# CERTIFICADOS DE SERVIDOR WEB SSL

*Política de Certificado*

**Versión:** 180719
**Clasificación:** Público

Firmado digitalmente por:
FIRMAPROFESIONAL, S.A.

**ATENCIÓN:** El original vigente de este documento se encuentra en formato electrónico en la web de Firmaprofesional: https://www.firmaprofesional.com/cps

# *Histórico de versiones*

| Versión | Cambios | Fecha publicación |
|---|---|---|
| 6.3 | (para consultar cambios entre versiones anteriores, por favor envíe un correo a info@firmaprofesional.com) | 17/10/2008 |
| 171121 | Cambio de plantilla y numeración de versiones, pasando a seguir el formato AAMMDD (año, mes y día de la publicación).<br><br>Inclusión del presente apartado.<br><br>Sección "1.1 Descripción general":<br>● Se elimina la referencia explícita a la versión de *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"* y *"Guidelines for the issuance and management of Extended Validation certificates"* referenciando a "vigente en el momento de la publicación de la presente política"<br>Sección "2.1 Autoridades de Certificación (CA)":<br>● Se corrige que hasta la versión 6.3 (incluida) de la presente política la emisión se podía realizar desde las CAs subordinadas "***AC Firmaprofesional – CA1***" y "***AC Firmaprofesional - INFRAESTRUCTURA***"<br>Sección "4.3 Verificación de información de larga duración"<br>● Se adecúa el contenido de las verificaciones de información a las duraciones de los certificados.<br>Sección "4.4 Renovación de certificados":<br>● Se simplifica el proceso de renovación, equiparándolo al de nueva emisión.<br>Sección "5 PERFIL DE LOS CERTIFICADOS":<br>● Se elimina el keyUsage "nonRepudiation", que erróneamente aparecía<br>● Se añade el keyUsage "keyAgreement", usado hasta la versión 6.3 (incluída) de la presente política, y eliminado a partir de la actual<br>● Se aclara que el campo "organizationalUnit" es opcional hasta la versión 6.3 (incluida) de la presente política y no está presente en adelante<br>Adaptación a eIDAS | 21/11/2017 |
| 180221 | ● Revisión respecto a *Mozilla Root Store Policy Version 2.5*.<br>● Validez máxima de certificados SSL y EV de 2 años. | 21/02/2018 |

| | | |
|---|---|---|
| 180517 | • Actualizado “4.5. Procedimiento de notificación de problemas por parte del suscriptor en caso problema”<br>• Actualizado “4.1. Proceso de emisión de certificados”: en “a) Solicitud” y “b) Aceptación de la solicitud” | 17/05/2018 |
| 180719 | Se añade el EKU clientAuthentication al perfil | 19/07/2018 |

# *Índice*

# 1. INTRODUCCIÓN

## 1.1. Descripción general

Los **Certificados de Servidor Web SSL** son certificados expedidos a organizaciones para servidores web. La finalidad del certificado es poder autenticar de forma segura el servidor en la red y permitir a los usuarios crear una conexión segura mediante protocolos criptográficos estándar, como SSL o TLS.

Los **Certificados de Servidor Web SSL** son certificados cualificados porque cumplen los requisitos establecidos en el anexo IV del Reglamento UE 910/2014.

En el presente documento se exponen las Condiciones Particulares referentes a este tipo de certificado. Esta Política de Certificación está subordinada al cumplimiento de las Condiciones Generales expuestas en la Declaración de Prácticas de Certificación (CPS) de Firmaprofesional.

Firmaprofesional emite dos tipos de Certificados de Servidor Web SSL:

- **Certificados SSL estándar**:
    - Garantizan que un determinado dominio ha sido registrado a nombre de la organización identificada en el certificado y que la comunicación entre el navegador del cliente y el servidor de páginas es confidencial debido al empleo del protocolo SSL.
    - Se ajustan a los requerimientos del CA/Browser Forum establecidos en el documento ***"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates,"*** vigente en el momento de la publicación de la presente política.
- **Certificados SSL *Extended Validation* (EV)**:
    - Son certificados emitidos a servidores de páginas web expedido de acuerdo con un conjunto específico de criterios de verificación de la identidad de la organización identificada en el certificado.
    - Un certificado SSL EV permite a los navegadores que se conectan a este servicio, mostrar un nivel de seguridad adicional. Esto se indica en el navegador mostrando un fondo verde en la línea de direcciones del navegador.
    - Se ajustan a los requerimientos del CA/Browser Forum establecidos en el documento ***"Guidelines for the issuance and management of Extended Validation certificates"*** vigente en el momento de la publicación de la presente política.

