# Política de Certificación de Certificados de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Sede Electrónica y Sede Electrónica con Validación Extendida (Sede EV). Perfil de Certificado







Paseo de la Castellana, 79 – 28046 - Madrid (España)
Teléfono: 902 902 172 (llamadas desde España)
Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

**Nivel de Seguridad**

Público

---

**Aviso Importante**



Dirección: Paseo de la Castellana, 79. 28046 Madrid (España)

Teléfono: 902 902 172 (llamadas desde España) Internacional (+34) 933 935 946

Fax: (+34) 933 031 611. Web: www.anf.es

# Certificado de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Sede Electrónica y Sede Electrónica con Validación Extendida (Sede EV)

**(AUTENTICACION) (FIRMA) (CIFRADO)**
**TOKEN POR SOFTWARE - TOKEN HSM**

| Campo | Valor | | Crít | Oblig |
|---|---|---|---|---|
| Versión | 2 = (V3) | | | SI |
| Número de serie | | | | SI |
| Algoritmo de firma.<br><br>*SignatureAlgorithm* | sha256WithRSAEncryption | | | SI |
| Algoritmo Hash de firma<br><br>*SignatureHashAlgorithm* | sha256 | | | SI |
| **Emisor** | Common Name<br><br>(CN) | *p.e. ANF Assured ID CA1* | | SI |
| | SERIALNUMBER | G63287510 | | SI |
| | Organisation Identifier | *Se trata del VAT number, en España denominado NIF-IVA no es el CIF. Es el NIF para el IVA en la UE*<br><br>*En la actualidad ANF AC no lo incluye* | | |
| | EmailAddress (E) | info@anf.es | | |
| | Organisational Unit (OU) | Unidad organizativa dentro del Prestador de Servicios de Certificación responsable de la emisión del certificado | | SI |
| | Organisation (O) | *p.e. ANF Autoridad de Certificacion* | | SI |
| | Locality (L) | *p.e. Barcelona (ver dirección actual en http://www.anf.es/es/address-direccion.html* | | |
| | State (ST) | *p.e. Barcelona* | | |
| | Country (C) | *p.e. ES* | | SI |
| AuthorityCertIssuer | | | | |
| AuthorityCertSerial Number | | | | |
| Identificador de la clave de la entidad emisora –<br><br>*Authority KeyIdentifier* | Hash con SHA1 de la clave pública utilizada para<br><br>firmar el certificado | | | SI |

| | | | | | |
|---|---|---|---|---|---|
| *Issuer Alternative Name* | | | | | |
| Válido desde<br><br>*NotBefore* | | | | | SI |
| Válido hasta<br><br>*NotAfter* | | | | | SI |
| **Sujeto**<br><br>*(todos los campos codificados utilizando UTF-8)* | *Subject* | | | | |
| | Country (C) | *País del sujeto=suscriptor* | | | SI |
| | Locality (L) | *Ciudad del sujeto* | | | SI |
| | State (ST) | *Provincia del sujeto* | | | SI |
| | EmailAddress (E) | *Email del sujeto* | | | |
| | SERIAL NUMBER (SN) | *Por ejemplo*<br><br>*p. ej.: IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad* | | | SI |
| | OrganizationIdentifier | *El certificado debe de incluir al menos = Serial Number o OrganizationIdentifier (NIF-IVA), p.e.*<br><br>*VATES-B0085974Z* | | | |
| | OrganizationName (O) | *p. ej.: Nombre empresa. S.L.* | | | SI |
| | Given Name (G) | *Nombre de pila del representante legal, de acuerdo con documento de identidad (DNI/Pasaporte)* | | | SI |
| | SurName (SN) | *Apellidos del representante legal.*<br><br>*Primer apellido, espacio en blanco, segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte* | | | SI |
| | Common Name<br><br>(CN) | *p.e.* anf.es | | | SI |
| | Organisational Unit (OU) | **SSL DV** | *Certificado de Servidor Seguro SSL DV* | | SI |
| | | **SSL OV** | *Certificado de Servidor Seguro SSL OV* | | |
| | | **SSL EV** | *Certificado de Servidor Seguro SSL EV* | | |
| | | **Sede Nivel Medio** | *Certificado de Sede Electronica Nivel Medio* | | |
| | | **Sede EV Nivel Medio** | Certificado de Sede Electronica EV Nivel Medio | | |
| | | **Sede Nivel Alto** | Certificado de Sede Electronica | | SI |

