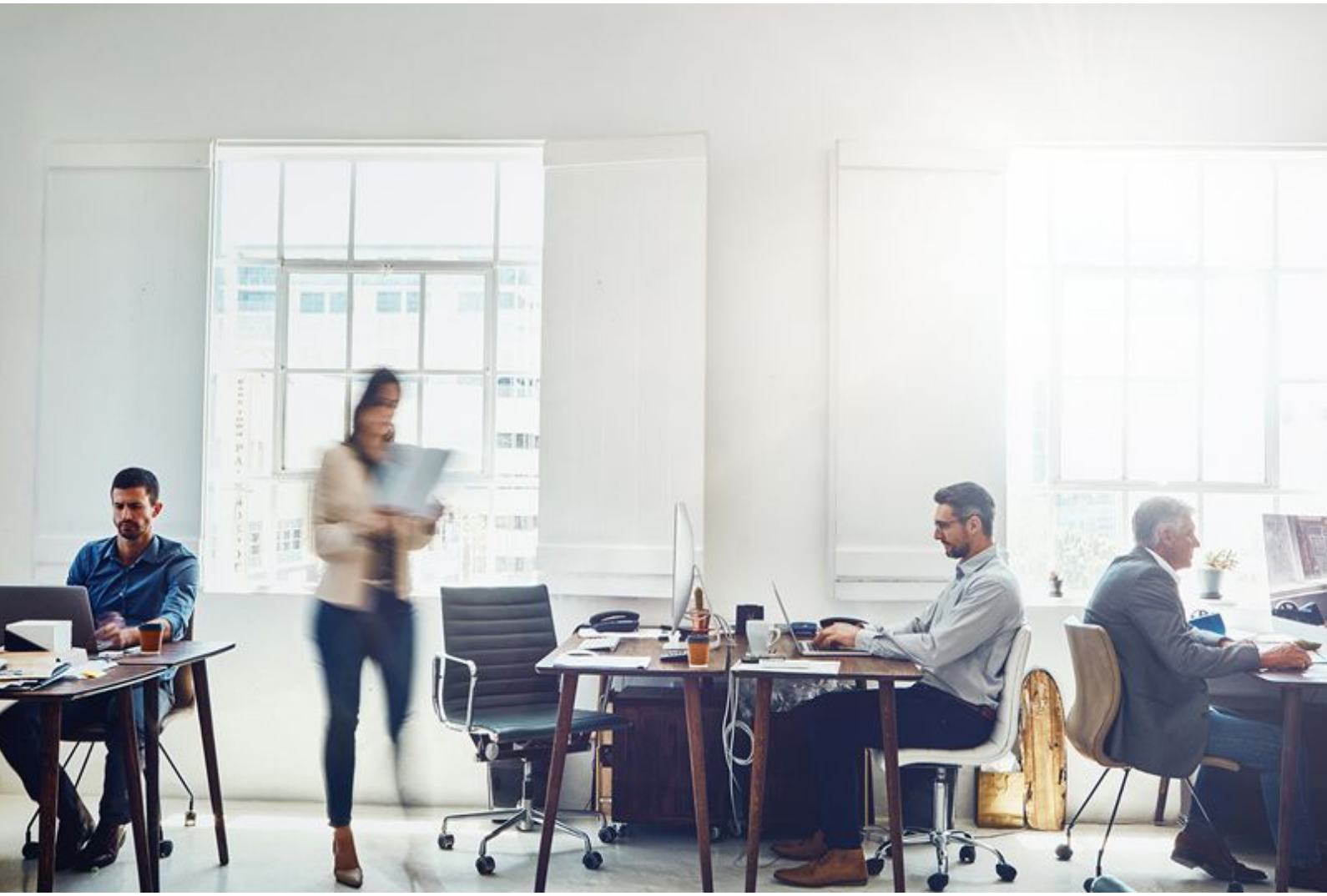
Política de Certificación

Certificados de Autenticación de sitios Web

Versión: 181221

Clasificación: Público



Firmado digitalmente por:
FIRMAPROFESIONAL, S.A.
Fecha y hora: 21.12.2018
14:48:41

BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL M2
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Histórico de versiones

Versión	Sección y cambios	Fecha de publicación
181221	Elaboración de una nueva política certificados de autenticación de sitios web, que integra las anteriores políticas de certificado de sede electrónica y de servidor seguro SSL, que pueden ser consultadas en http://www.firmaprofesional.com/cps Además de la integración de las Políticas, se realizan las siguientes modificaciones: ● Se matiza el apartado 2.2 Autoridad de Registro (RA) ● Se marca el campo SerialNumber como opcional, dado que la misma información la contiene el campo OrganizationIdentifier. ● Se actualizan los procedimientos de verificación del dominio y la organización. ● Se explicita el tratamiento de CAA. ● Aclaración de los requisitos para la generación de claves de certificado de Sede Electrónica de nivel Alto	21/12/2018

Índice

1. Introducción

1.1. Descripción general

Los certificados de autenticación de sitios web son certificados expedidos a organizaciones para servidores web, y garantizan a la persona que visita un sitio web que existe una entidad auténtica y legítima que respalda la existencia del sitio web. Como se establece en el Considerando 67 del Reglamento UE 910/2014 del Parlamento y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, estos certificados contribuyen a crear confianza y fe en la realización de operaciones mercantiles y administrativas en línea, dado que los usuarios se fiarán de un sitio web que haya sido autenticado.

En la actualidad, Firmaprofesional emite tres tipos de Certificados de Autenticación de sitios Web:

- **Certificados de Sede**
    - Son certificados expedidos a Administraciones Públicas, de acuerdo con las indicaciones del artículo 38 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
    - Son certificados cualificados porque cumplen los requisitos establecidos en el anexo IV del Reglamento UE 910/2014.
    - Estos certificados se adhieren a las definiciones de los niveles de aseguramiento alto y medio y a los perfiles de certificados establecidos en el punto 8 del documento "Perfiles de Certificados electrónicos" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.
- **Certificados SSL Organization Validation (OV)**:
    - 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.
  - 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.
  - 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 estos certificados. Esta Política de Certificación (en adelante, la "CP") está sujeta al cumplimiento de la Declaración de Prácticas de Certificación (en adelante, la "CPS") de Firmaprofesional, a la que incorpora por referencia.

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:	Política de Certificación para Certificados de Autenticación de sitios Web
Versión:	181221
Descripción:	Política de Certificación para Certificados de Autenticación de sitios Web
Fecha de Emisión:	21/12/2018

OIDs	1.3.6.1.4.1.13177.10.1.20.1 Sede Electrónica Nivel Alto 1.3.6.1.4.1.13177.10.1.20.2 Sede Electrónica Nivel Medio 1.3.6.1.4.1.13177.10.1.3.1 SSL OV 1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Cualificado
Localización	http://www.firmaprofesional.com/cps

Esta Política de Certificación agrupa las siguiente Políticas, que quedan derogadas con la publicación de ésta:

- Política de Certificación de Certificados de Sede Electrónica (Versión 171121). Esta Política puede ser consultada en https://www.firmaprofesional.com/cps, en el apartado "Políticas y Prácticas de Certificación anteriores"
- Política de Certificación de Certificados de Servidor Web Seguro (Versión 180719). Esta Política puede ser consultada en https://www.firmaprofesional.com/cps, en el apartado "Políticas y Prácticas de Certificación anteriores"

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)

Desde la fecha de publicación de la presente Política, todos los certificados de Autenticación Web son emitidos por la CA Subordinada "AC Firmaprofesional - INFRAESTRUCTURA".

2.2. Autoridad de Registro (RA)

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

La gestión de las emisiones únicamente podrá ser realizada por Firmaprofesional.

2.3. Solicitante

Es la persona física o jurídica que solicita el certificado.

En general, 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.

En el caso de certificados de Sede Electrónica, podrán solicitarlos los administradores, representantes legales y voluntarios de las Corporaciones Públicas, con poder bastante a estos efectos

2.3.1. Roles intervinientes

Siguiendo lo estipulado en la versión vigente del documento "*Guidelines For The Issuance And Management Of Extended Validation Certificates*", emitido por CA/Browser Forum, se establecen una serie de roles que pueden desempeñar diferentes personas relacionadas con el solicitante de un certificado SSL EV.

