

RACER CERTIFICADO DE PERSONA FÍSICA

Son certificados X.509 versión 3, firmados con el algoritmo sha1WithRSAEncryption por la CA de Camerfirma "RACER" que es subordinada de la CA intermedia "AC Camerfirma" que es subordinada de la CA raíz "Global Chambersign Root", que es reconocida por los principales navegadores.

Su duración es de 2 años.

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

El uso de la clave es:

- digitalSignature
- contentCommitment
- keyEncipherment
- dataEncipherment
- keyAgreement

El uso extendido de la clave es:

- clientAuth
- emailProtection

Tienen declaración de certificado cualificado:

- QcCompliance
presente
- QcEuLimitValue igual a 0 EUR

El asunto del certificado está compuesto por los siguientes campos:

- Country = ES
- Common Name = Nombre y apellidos del suscriptor
- Email Address = Email del suscriptor
- Surname = Apellidos del suscriptor
- Given Name = Nombre del suscriptor
- 1.6.6 1.3.6.1.4.1.17326.30.4 = Tipo de documento identificativo del suscriptor
- Serial Number = Número del documento identificativo del suscriptor
- L = Localidad del suscriptor
- ST = Provincia del suscriptor
- Description = Qualified Certificate: RACER-PF-SW-KPSC

Las políticas de certificación bajo las que se emiten estos certificados pueden encontrarse en <https://policy.camerfirma.com> y su OID es 1.3.6.1.4.1.17326.10.8.6.[1-2].[1-2].