| | | | | | |
|---|---|---|---|---|---|
| | | | Nivel Alto | | |
| | | **Sede EV Nivel Alto** | Certificado de Sede Electronica EV Nivel Alto | | SI |
| | Organisational Unit (OU) | **Certificado de SEDE ELECTRONICA** | *p. ej.: PUNTO DE ACCESO GENERAL* | | |
| | businessCategory | PrivateOrganization | *para organización privada* | | SI |
| | | GovernmentEntity | *para entidad pública* | | |
| | | BusinessEntity | *para empresa* | | |
| | | Non-commercialEntity | *para entidad no comercial* | | |
| | JurisdictionCountryName | Solo certificados EV | *p. ej. ES* | | SI |
| | JurisdictionOfIncorporationLocalityName | Solo certificados EV | *p. ej. Badalona* | | |
| | JurisdictionOfIncorporationStateOrProvinceName | Solo certificados EV | *p. ej. Barcelona* | | |
| Nombre alternativo del sujeto – SubjectAlternativeName | Nombre alternativo del sujeto – SubjectAlternativeName - 2.5.29.17 | | | | |
| | *eMail ejemplo: pedro@cial.com* | | | | SI |
| | *DNSName* | *p.e. anf.es* | | | |
| | *Directory Name* | *frater.es* | | | |
| SubjectDirectoryAttributes | *SubjectDirectoryAttributes – 2.5.29.9* | | | | |
| | 2.5.4.20 | *TelephoneNumber* | | | |
| | 2.5.4.23 | *Facsimile* | | | |
| | 2.5.4.9 | *StreetAddress* | | | |
| | 2.5.4.16 | *PostalAddress* | | | |
| | 2.5.4.17 | *PostalCode* | | | |
| Identificador de la clave del sujeto - Subject Key Identifier | Hash en SHA1 de la clave pública utilizada para firmar el certificado | | | | SI |
| SubjectPublic KeyInfo | RSA (2048) | | | | SI |
| Acceso a la información de entidad emisora | AccessMethod [1] | *[1]Acceso a información de autoridad* *Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)* | | | SI |
| | AccessLocation [1] | *Nombre alternativo: Dirección URL=http://* | | | SI |

