

## AC CAMERFIRMA CERTIFICADO DE SELLO DE ORGANO 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.

Estos certificados sólo se emiten en soporte HW cualificado.

El uso de la clave es:

- digitalSignature
- contentCommitment
- keyEncipherment
- dataEncipherment

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 = "sello electrónico".
- Serial Number = Número secuencial único asignado por el prestador (no deberá haber repetidos), se recomienda usar el NIF de la entidad.
- Surname = Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI.
- Given Name = Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte).
- Common Name = Denominación de sistema o aplicación de proceso automático.

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 =
  - 2.16.724.1.3.5.2.1.1 = sello electrónico
  - 2.16.724.1.3.5.2.1.2 = Nombre de la entidad suscriptora
  - 2.16.724.1.3.5.2.1.3 = NIF entidad suscriptora
  - 2.16.724.1.3.5.2.1.4 = DNI/NIE del responsable del Sello
  - 2.16.724.1.3.5.2.1.5 = Denominación de sistema o componente
  - 2.16.724.1.3.5.2.1.6 = Nombre de pila del responsable del certificado
  - 2.16.724.1.3.5.2.1.7 = Primer apellido del responsable del certificado
  - 2.16.724.1.3.5.2.1.8 = Segundo apellido del responsable del certificado
  - 2.16.724.1.3.5.2.1.9 = Correo electrónico de la persona responsable del certificado

Las políticas de certificación bajo las que se emiten estos certificados pueden encontrarse en <https://policy.camerfirma.com> y su OID es 1.3.6.1.4.1.17326.1.3.3.1.[1-2].[1-2].