemplo: |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | | | | | DNSName = www.xxxxxx.es |
| 15. CRL Distribution Point | | Informa acerca de cómo se obtiene la información de la CRL asociada al certificado. | Sí | No | |
| | 15.1. Distribution Point 1 | Punto de publicación de la CRL1.<br>http://www.cert.fnmt.es/crlscomp/CRLnnn.crl<br>*nnn: número entero identificador de la CRL (CRL particionadas) | Sí | | Ruta donde reside la CRL (punto de distribución 1). |
| 16. Authority Info Access | | | Sí | No | |
| | 16.1. Access Method 1 | Identificador de método de acceso a la información de revocación:<br>1.3.6.1.5.5.7.48.1 (ocsp) | Sí | | |
| | 16.2. Access Location 1 | http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder | Sí | | |
| | 16.3. Access Method 2 | Identificador de método de acceso a la información de certificados adicionales necesarios para la validación:<br>1.3.6.1.5.5.7.48.2 (ca cert) | Sí | | Entidad emisora de los certificados (CA Subordinada)<br>De la rfc 5280: "*the id-ad-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.*" |
| | 16.4. Access Location 2 | http://www.cert.fnmt.es/certs/ACCOMP.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 la raíz de la FNMT-RCM. |
| 17. Basic Contraints | | 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. Subject Type | Valor FALSE (entidad final) | | | Con este certificado no se pueden emitir otros certificados. |
| 18. Extension SCTs para certificate transparency | | Se incluiran 3 SCTs de diversos servidores de logs de transparencia | Sí | No | OID 1.3.6.1.4.1.11129.2.4.2<br>Especificada en RFC 6962 |

### 2.2.4. Certificado de autenticación de sitio web multidominio (SAN / UCC)

| Campo | | Contenido | Obligatoriedad | Criticidad | 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>Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- $2^{159}$).<br>El número de serie se asignará de forma aleatoria. |
| 3. Signature Algorithm | | Sha256withRsaEncryption | Sí | | Identificando el tipo de algoritmo<br>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).<br>O=FNMT-RCM. | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 4.3. Organization Unit | OU=AC Componentes Informáticos | Sí | | UTF8 String, tamaño máximo 128 (rfc5280). |
| 5. Validity | | 12 meses | Sí | | La vigencia máxima es de 12 meses. |
| 6. Subject | | Identificación/descripción del suscriptor del certificado y del componente | 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. LocalityName | Nombre de la localidad del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>L=Madrid |
| | 6.3. Organization | Denominación del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>O=Ministerio de Economía |
| | 6.4. Serial Number | NIF del suscriptor | Sí | | PrintableString (rfc5280). Por ejemplo:<br>SN= Q0000000J |
| | 6.5. OrganizationIdentifier | Identificador de la Organización | Sí | | Por ejemplo:<br>organizationidentifier=VATES-Q0000000J |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | | Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad) | | | |
| | 6.6. Common Name | Dominio principal para el que se expide el certificado | Sí | | UTF8String (rfc5280).<br>CN=www.fnmt.es |
| 7. Authority Key Identifier | | Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente. | Sí | No | 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>Coincide con el campo Subject Key Identifier de la CA emisora. |
| 8. Subject Public Key Info | | Clave pública del componente, codificada según el estándar PKCS#1 de RSA.<br>La longitud de la clave será 2048 bits. | Sí | No | Campo que contiene la clave pública del certificado. |
| 9. Subject Key Identifier | | Identificador de la clave pública del componente. | Sí | No | 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. | No | Sí | Normalizado en norma X509 |
| | 10.1. Digital Signature | 1 | 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 | 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. Se utiliza en los certificados de autoridades de certificación. |
| | 10.7. CRL Signature | 0 | Sí | | Se permite para firmar listas de revocación de certificados. |
| 11. Extended Key Usage | | Uso mejorado o extendido de las claves | Sí | No | 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. Server Authentication | 1.3.6.1.5.5.7.3.1 | Sí | | Autenticación de servidor |