Estos roles son los siguientes:

1. **El peticionario de certificados**:

   La solicitud de un certificado SSL EV debe ser realizada por un peticionario autorizado por el solicitante. Un peticionario puede ser el mismo solicitante (si este es una persona física), un empleado del solicitante, un agente autorizado que está autorizado por el solicitante para representarle, un empleado de una tercera parte (por ejemplo, un ISP o una empresa de hosting de sitios web). El peticionario cumple la siguiente función:

   a. Completar y enviar las solicitudes de certificados.

2. **El aprobador de certificados**:

   La solicitud de un certificado SSL EV debe ser aprobada por un aprobador autorizado por el solicitante. Un aprobador puede ser el mismo solicitante (si este es una persona

física), un empleado del solicitante, un agente autorizado por el solicitante para representarle. El aprobador puede cumplir las siguientes funciones:

a. Actuar como un peticionario, completando y enviando solicitudes de certificados.
b. Autorizar a otros empleados o a terceras partes para actuar como peticionarios.
c. Aprobar las solicitudes de certificados enviadas por peticionarios.

3. **El firmante del contrato de suscriptor**:

Para solicitar un certificado SSL EV se debe firmar un contrato de suscriptor por un firmante autorizado para ello. Un firmante de contrato es una persona física que puede ser el mismo solicitante, un empleado del solicitante o un agente autorizado por el solicitante para representarlo, que dispone de la autoridad para firmar el contrato de suscriptor en representación del solicitante. El firmante cumple la siguiente función:

a. Firmar el contrato del suscriptor.

4. **El representante del solicitante**:

En el caso de que la CA y el suscriptor sean compañías filiales, los términos de uso aplicables a la solicitud de certificados SSL EV deben ser conocidos y aceptados por un representante autorizado del solicitante. Un representante del solicitante es una persona física que puede ser el mismo solicitante, o un agente autorizado por el solicitante para representarle, y tiene la autoridad de confirmar el conocimiento y la aceptación de los términos de uso en representación del solicitante.

2.4. Suscriptor

El suscriptor del certificado de autenticación de sitios web será la organización que aparece como "Registrante" ("Registrant") en el registro oficial del dominio, o la Administración, Órgano o Entidad de Derecho público identificada en el certificado.

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. La plataforma @firma, la Plataforma de validación y firma electrónica del Gobierno de España, admite y valida los certificados de Sede Electrónica, nivel medio y alto y los certificados de SSL OV.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso, tanto cuantitativas como cualitativas, que se contienen en la CPS y en la presente CP.

3. Características de los certificados

3.1. Periodo de validez de los certificados

El periodo de validez será el que se indique en el propio certificado, con un máximo siguiente:

- Certificados de Sede Electrónica: Validez máxima de 3 años
- Certificados SSL Organization Validation (OV): Validez máxima de 2 años.
- Certificados SSL Extended Validation (EV): 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 OV.

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.

Únicamente se permite emitir certificados multidominio para certificados de servidor SSL OV.

Los Certificados de Servidor Web SSL EV y los certificados de Sede Electrónica 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 Autenticación de sitios Web pueden ser utilizados para autenticar la identidad de un servidor o de una Sede Electrónica mediante el protocolo SSL (o TLS) y establecer luego un canal de transmisión seguro entre el servidor o la Sede y el usuario del servicio.

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 Prácticas 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.

No se permite la utilización distinta de lo establecido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público para los certificados de Sede Electrónica.

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 adecuados 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:

4.1.1. Solicitud

El proceso de solicitud difiere entre los certificados de Sede Electrónica, los certificados SSL OV, y los certificados SSL EV . Los detalles son los siguientes:

4.1.1.1. Solicitud para certificados de Sede Electrónica

Se deberá presentar la referencia al Diario Oficial en el que aparece la disposición de creación de la Sede Electrónica. En dicha disposición deberá aparecer:

- Identificación del Diario Oficial, artículo y fecha de publicación
- Nombre de la Sede Electrónica
- URL de la Sede Electrónica
- Titular de la Sede Electrónica

La solicitud del certificado la deberá realizar un representante del Titular de la Sede Electrónica debidamente acreditado y autorizado para ello.