En el caso de cualquier incompatibilidad entre este documento y los requisitos publicados por el CA/Browser Forum, los requisitos tienen prioridad sobre este documento.

## 1.2. Identificación del Documento

| | |
|---|---|
| **Nombre:** | CP Servidor Web |
| **Versión:** | 180719 |
| **Descripción:** | Política de Certificación<br>para Certificados de Servidor Web (SSL) |

| | |
|---|---|
| **Fecha de Emisión:** | 17/05/2018 |
| **OIDs** | 1.3.6.1.4.1.13177.10.1.3.1 SSL Estándar<br>1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Cualificado |
| **Localización** | http://www.firmaprofesional.com/cps |

Anteriormente, esta Política de Certificación recibía el nombre de:

- Tipo II.C - CERTIFICADOS DE SERVIDOR SEGURO (1.3.6.1.4.1.13177.10.1.3.1)

### 1.3. Definiciones y acrónimos

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional (http://www.firmaprofesional.com/cps).

## 2. ENTIDADES PARTICIPANTES

### 2.1. Autoridades de Certificación (CA)

Hasta la fecha, estos certificados se han emitido por la CAs Suborddinadas "***AC Firmaprofesional – CA1***" y "***AC Firmaprofesional - INFRAESTRUCTURA***".

Desde la fecha de publicación de la presente versión de esta política, estos certificados deben ser emitidos únicamente por la CA Subordinada "***AC Firmaprofesional - INFRAESTRUCTURA***".

### 2.2. Autoridad de Registro (RA)

La gestión de las solicitudes y emisiones de los certificados será realizada por Firmaprofesional o por un Intermediario autorizado.

Los Intermediarios autorizados serán entidades registradoras de dominio acreditadas por ICANN con las que Firmaprofesional tenga un acuerdo de colaboración.

### 2.3. Solicitante

Podrá realizar la solicitud de estos certificados en nombre de una organización la persona que aparezca como "Contacto Administrativo" en el registro oficial del dominio.

### 2.4. Suscriptor

El suscriptor del certificado será la organización que aparece como "Registrante" ("*Registrant*") en el registro oficial del dominio.

### 2.5. Tercero que confía en los certificados

Estos certificados están reconocidos por Microsoft en todas sus aplicaciones, incluyendo Internet Explorer, por la Fundación Mozilla, incluyendo el navegador Firefox y por Apple, incluyendo el navegador Safari.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

# 3. CARACTERÍSTICAS DE LOS CERTIFICADOS

## 3.1. Periodo de validez de los certificados

- Certificados SSL estándar: Validez máxima de 2 años.
- Certificados SSL Extended Validation: Validez máxima de 2 años

## 3.2. Certificados extended validation (EV)

Los Certificados de Servidor Web SSL EV permiten a los navegadores que se conectan a este servicio mostrar un nivel de seguridad adicional al de los Certificados de Servidor Web SSL estándar.

Para ello se emiten de acuerdo con un conjunto específico de criterios de verificación de la identidad de la organización identificada en el certificado muy riguroso. Estos criterios requieren una verificación exhaustiva de la identidad de la organización solicitante y de la persona que hace efectiva la solicitud. Mediante la firma electrónica de la solicitud de un Certificado de Servidor Web SSL EV realizada con un Certificado Corporativo de Representante Legal emitido por Firmaprofesional se cubre gran parte de estos requisitos.

## 3.3. Certificados multidominio

Los Certificados de Servidor Web Multidominio permiten validar diferentes URLs del mismo dominio con el mismo certificado.

Esta funcionalidad se consigue utilizando “Caracteres Wildcards” para las URLs tal como se definen en el estándar ***RFC 2818 “HTTP Over TLS”.***

Según este estándar, se permite utilizar el carácter “asterisco” como comodín dentro de una URL. De este modo, un certificado con la URL “*.dominio.com” podrá ser utilizado para cualquier subdominio, como “subdominio1.dominio.com”, “subdominio2.domino.com”, “www.dominio.com”, etc…

El uso de “wildcards” en Certificados de Servidor Web SSL está soportado por los principales navegadores de Internet y resulta muy útil cuando se disponen de muchos subdominios del mismo dominio de Internet y se desea utilizar un único certificado para todos ellos.