| Campo | | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|---|
| | 11.2. Client Authentication | | 1.3.6.1.5.5.7.3.2 | Si | | 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. QcEuRetentionPeriod (0.4.0.1862.1.3) | | 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.". |
| | 12.2. QcType (0.4.0.1862.1.6) | | qct-web (0.4.0.1862.1.6.3) | Sí | | Certificado de autenticación web |
| | 12.3. QcPDS (0.4.0.1862.1.5) | | {https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en} | Sí | | Lugar donde se encuentra la declaración PDS, así como el idioma del documento. |
| 13. Certificate Policies | | | Política de certificación | Sí | No | |
| | 13.1. Policy Identifier | | 2.23.140.1.2.2 (organization-validated) | Sí | | {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2), |
| | 13.2. Policy Identifier | | 1.3.6.1.4.1.5734.3.9.18 | Sí | | Identificador de la política asociado a la DPC o PC |
| | 13.2.1 Policy Qualifier Id | | | Sí | | |
| | | 13.2.1.1 CPS Pointer | http://www.cert.fnmt.es/dpcs/ | Sí | | IA5String String. URL de las condiciones de uso. |
| | 13.3. Policy Identifier | | OVCP (0.4.0.2042.1.7) | Sí | | Política de certificación OV para certificados de sitio web acorde al Reglamento UE 910/2014<br>itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7) |
| 14. Subject Alternative Names | | | | Sí | No | |
| | 14.1. DNSName | | Id Campo / Valor:<br>NombreDNS = Dominio | Sí | | Dominio para el que se emite el certificado |
| | 14.2. DNSName | | Id Campo / Valor:<br>NombreDNS = Dominio_2 | Sí | | Dominio para el que se emite el certificado |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | 14.3. DNSName | Id Campo / Valor:<br><br>NombreDNS = Dominio_*n* | No | | Dominio para el que se emite el certificado<br><br>n <= 12 |
| 15. CRL Distribution Point | | Informa acerca de cómo se obtiene la información de la CRL asociada al certificado. | Sí | No | |
| | 15.1. Distribution Point 1 | Punto de publicación de la CRL1.<br><br>http://www.cert.fnmt.es/crlscomp/CRLnnn.crl<br><br>*nnn: número entero identificador de la CRL (CRL particionadas) | Sí | | Ruta donde reside la CRL (punto de distribución 1). |
| 16. Authority Info Access | | | Sí | No | |
| | 16.1. 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 | | |
| | 16.2. Access Location 1 | http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder | Sí | | |
| | 16.3. Access Method 2 | Identificador de método de acceso a la información de certificados adicionales necesarios para la validación:<br><br>1.3.6.1.5.5.7.48.2 (ca cert) | Sí | | Entidad emisora de los certificados (CA Subordinada)<br><br>De la rfc 5280: "*the id-ad-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.*" |
| | 16.4. Access Location 2 | http://www.cert.fnmt.es/certs/ACCOMP.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 la raíz de la FNMT-RCM. |
| 17. Basic Contraints | | 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. Subject Type | Valor FALSE (entidad final) | | | Con este certificado no se pueden emitir otros certificados. |
| 18. Extension SCTs para certificate transparency | | Se incluiran 3 SCTs de diversos servidores de logs de transparencia | Sí | No | OID 1.3.6.1.4.1.11129.2.4.2<br><br>Especificada en RFC 6962 |

### 2.2.5. Certificado cualificado de autenticación de sitio web estándar

| Campo | | Contenido | Obligatoriedad | Criticidad | 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>Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- $2^{159}$).<br>El número de serie se asignará de forma aleatoria. |
| 3. Signature Algorithm | | Sha256withRsaEncryption | Sí | | Identificando el tipo de algoritmo<br>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).<br>O=FNMT-RCM. | Sí | | UTF8 String, tamaño máximo 128 (rfc5280) |
| | 4.3. Organization Unit | OU=AC Componentes Informáticos | Sí | | UTF8 String, tamaño máximo 128 (rfc5280). |
| 5. Validity | | 12 meses | Sí | | La vigencia máxima es de 12 meses. |
| 6. Subject | | Identificación/descripción del suscriptor del certificado y del componente | 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. LocalityName | Nombre de la localidad del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>L=Madrid |
| | 6.3. Organization | Denominación del suscriptor | Sí | | UTF8String (rfc5280). Por ejemplo:<br>O=Ministerio de Economía |
| | 6.4. Serial Number | NIF del suscriptor | Sí | | PrintableString (rfc5280). Por ejemplo:<br>SN= Q0000000J |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | 6.5. OrganizationIdentifier | Identificador de la Organización<br><br>Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad) | Sí | | Por ejemplo: organizationidentifier=VATES-Q0000000J |
| | 6.6. Common Name | Dominio para el que se expide el certificado | Sí | | UTF8String (rfc5280).<br><br>CN=www.fnmt.es |
| 7. Authority Key Identifier | | Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente. | Sí | No | 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 CA emisora. |
| 8. Subject Public Key Info | | Clave pública del componente, codificada según el estándar PKCS#1 de RSA.<br><br>La longitud de la clave será 2048 bits. | Sí | No | Campo que contiene la clave pública del certificado. |
| 9. Subject Key Identifier | | Identificador de la clave pública del componente. | Sí | No | 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 | | | Permite realizar la operación de firma electrónica |
| | 10.2. Content Commitment | 0 | | | 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 | 1 | | | Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras |
| | 10.4. Data Encipherment | 0 | | | Se utiliza para cifrar datos que no sean claves criptográficas. |
| | 10.5. Key Agreement | 0 | | | Para uso en el proceso de acuerdo de claves |
| | 10.6. Key Certificate Signature | 0 | | | Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación. |
| | 10.7. CRL Signature | 0 | | | Se permite para firmar listas de revocación de certificados. |
| 11. Extended Key Usage | | Uso mejorado o extendido de las claves | Sí | No | 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 |