4.1.1.2. Solicitud para certificados OV

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

El solicitante puede realizar la solicitud por los siguientes medios electrónicos:

- Por la Web de Firmaprofesional.
- Por correo electrónico.
- Enviando un formulario de solicitud facilitado por Firmaprofesional.

Firmaprofesional recibe la solicitud y comienza con el proceso de verificación.

4.1.1.3. Solicitud para certificados EV

Para la solicitud del certificado se seguirán los siguientes pasos:

1. **Firma del contrato de suscriptor y la carta de autorización:**

   Un representante legal del solicitante debe firmar un contrato de suscriptor y una carta de autorización. El representante deberá tener poderes, al menos, para solicitar este tipo de certificados en nombre de su organización.

   Además, firmará una carta de autorización, mediante la cual, autoriza a una persona o a varias a desempeñar el rol de aprobador de certificados. Mediante este rol, las personas autorizadas podrán solicitar y aprobar la emisión de los certificados. Esta carta deberá incluir la firma de las personas autorizadas, adicionalmente a la firma del representante legal. A partir de ese momento, se podrán solicitar certificados.

   La firma de ambos documentos podrá realizarse de dos maneras.

   a. Manuscritamente. En este caso, el solicitante deberá enviar el contrato escaneado y firmado manuscritamente, por correo electrónico. Firmaprofesional verificará que el contrato lo ha firmado el representante realizando una llamada telefónica.
   b. Electrónicamente con un certificado cualificado de representante legal. En este caso, no sería necesaria ninguna verificación adicional.

2. **Solicitud de los certificados:**

   La solicitud de certificados se realiza mediante un formulario PDF enviado desde el E-Mail de uno de los aprobadores de certificados. El hecho de solicitar la emisión supone también el hecho de aprobar la emisión del certificado, por parte de una de las personas relacionadas en el punto 2.3.1

En el proceso de solicitud de certificados SSL EV de Firmaprofesional se utilizarán, al menos, dos de esos perfiles.

4.1.2. Aceptación de la solicitud

El proceso de aceptación de solicitud difiere entre los certificados de Sede Electrónica, de SSL OV y de SSL EV. Los detalles son los siguientes:

4.1.2.1. Aceptación de la solicitud para certificados de Sede Electrónica

Cada Autoridad de Registro de Firmaprofesional tendrá acreditadas a una serie de personas para actuar como Operador de RA frente a Firmaprofesional. Los Operadores de RA habrán sido autorizados por la RA para realizar esta función y habrán sido previamente instruidos en la operativa de emisión de certificados. Cada Operador de RA dispondrá de un Certificado Digital en DCCF (Dispositivo Cualificado de Creación de Firma) propio, que le permitirá gestionar las solicitudes de certificados de usuarios.

El Operador de RA de Firmaprofesional verificará la disposición de creación de la Sede Electrónica así como la identidad de la persona solicitante y su capacidad de representación del Titular.

En caso de solicitar nivel ALTO, se deberá aportar evidencia de que la generación y custodia de claves se realiza en un dispositivo hardware criptográfico.

4.1.2.2. Aceptación de la solicitud para certificados OV

El proceso de verificación se realiza cumpliendo con lo estipulado en la versión vigente del documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", emitido por CA/Browser Forum.

4.1.2.2.1. Verificación de la identidad del solicitante

Se siguen los siguientes pasos para verificar la información del certificado:

1. **Si el solicitante es una organización (persona jurídica)**: se verifica su existencia, nombre, dirección y país de la organización, utilizando uno de los siguientes medios:

    a. Consulta al registro oficial dependiendo del tipo de organización de que se trate. Por ejemplo, para empresas, se realizará la consulta al Registro Mercantil. En el caso de entidades públicas, se realizará una consulta a un registro de entidades públicas.
    También se admite un certificado emitido por un registro oficial 825 días antes de la emisión del certificado.

    b. Consulta en una base de datos de un tercero periódicamente actualizada y que es considerada como fuente de datos confiable. Como fuente de datos confiable se entiende una base de datos usada para verificar información acerca de la identidad de organizaciones, reconocida entre las empresas comerciales y administraciones públicas como fuente confiable y creada por una tercera parte, que no sea el mismo solicitante.
    También es válido un documento o informe emitido por una fuente confiable, como por ejemplo, einforma, DUN & BRADSTREET, Legal Entity Identifier (LEI).

    c. Una declaración escrita por un funcionario público, notario o despacho de abogados. En el anexo X se puede encontrar un modelo de texto para la declaración.