**Los Certificados de Servidor Web SSL EV no pueden ser multidominio.**

## 3.4. Nombres de dominio

No se permite la emisión certificados a direcciones IP o Nombres de Dominio internos, privados o reservados.

El uso de nombres de dominio internacionalizados (IDN por sus siglas en inglés) no está permitido bajo esta política de certificado. Esta medida previene ataques de *spoofing* homográfico.

## 3.5. Uso particular de los Certificados

### 3.5.1. Usos apropiados de los certificados

Los Certificados de Servidor Web pueden ser utilizados para autenticar la identidad de un servidor, y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio. En

general estos certificados se utilizarán para autenticar un Servidor Web mediante el protocolo SSL (o TLS).

### 3.5.2. Usos no autorizados de los certificados

No se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Practicas de Certificación.

No se permite el uso de este tipo de certificado para la firma electrónica de documentos. Firmaprofesional dispone de otras políticas de certificado apropiadas para tal fin.

### 3.5.3. Notificación de usos no autorizados, quejas o sugerencias

En caso de detectar un uso no autorizado de los certificados o tener alguna queja o sugerencia, éstas se deben hacer llegar a Firmaprofesional mediante correo electrónico a la dirección soporte@firmaprofesional.com, indicando en el asunto si se trata de un “Uso no autorizado”, una “Queja” o una “Sugerencia” y aportando en el cuerpo del correo y mediante archivos adjuntos la información necesaria para que Firmaprofesional pueda validar la veracidad de las afirmaciones realizadas

## 3.6. Tarifas

Firmaprofesional podrá establecer las tarifas que considere oportunas a los suscriptores, así como establecer los medios de pago que considere más adecuado en cada caso. Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar con el Departamento Comercial de Firmaprofesional.

# 4. PROCEDIMIENTOS OPERATIVOS

## 4.1. Proceso de emisión de certificados

Los pasos a seguir para la obtención del certificado se detallan a continuación:

**a) Solicitud**

Para poder solicitar un Certificados de Servidor Web SSL la organización debe ser la poseedora del dominio.

Los pasos para realizar la solicitud son los siguientes:

1. Ponerse en contacto con Firmaprofesional o con un Intermediario autorizado

2. Enviar por los medios electrónicos (por ejemplo, correo electrónico o formulario web) que Firmaprofesional ponga a disposición de los solicitantes, como mínimo la siguiente información:

    - Datos de la persona de contacto: nombre y apellidos, cargo, teléfono, correo electrónico. Deben coincidir con los datos de la persona que aparezca como "Contacto Administrativo" o "Contacto Técnico" en el registro oficial del dominio.

    - Nombre de dominio (URL para la que se desea emitir el certificado)

    - Razón social y CIF de la organización

Para el caso de Certificados de Servidor SSL EV, los datos anteriores deben incluirse en un contrato firmado electrónicamente por un Certificado Corporativo de Representante Legal de la organización solicitante emitido por Firmaprofesional. También será válido un contrato firmado de manera manuscrita por el representante legal.

Para el caso de Certificados de Servidor SSL Estándar, un representante legal o un apoderado de la organización deberá firmar el contrato de prestación de servicios de certificación electrónica y la hoja de aceptación y entrega. La entidad solicitante deberá enviar a Firmaprofesional una copia escaneada del contrato firmado, acompañada de una fotocopia del DNI del representante legal o apoderado.

En ambos casos, con la firma de estos documentos, el representante legal o apoderado de la entidad solicitante aceptará las condiciones generales de contratación de Firmaprofesional, las DPC y la PC del certificado que se entrega.

**b) Aceptación de la solicitud**

Sin perjuicio de lo establecido en la correspondiente Declaración de Prácticas de Certificación (CPS) de Firmaprofesional, para garantizar que una organización solicitante tiene control sobre el dominio (URL) que solicita incluir en un certificado se realizan las siguientes comprobaciones:

1. Se consultan los siguientes servicios *whois* autenticados:

    - Para dominios "*.es", consultar el siguiente servicio WHOIS autenticado: https://www.nic.es/sgnd/dominio/publicInformacionDominios.action

- Para el resto de dominios, consultar en http://www.iana.org/domains/root/db/ cuál es el servidor WHOIS autorizado para buscar información sobre el dominio, dependiendo del dominio de alto nivel (TLD), es decir, dependiendo de si el dominio acaba en .com, .org, .net, ...

