

AC CAMERFIRMA CERTIFICADO DE EMPLEADO PÚBLICO NIVEL ALTO CIFRADO

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:

- 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 Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.
- OU = "certificado electrónico de empleado público"
- OU = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado
- OU = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP [opcional].
- T = Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.
- Serial Number = Número secuencial único asignado por el prestador (no deberá haber repetidos), se recomienda usar el DNI/NIE del empleado público.
- 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 = Se recomienda introducir el nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI.

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

- rfc822Name = Correo electrónico de la persona responsable del certificado.
- dnsName =
 - 2.16.724.1.3.5.3.1.1 = certificado electrónico de empleado público
 - 2.16.724.1.3.5.3.1.2 = Nombre de la entidad suscriptora
 - 2.16.724.1.3.5.3.1.3 = NIF entidad suscriptora
 - 2.16.724.1.3.5.3.1.4 = DNI/NIE del responsable
 - 2.16.724.1.3.5.3.1.5 = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP
 - 2.16.724.1.3.5.3.1.6 = Nombre de pila del responsable del certificado
 - 2.16.724.1.3.5.3.1.7 = Primer apellido del responsable del certificado
 - 2.16.724.1.3.5.3.1.8 = Segundo apellido del responsable del certificado
 - 2.16.724.1.3.5.3.1.9 = Correo electrónico de la persona responsable del certificado
 - 2.16.724.1.3.5.3.1.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado
 - 2.16.724.1.3.5.3.1.11 = Puesto desempeñado por el suscriptor del certificado dentro de la administración

Las políticas de certificación bajo las que se emiten estos certificados pueden encontrarse en <https://policy.camerfirma.com> y su OID es 1.3.6.1.4.1.17326.1.3.4.3.[1-2].2