    Si el solicitante desea incorporar en el certificado la información de una **marca registrada o de un nombre comercial**, entonces se verifica que tiene derecho a usar la marca o el nombre usando uno los siguientes medios:

a. Certificado emitido por una entidad gubernamental o consulta a un registro oficial, en el que se demuestre que el solicitante tiene derecho a utilizar la marca o el nombre que aparecerá en el certificado. Por ejemplo, en España se realizará una búsqueda en el registro Web de la Oficina Española de Patentes y Marcas. También, serviría que el solicitante aporte un certificado de esta misma entidad.

b. Consulta en una base de datos de un tercero periódicamente actualizada y que es considerada como fuente de datos confiable. Como fuente de datos confiable se entiende una base de datos usada para verificar que una organización posee el derecho a usar una marca o un nombre comercial, y que es reconocida entre las empresas comerciales y administraciones públicas como fuente confiable y creada por una tercera parte, que no sea el mismo solicitante.
También es válido un documento o informe emitido por una fuente confiable.

c. Una declaración escrita por un funcionario público, notario o despacho de abogados, acompañada de documentación que acredite que el solicitante tiene derecho a usa el nombre comercial o la marca. En el anexo X se puede encontrar un modelo de texto para la declaración.

2. **Si el solicitante es una persona física:** se verifica el nombre, su dirección y país, utilizando uno de los siguientes medios:
   a. Fotocopia del DNI, pasaporte o carné de conducir, en la que aparezca una fotografía en la que se pueda discernir la cara del solicitante. Este medio servirá para verificar el nombre y la dirección del solicitante.

   b. Si la ubicación que se desea incluir en el certificado no es la misma que aparece en el DNI, pasaporte o carné de conducir, el solicitante puede

aportar una factura de agua o luz o un extracto bancario, en el que se asocie al solicitante con la ubicación que se desea incluir en el certificado.

4.1.2.2.2. Verificación del control del nombre de dominio

Firmaprofesional verifica, antes de la emisión del certificado SSL, que el solicitante tiene control sobre el dominio para el cual solicita el certificado, utilizando al menos uno de los siguientes métodos:

1. Se envía al solicitante un código único y aleatorio por correo electrónico, fax, mensaje SMS o carta por correo postal. Cualquier persona de la organización solicitante puede contestar por cualquiera de estos medios, indicando el código aleatorio. Lo más frecuente será que responda por E-Mail.
   Para enviar el código aleatorio, Firmaprofesional utilizará la dirección de correo electrónico, el número de fax, el número de teléfono móvil o la dirección de correo postal que aparece en el resultado de la búsqueda realizada en el servicio Whois.

2. Se realiza una llamada al contacto administrativo o técnico del nombre de dominio, que aparece en la consulta realizada al servicio Whois correspondiente. En la llamada se confirma que el solicitante ha realizado la petición de un certificado para el nombre de dominio en cuestión. La llamada se realiza al número de teléfono que muestra el resultado de la búsqueda al servicio Whois. La llamada es grabada y almacenada por Firmaprofesional.

3. Se envía un correo electrónico a una o más de las siguientes direcciones "admin", "administrator", "webmaster", "hostmaster" o "postmaster", seguido por el símbolo "@" y el nombre de dominio para el cual se solicita el certificado SSL. El correo electrónico enviado por Firmaprofesional incluye un código aleatorio y único. Cualquier persona de la organización solicitante debe responder el correo electrónico indicando el código aleatorio.