2. Se validarán los datos del solicitante como “Contacto Administrativo” o el “Contacto Técnico” del dominio.

3. Se validarán los datos de la empresa mediante alguno de los siguientes mecanismos:

   - Si se trata de una empresa con vinculación contractual con Firmaprofesional previa a la solicitud, basta con el contrato firmado previamente entre las dos partes previamente.

   - Si no es cliente de Firmaprofesional, se realizará una Consulta al Registro Mercantil. Como alternativa la empresa puede enviar a Firmaprofesional el certificado del Registro Mercantil o Certificado Oficial donde esté registrada.

4. Se deberá firmar el contrato mediante SMS; para ello se solicitará el nº de móvil del representante legal y se le enviará a ese teléfono el contrato. También se podrá firmar con certificado digital. Si no es posible ninguna de las dos opciones anteriores, como última opción, se podrá enviar el contrato escaneado con la firma manuscrita.

5. Se debe confirmar con el solicitante el control del dominio enviando un código aleatorio por correo electrónico. El solicitante deberá responde desde esa dirección de correo electrónico con el código enviado.

   La dirección de correo electrónico del destinatario se extraerá del contacto del dominio del registro. También se puede enviar el correo electrónico a más de un destinatario siempre que éstos sean identificados como representantes del nombre del dominio en el registro.

   En caso de que el registro del dominio no esté visible o los datos no coincidan con los de la empresa solicitante, se enviará un correo solicitando visibilidad al registro.

   Los correos electrónicos válidos serán las direcciones "admin", "administrador", "webmaster", "hostmaster" o "postmaster" seguido de @ y el nombre del dominio de autorización.

   El valor aleatorio debe ser único por lo que se propone que el operador utilice un generador de números aleatorios únicos.

6. El operador de RA deberá almacenar evidencia documental de las validaciones realizadas, por ejemplo, mediante el escaneo de la documentación en papel consultada, impresión de pantalla de los registros electrónicos consultados o anotación de la fecha, hora e interlocutor de las llamadas telefónicas realizadas.

**c) Generación de claves**

Las claves de firma serán generadas en los sistemas del solicitante utilizando sus propias aplicaciones compatibles con los estándares de PKI. Generalmente, las aplicaciones de servidores que pueden configurarse con el protocolo SSL, como IIS de Microsoft, incluyen herramientas para generar claves y peticiones de certificados.

Deben ser claves RSA con una longitud mínima de 2.048 bits.

**d) Tramitación**

El solicitante entregará a Firmaprofesional, directamente o a través de un Intermediario autorizado, una petición de certificado en formato PKCS#10.

Firmaprofesional realizará la validación técnica de la petición PKCS#10 y la validación de los datos que contenga.

**e) Emisión del certificado**

Si la solicitud está firmada electrónicamente mediante un Certificado Corporativo de Representante Legal de Firmaprofesional, ésta emitirá un Certificado de Servidor Web SSL EV; en otro caso, se emitirá un Certificado de Servidor Web SSL estándar.

Adicionalmente, la emisión de Certificado de Servidor Web SSL EV requiere de la aprobación de dos personas: el Operador de la RA encargado de la gestión de la solicitud y Administrador del Departamento Técnico encargado de la emisión del certificado.

**f) Entrega**

Firmaprofesional hará entrega del certificado al solicitante permitiendo su descarga de forma segura desde Internet.

## 4.2. Revocación de certificados

Según se especifica en la Declaración de Prácticas de Certificación (CPS)

## 4.3. Verificación de información de larga duración

La información contenida en los certificados SSL se verificará en cada emisión y renovación.

## 4.4. Renovación de certificados

Se deben seguir los mismos pasos que para la emisión de un nuevo certificado (4.1 Proceso de emisión de certificados)

## 4.5. Procedimiento de notificación de problemas por parte del suscriptor en caso problema

Si el suscriptor de certificados de autenticación Web detecta cualquier problema con el certificado podrá notificarlo por e-mail a soporte@firmaprofesional.com

Cualquier correo que se envía a esta dirección de correo entra en el Sistema de Atención al Cliente de Firmaprofesional.