| Campo | | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|---|
| | | | | | | básicos que se indican en la extensión KeyUsage. |
| | 11.1. Server Authentication | | 1.3.6.1.5.5.7.3.1 | Sí | | Autenticación de servidor |
| | 11.2. Client Authentication | | 1.3.6.1.5.5.7.3.2 | Si | | Autenticación de cliente |
| 12. Qualified Certificate Statements | | | Extensiones cualificadas. | Sí | No | ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados |
| | QcCompliance. (0.4.0.1862.1.1) | | Indica que el certificado es cualificado | Sí | | Obligatorio según ETSI EN 319 412-5 |
| | QcEuRetentionPeriod (0.4.0.1862.1.3) | | 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.". |
| | QcType (0.4.0.1862.1.6) | | qct-web ( 0.4.0.1862.1.6.3) | | | Certificado de autenticación web |
| | QcPDS (0.4.0.1862.1.5) | | {https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en} | Sí | | Lugar donde se encuentra la declaración PDS, así como el idioma del documento. |
| 13. Certificate Policies | | | Política de certificación | Sí | No | |
| | 13.1. Policy Identifier | | 2.23.140.1.2.2 (organization-validated) | Si | | joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2), |
| | 13.2. Policy Identifier | | 1.3.6.1.4.1.5734.3.9.21 | Sí | | Identificador de la política asociado a la DPC o PC |
| | 13.2.1 Policy Qualifier Id | | | Sí | | |
| | | 13.2.1.1 CPS Pointer | http://www.cert.fnmt.es/dpcs/ | Sí | | IA5String String. URL de las condiciones de uso. |
| | 13.3. Policy Identifier | | QNCP-w (0.4.0.194112.1.5) | Sí | | Política de certificación OV para certificados de sitio web acorde al Reglamento UE 910/2014<br><br>itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7) |
| 14. Subject Alternative Names | | | | Sí | No | |

| Campo | | Contenido | Obligatoriedad | Criticidad | Especificaciones |
|---|---|---|---|---|---|
| | 14.1. DNSName | Id Campo / Valor:<br>NombreDNS = Dominio | Sí | | Dominio para el que se emite el certificado |
| 15. CRL Distribution Point | | Informa acerca de cómo se obtiene la información de la CRL asociada al certificado. | Sí | No | |
| | 15.1. Distribution Point 1 | Punto de publicación de la CRL1.<br>http://www.cert.fnmt.es/crlscomp/CRLnnn.crl<br>*nnn: número entero identificador de la CRL (CRL particionadas) | Sí | | Ruta donde reside la CRL (punto de distribución 1). |
| 16. Authority Info Access | | | Sí | No | |
| | 16.1. Access Method 1 | Identificador de método de acceso a la información de revocación:<br>1.3.6.1.5.5.7.48.1 (ocsp) | Sí | | |
| | 16.2. Access Location 1 | http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder | Sí | | |
| | 16.3. Access Method 2 | Identificador de método de acceso a la información de certificados adicionales necesarios para la validación:<br>1.3.6.1.5.5.7.48.2 (ca cert) | Sí | | Entidad emisora de los certificados (CA Subordinada)<br>De la rfc 5280: "*the id-ad-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.*" |
| | 16.4. Access Location 2 | http://www.cert.fnmt.es/certs/ACCOMP.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 la raíz de la FNMT-RCM. |
| 17. Basic Contraints | | 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. Subject Type | Valor FALSE (entidad final) | | | Con este certificado no se pueden emitir otros certificados. |
| 19. Extension SCTs para certificate transparency | | Se incluiran 3 SCTs de diversos servidores de logs de transparencia | Sí | No | OID 1.3.6.1.4.1.11129.2.4.2<br>Especificada en RFC 6962 |