

## **CAMERFIRMA EXPRESS CORPORATE SERVER CERTIFICADO DE SERVIDOR**

Son certificados X.509 versión 3, firmados con el algoritmo sha1WithRSAEncryption por la CA de Camerfirma "AC Camerfirma Express Corporate Server v3" que es subordinada de la CA raíz "Chambers of Commerce Root", que es reconocida por los principales navegadores.

Su duración puede ser de 1, 2, 3 o 4 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:

- serverAuth

El asunto del certificado está compuesto por los siguientes campos:

- Country = ES
- Common Name = URL
- Email Address = Email del suscriptor
- Serial Number = CIF de la organización del suscriptor
- O = Organización del suscriptor
- OU = Departamento de la organización del suscriptor
- L = Localidad del suscriptor
- ST = Provincia del suscriptor

Las políticas de certificación bajo las que se emiten estos certificados pueden encontrarse en <https://policy.camerfirma.com> y su OID es 1.3.6.1.4.1.17326.10.11.2

En el userNotice del certificado llevan una declaración:

"Certificado de Servidor Seguro Camerfirma Express Corporate Server perteneciente a la empresa con identificación fiscal CIF=<CIF de la organización del suscriptor>"