

## AC CAMERFIRMA CERTIFICADO DE SEDE ELECTRÓNICA NIVEL ALTO

Son certificados X.509 versión 3, firmados con el algoritmo sha1WithRSAEncryption por la CA de Camerfirma "AC Camerfirma AAPP" que es subordinada de la CA raíz "Chambers of Commerce Root", que es reconocida por los principales navegadores.

Su duración es de 3 años.

El algoritmo de clave pública es rsaEncryption con clave RSA de 2048 bits.

El uso de la clave es:

- digitalSignature
- keyEncipherment

El uso extendido de la clave es:

- clientAuth
- emailProtection

Tienen declaración de certificado cualificado:

- QcCompliance presente
- QcEuRetention Period igual a 15 años
- QcSSCD presente

El asunto del certificado está compuesto por los siguientes campos:

- Country = Código de país de dos dígitos según ISO 3166-1.
- O = Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado).
- OU = "sede electrónica".
- OU = El nombre descriptivo de la sede.
- Serial Number = Número secuencial único asignado por el prestador (no deberá haber repetidos), se recomienda usar el NIF de la entidad.
- Common Name = Denominación de nombre de dominio (DNS o IP) donde residirá el certificado.

El Subject Alternative Name del certificado está compuesto por los siguientes campos:

- rfc822Name = Correo electrónico de contacto de la entidad suscriptora del sello electrónico.
- dnsName =
  - 2.16.724.1.3.5.1.2.1 = sede electrónica
  - 2.16.724.1.3.5.1.2.2 = Nombre de la entidad suscriptora
  - 2.16.724.1.3.5.1.2.3 = NIF entidad suscriptora
  - 2.16.724.1.3.5.1.2.4 = Nombre descriptivo de la sede electrónica
  - 2.16.724.1.3.5.1.2.5 = Denominación de nombre de dominio IP

Las políticas de certificación bajo las que se emiten estos certificados pueden encontrarse en

<https://policy.camerfirma.com> y su OID es 1.3.6.1.4.1.17326.1.3.2.1.[1-2].[1-2].