4. El solicitante realiza un cambio en el registro DNS del dominio para el que peticiona el certificado SSL. Firmaprofesional le indica un código aleatorio y único. El solicitante debe añadir el código aleatorio en un campo CNAME, TXT o CAA, en su registro DNS. Una vez realizado el cambio por parte del solicitante, Firmaprofesional lo verifica.

5. Se realiza una consulta DNS lookup del dominio y se debe extraer la dirección IP del campo A o del campo AAAA. Después, se verifica que el solicitante tiene asignada la dirección IP obtenida, realizando una búsqueda en Internet Assigned Numbers Authority (IANA) o en Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

4.1.2.3. Aceptación de la solicitud para certificados EV

Lo requisitos de verificación para la emisión de un Certificado de Servidor Web SSL EV de Firmaprofesional son los siguientes:

4.1.2.3.1. Verificación de la existencia legal e identidad del solicitante

Tipo de entidad	**Aspectos a verificar**	**Métodos de verificación – Una de las siguientes opciones**	**Evidencia**
Organización privada (Entidades no gubernamentales cuya creación fue gracias a un acto de incorporación a un registro legal)	- Existencia legal - Nombre de la organización - Nº de registro o CIF - Registro oficial	1) Consulta On-Line a: - Registro Mercantil. - Cámara de Comercio nacional. - O Legal Entity Identifier (LEI). 2) Certificado o documento expedido dos años antes de la emisión del certificado SSL por Registro Mercantil o equivalente, LEI o Cámara de Comercio.	Copia de la consulta o del certificado o documento expedido.
Organización pública u organización gubernamental	- Existencia legal -Nombre de la organización - Nº de registro o CIF	1) Consulta a registro oficial. 2) Consulta LEI. 3) Certificado o documento expedido dos años antes de la emisión del certificado SSL por registro oficial o LEI.	Copia de la consulta o del certificado o documento expedido.

Business Entity / Entidad Comercial (Cualquier entidad que no sea una organización privada, entidad pública o entidades no comerciales)	- Existencia legal - Nombre de la organización - Nº de registro o CIF	1) Para Colegios profesionales: Estatutos de creación y su publicación en el BOE y tarjeta CIF, o LEI. 2) Para otros: Consulta a registro oficial público o LEI. 3) Certificado o documento expedido dos años antes de la emisión del certificado SSL por registro oficial o LEI.	Para Colegios: - Copia de los estatutos - Copia de la publicación en el BOE - Copia del CIF - O LEI - Copia del certificado o documento expedido. Para otros: - Copia de consulta. - O LEI. - Copia del certificado o documento expedido.
	- Apoderado o representante principal	Declaración responsable de un responsable de recursos humanos o Gerente, del área legal o del secretario general, confirmando que el representante lo es y sus poderes son vigentes.	Copia de la declaración responsable.
Entidades no comerciales (Organización internacional)	- Existencia legal - Nombre de la organización - Nº de registro o CIF	1) Documento de constitución. 2) LEI.	- Copia del documento de constitución - O LEI.
Marcas registradas o nombres comerciales (si una entidad desea que el certificado SSL EV incorpore su nombre comercial o una marca registrada)	- El solicitante ha registrado el nombre comercial o la marca registrada. - Vigencia del uso de la marca registrada o nombre comercial.	1) Consulta On-Line al registro oficial nacional. 2) Consulta On-Line al registro oficial internacional. 3) Certificado o documento expedido por el registro oficial nacional dos años antes de la emisión del certificado SSL.	Copia de la consulta o del certificado o documento expedido.

4.1.2.3.2. Verificación de la ubicación geográfica en la que el solicitante desarrolla su negocio:

Tipo de entidad	Aspectos a verificar	Métodos de verificación – Una de las siguientes opciones	Evidencia
Para todos los tipos de organizaciones	- Ubicación geográfica en la que desarrolla su negocio el solicitante.	1) Si la ubicación geográfica del solicitante aparecen en alguno de los métodos de verificación mencionados en el apartado de "Verificación de la existencia legal e identidad del solicitante", entonces no se realiza ninguna comprobación adicional. 2) Consulta a base de datos confiable. Por ejemplo, einforma, DUN & BRADSTREET, Legal Entity Identifier (LEI). 3) Documento notarial que certifique la ubicación geográfica.	Evidencias recogidas en el apartado a), copia de consulta a la base de datos confiable o copia del documento notarial.