# 5. PERFIL DE LOS CERTIFICADOS

## 5.1. Nombre distinguido (DN)

| Campo | Valor | Descripción |
|---|---|---|
| CN, Common Name | Nombre | *(EVG 9.2.3) Nombre de un único dominio.*<br>*(BR. 7.1.4.2.2.a) Este dominio debe coincidir con el indicado (o con uno de los indicados) en el Subject Alt Names).* |
| O, Organization | Razón Social | *Nombre Oficial de la Organización subscriptora del certificado* |
| OU, Organizational Unit | Departamento | *Opcional hasta versión 6.3 (incluida) de la presente política. No presente en adelante.*<br>*(BR. 7.1.4.2.2.i) Opcional* |
| serialNumber | CIF | *CIF de la Organización subscriptora del certificado* |
| OrganizationIdentifier | | Identificador de la organización, según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) |
| businessCategory | *Private Organization*<br>*Government Entity*<br>*Business Entity*<br>*Non-Commercial Entity* | (EVG 9.2.4) Business Category |
| L, Locality | Ciudad | Address of Place of Business: City |
| ST, StateOfProvince | Provincia | Provincia de registro de la organización |
| C, Country | País | Código de país de dos dígitos según ISO 3166-1. Por defecto “ES”. |
| jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3 | País | (EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration |

Los campos (EVG 9.2.X) son requerimientos específicos para certificados *Extended Validation* según establece el CA/Browser Forum.

Las indicaciones (BR.X) son requerimientos de la *Baseline Requeriments Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* del CA/Browser Forum, vigente en el momento de la publicación de la presente política.

## 5.2. Extensiones de los certificados

| Extensión | Crítica | Valores |
|---|---|---|
| *X509v3 Subject Alternative Name* | - | *URL, nombre de dominio o identificación del dispositivo o servicio poseedor de las claves o de la aplicación.*<br>*(EVG 9.2.2) Se puede incluir más de 1 dominio, pero no wilcards.* |

| | | |
|---|---|---|
| | | *Para certificados multidominio, la URL seguirá el formato "*.dominio.com" (esta indicación está prohibida para certificados EV)* |
| *X509v3 Basic Constraints* | *Sí* | *CA:FALSE* |
| *X509v3 Key Usage* | *Sí* | *Digital Signature*<br>*Key Encipherment*<br>*Data Encipherement* |
| *X509v3 Extended Key Usage* | - | *Server Authentication (1.3.6.1.5.5.7.3.1)*<br>*Client Authentication (1.3.6.1.5.5.7.3.2)* |
| *X509v3 Subject Key Identifier* | - | *<id de la clave pública del certificado, obtenido a partir del hash de la misma>* |
| *X509v3 Authority Key Identifier* | - | *<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>* |
| *X509v3 Authority Information Access* | - | *Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1)*<br>*Access Location 1: http://ocsp.firmaprofesional.com*<br>*Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)*<br>*Access Location 2: http://crl.firmaprofesional.com/infraestructura.crt* |
| *X509v3 CRL Distribution Points* | - | *http://crl.firmaprofesional.com/infraestructura.crl* |
| *X509v3 Certificate Policies* | - | *<OID de la política de certificación correspondiente al certificado>*<br>1.3.6.1.4.1.13177.10.1.3.1 SSL Estándar<br>1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Cualificado<br><br>*<URI de la CPS>*<br><br>*User Notice: "Este es un Certificado de Servidor Web cualificado con Validación Extendida" (para los certificados EV)*<br><br>*User Notice: "Este es un Certificado de Servidor Web" (para los certificados sin EV)*<br><br>*<OID "EU qualified website authentication certificates" según ETSI EN 319 411-2: QCP-w: 0.4.0.194112.1.4 > (para los certificados EV)*<br><br>*<OID de la política EV de certificación correspondiente al certificado: 0.4.0.2042.1.4> (para los certificados EV)* |
| *Qualified Certificate Statements*<br>*(solo para EV)* | - | *Id-etsi-qcs-QcCompliance:* 0.4.0.1862.1.1<br>*(indicando que el certificado cualificado)*<br><br>*Id-etsi-qcs-QcRetentionPeriod:* 0.4.0.1862.1.3<br>*(con un valor de 15 años)*<br><br>*Id-etsi-qcs-QcPDS*[1]*:* 0.4.0.1862.1.5<br>*(URI: https://www.firmaprofesional.com/cps/pds_en.pdf)*<br><br>*Id-etsi-qcs-QcType:* 0.4.0.1862.1.6.3<br>*(**qct-web**, indica que es un certificado para crear firmas electrónicas).* |

[1] Obligatoria en lengua inglesa. Pueden incluirse otros QcPDS en otras lenguas.