| | | | | | |
|---|---|---|---|---|---|
| | AccessMethod [2] | *1.3.6.1.5.5.7.48.2* | | | |
| | AccessLocation [2] | *Dirección URL=* | | | |
| Puntos de distribución CRL | cRLDistributionPoint [1] | *1]Punto de distribución CRL*<br>*Nombre del punto de distribución:*<br>*Nombre completo:*<br>*Dirección URL* | | | SI |
| Declaraciones de certificados reconocidos<br>*Qualified Certificate Statement*<br>TSI EN 319 412-1, antes ETSI TS 101 862 | QcCompliance | **SOLO EV** | ***Presente** si el certificado es expedido con la calificación de reconocido. Anexo I eIDAS* | | SI |
| | QcSSCD | **SOLO EV con HSM** | ***SOLO si el dispositivo es SSCD***<br>Secure Signature Creation Device (SSCD) | | SI |
| | QcType- esign | **SOLO EV**<br>*QcType 3* | *se reseña QcType 3*<br>*ETSI EN 319 412-5* | | SI |
| | QcPDS | **SOLO EV** | *https://anf.es/en/*<br>*URL que permite acceder a todas las políticas de la PKI en inglés. Protocolo https*<br>*ETSI EN 319 412-5* | | SI |
| | QcLimitValue | **SOLO EV** | *Importe límite de responsabilidad asumido por el emisor expresado en EUROS* | | SI |
| | QcRetentionPeriod | **SOLO EV** | *Integer: =15*<br>*([ETSI EN 319 412-5]*<br>*describe el periodo de conservación*<br>*de toda la información relevante para el uso de un certificado, tras la*<br>*caducidad de este)* | | SI |
| | semnaticsId-Natural | **SOLO EV** | Para indicar semántica de persona física definida por la EN 319 412-1 | | |
| Directivas del certificado –<br>*Certificate Policies* | PolicyIdentifier | **SSL DV** | [1]Directiva de certificados:<br>Identificador de<br>directiva=1.3.6.1.4.1.18332.55.1.1.1.22 | | SI |
| | | **SSL OV** | [1]Directiva de certificados:<br>Identificador de | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | directiva=1.3.6.1.4.1.18332.55.1.1.7.22 | | |
| | | **SSL EV** | [1]Directiva de certificados:<br>Identificador de directiva=1.3.6.1.4.1.18332.55.1.1.2.22 | | |
| | | **Sede Nivel Medio** | [1]Directiva de certificados:<br>Identificador de<br>directiva=1.3.6.1.4.1.18332.55.1.1.3.22 | | |
| | | **Sede Nivel Medio EV** | [1]Directiva de certificados:<br>Identificador de<br>directiva=1.3.6.1.4.1.18332.55.1.1.5.22 | | |
| | | **Sede Nivel Alto** | [1]Directiva de certificados:<br>Identificador de<br>directiva=1.3.6.1.4.1.18332.55.1.1.4.22 | | |
| | | **Sede Nivel Alto EV** | [1]Directiva de certificados:<br>Identificador de<br>directiva=1.3.6.1.4.1.18332.55.1.1.6.22 | | |
| | PolicyIdentifier | **SSL DV** | 2.23.140.1.2.1 | | SI |
| | | **SSL OV** | 2.23.140.1.2.2 | | |
| | | **SSL EV** | 2.23.140.1.1 | | |
| | | **Si el suscriptor es una persona física** | 2.23.140.1.2.3 | | |
| | | **Sede electrónica NIVEL ALTO** | 2.16.724.1.3.5.5.1 | | |
| | | **Sede electrónica NIVEL MEDIO** | 2.16.724.1.3.5.5.2 | | |
| | PolicyIdentifier | **SSL DV** | 0.4.0.2042.1.6 | | SI |
| | | **SSL OV** | 0.4.0.2042.1.7 | | |
| | | **SSL EV** | 0.4.0.2042.1.4 | | |
| | | **Sede EV** | 0.4.0.2042.1.4 | | |
| | | **Emitido como cualificado + HSM** | 0.4.0.1456.1.1 | | |
| | | [1,1]Información de certificador de directiva:<br>Id. de certificador de directiva=CPS | | | |

| | | | | | |
|---|---|---|---|---|---|
| | PolicyCPSLocation | Certificador:<br>http://www.anf.es/documentos | | | |
| | User notice | [1,2]Información de certificador de directiva:<br>Id. de certificador de directiva=Aviso de usuario<br>Certificador:<br>Texto de aviso=Certificado conforme a la legislación firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados. | | | SI |
| | PolicyIdentifier | SSL EV | 0.4.0.194112.1.4<br>(qcp-web) | | SI |
| | | Sede EV | | | |
| Restricciones básicas<br>*Basic Constraints* | Tipo de asunto=Entidad final<br>Restricción de longitud de ruta=Ninguno<br>CA = FALSE | | | **SI** | |
| Uso de la clave<br>*Key usage* | Digital Signature | Se utiliza cuando se realiza la función de autenticación | | **SI** | |
| | Key Encipherment | Se utiliza para gestión y transporte de claves | | | |
| Uso mejorado de las claves -<br>*Extended key usage* | Autenticación servidor | Autenticación TSL web Server<br>1.3.6.1.5.5.7.3.1 | | | SI |
| | Autenticación del cliente | Autenticación TSL web Cliente<br>1.3.6.1.5.5.7.3.2 | | | |
| | emailProtection | Protección de eMail<br>1.3.6.1.5.5.7.3.4 | | | |
| Algoritmo de identificación | sha1 | | | | SI |
| Signature Value | | | | | SI |
| Huella digital | | | | | SI |