4.1.2.3.3. Verificación de la existencia operativa del solicitante:

Tipo de entidad	Aspectos a verificar	Métodos de verificación – Una de las siguientes opciones	Evidencia
Para todos los tipos de organizaciones	- Ubicación geográfica en la que desarrolla su negocio el solicitante.	1) Si la ubicación geográfica del solicitante aparecen en alguno de los métodos de verificación mencionados en el apartado de "Verificación de la existencia legal e identidad del solicitante", entonces no se realiza ninguna comprobación adicional. 2) Consulta a base de datos confiable. Por ejemplo, einforma, DUN & BRADSTREET, Legal Entity Identifier (LEI). 3) Documento notarial que certifique la ubicación geográfica.	Evidencias recogidas en el apartado a), copia de consulta a la base de datos confiable o copia del documento notarial.

4.1.2.3.4. Verificación del control del nombre de dominio

Firmaprofesional verifica, antes de la emisión del certificado SSL, que el solicitante tiene control sobre el dominio para el cual solicita el certificado, utilizando al menos uno de los siguientes métodos:

1. Se envía al solicitante un código único y aleatorio por correo electrónico, fax, mensaje SMS o carta por correo postal. Cualquier persona de la organización solicitante puede contestar por cualquiera de estos medios, indicando el código aleatorio. Lo más frecuente será que responda por E-Mail.

2. Para enviar el código aleatorio, Firmaprofesional utilizará la dirección de correo electrónico, el número de fax, el número de teléfono móvil o la dirección de correo postal que aparece en el resultado de la búsqueda realizada en el servicio Whois.

3. Se realiza una llamada al contacto administrativo o técnico del nombre de dominio, que aparece en la consulta realizada al servicio Whois correspondiente. En la llamada se confirma que el solicitante ha realizado la petición de un certificado para el nombre de dominio en cuestión. La llamada se realiza al número de teléfono que muestra el resultado de la búsqueda al servicio Whois. La llamada es grabada y almacenada por Firmaprofesional.

4. Se envía un correo electrónico a una o más de las siguientes direcciones "admin", "administrator", "webmaster", "hostmaster" o "postmaster", seguido por el símbolo "@" y el nombre de dominio para el cual se solicita el certificado SSL. El correo electrónico enviado por Firmaprofesional incluye un código aleatorio y único. Cualquier persona de la organización solicitante debe responder el correo electrónico indicando el código aleatorio.

El solicitante realiza un cambio en el registro DNS del dominio para el que peticiona el certificado SSL. Firmaprofesional le indica un código aleatorio y único. El solicitante debe añadir el código aleatorio en un campo CNAME, TXT o CAA, en su registro DNS. Una vez realizado el cambio por parte del solicitante, Firmaprofesional lo verifica.

Se realiza una consulta DNS lookup del dominio y se debe extraer la dirección IP del campo A o del campo AAAA. Después, se verifica que el solicitante tiene asignada la dirección IP

obtenida, realizando una búsqueda en Internet Assigned Numbers Authority (IANA) o en Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

4.1.2.3.5. Verificación del nombre, cargo y autoridad del firmante del contrato de suscriptor y de aprobador del certificado

El solicitante deberá firmar un contrato de suscriptor y hacerle llegar al menos una copia escaneada a Firmaprofesional. En el contrato de suscriptor se establece que el solicitante podrá pedir a Firmaprofesional Certificados SSL EV para los dominios bajo su control y que tenga poder de utilizar.

El contrato deberá firmarlo la persona que actúe como firmante del contrato de suscriptor, según la definición de roles incluida en el punto 4.1.1.3.1 de esta Política.

El contrato incluye una declaración responsable, en la que reconoce que tiene autoridad y poderes para actuar en nombre del solicitante para pedir un certificado SSL EV a Firmaprofesional, hacer uso de él y custodiarlo. De este modo, se verifican los poderes del firmante del contrato de suscriptor.

El contrato del suscriptor irá acompañado de una carta de autorización, mediante la cual, el solicitante autoriza a personas concretas para desempeñar los roles descritos en el punto 4.1.1.3.1 de esta Política. La carta deberá incluir las firmas de cada una de las personas autorizadas, además de la firma del firmante del contrato de suscriptor. De este modo, se verifican el nombre, el cargo, la oficina y la autoridad del aprobador de certificados.

4.1.2.3.6. Verificación de la firma del contrato de suscriptor.

Firmaprofesional utiliza uno de los siguientes métodos para verificar la firma del contrato de suscriptor:

1. Realizando una llamada telefónica al solicitante y haciendo un cuestionario de preguntas al firmante del contrato de suscriptor. La llamada es grabada y

almacenada como evidencia.

2. Si el contrato de suscriptor es firmado con un certificado de representante legal de la organización solicitante, este se almacena como evidencia y no son necesarias más comprobaciones.

4.1.2.3.7. Verificación de la aprobación para la emisión de un certificado SSL EV.

Para poder emitir un certificado SSL EV, el aprobador de certificado autorizado mediante la carta de autorización (en la que aparece su dirección de correo electrónico) deberá enviar desde su correo electrónico la solicitud del certificado. Mediante este hecho ya estaría autorizando la emisión del certificado.

4.1.3. 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, incluye herramientas para generar claves y peticiones de certificados.

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

4.1.4. Tramitación

En el caso de los **certificados de Sede Electrónica**, el Operador de RA validará la veracidad y exactitud de los datos del solicitante y la sede electrónica, así como que el solicitante está en posesión de la clave privada asociada a la clave pública incluida en la petición de certificación. El Operador de RA generará la petición de certificado en un formato estándar y la enviará a Firmaprofesional.

Para tramitar los **certificados de SSL OV y SSL EV,** 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.

4.1.5. Emisión del certificado

Previa a la emisión del certificado de Sede Electrónica, el Operador de RA generará la petición de certificado en un formato estándar y la enviará a Firmaprofesional.

Firmaprofesional validará la integridad de la petición y que ha sido generada por un Operador de RA debidamente autorizado. Tras esta validación se procederá a la emisión del certificado.

En los casos en que Firmaprofesional tenga garantía de que se cumplen los requisitos para que el certificado sea considerado que tiene un nivel de seguridad Alto conforme al documento de Perfiles de Certificados elaborado por el Gobierno de España, el certificado se emitirá con el OID correspondiente.

Previa a la emisión de los certificados SSL OV y SSL EV, se valida la existencia de registro CAA para cada nombre DNS de las extensiones CN y subjectAltName del certificado. En el caso de que se emita el certificado, la validación se realizará antes del TTL del registro CAA. Firmaprofesional procesa los tags "issue" e "issuewild". El registro CAA que identifica a dominios para los que se autoriza la emisión por parte de Firmaprofesional es "firmaprofesional.com".

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 OV.

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.

4.1.6. Entrega

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

Los certificados de sede deben ser aceptados formalmente por el solicitante, dejando evidencia documental en poder de la RA.

4.2. Revocación de certificados

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

4.3. Renovación de certificados

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

4.4. Procedimiento de notificación de problemas por parte del suscriptor

Si el suscriptor de certificados de autenticación de sitios 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

Al amparo de las prescripciones contenidas en la presente Política de Certificación se emiten los siguientes tipos de certificados, con sus OID asociados:

Tipo de certificado	**OID**
Sede Electrónica Nivel Alto	1.3.6.1.4.1.13177.10.1.20.1
Sede Electrónica Nivel Medio	1.3.6.1.4.1.13177.10.1.20.2
SSL OV	1.3.6.1.4.1.13177.10.1.3.1
SSL EV / Cualificado	1.3.6.1.4.1.13177.10.1.3.10

Las extensiones utilizadas por cada tipo de certificado emitidos bajo la presente política se publican en el documento denominado "Perfiles de los certificados de Firmaprofesional" en la web de Firmaprofesional (http://www.firmaprofesional.com/cps).

Firmaprofesional, S.A.

Diciembre de 2018