

# Contratar un SSL para un dominio

## Introducción

El certificado SSL (Secure Socket Layer) es un procedimiento de seguridad de transacción de datos. Su principio consiste en establecer un canal de comunicación segura ( cifrada) en la máquina del cliente y el servidor con el fin de mantener la confidencialidad, o proteger datos.

El uso de un certificado Ssl por un sitio de internet se diferencia en su barra de direcciones de internet (https en vez de http).

### Selección de la URL

El nombre del sitio web a autenticar representa el nombre completo de dominio. Así de esta manera `www.ovh.es` no es lo mismo que `ovh.es`.

Si quiere asegurar estos dos nombres tendrá que solicitar dos autenticaciones : una para `www.ovh.es` y otra para `ovh.es`

## Requisitos

- Su dominio tiene que estar registrado con OVH
- Debe tener un número de teléfono
- Tiene que verificar que los datos del propietario en el WHOIS son correctos

Para verificar los datos del propietario vaya a su espacio manager, seleccione su nombre de dominio.

Haga clic en *Gestión de contactos*

### **Gestión de contactos**

Haga clic en *Modificar*

### **Modificar**

Tiene que verificar que los datos del whois son los mismos que el propietario

- Para los nombre de dominio genericos (.com,.net,.biz,.info) puede utilizar el whois de OVH

- Para los dominios en .org puede ir a <http://pir.org/>
- Para los dominios en .be puede ir a la página <http://www.dns.be>
- Para los dominios en .fr .asso.fr .re puede ir a la página <http://afnic.fr>
- Para los dominios en .eu puede ir a la página <http://eurid.eu/>
- Para los dominios en .es puede ir a la página <https://www.nic.es/>

## Compra de un certificado

Para obtener su certificado tiene que ir a espacio manager, en la sección *Más servicios*

### **Más servicios**

A continuación, solicite una *Nueva autenticación SSL*

### **Nueva autenticación SSL**

#### **Paso 1/4. Introducción del nombre de dominio**

Aparecerá la pantalla **Contratar una autenticación para un certificado SSL**

Introduzca el nombre del sitio web a autenticar (en nuestro caso **www.mi\_dominio.com**)

**Atención** : El nombre del sitio web a autenticar, representa el nombre completo de dominio. Así **www.ovh.es** no es lo mismo que **ovh.es**. Si quiere securizar ambos nombres, deberá contratar dos certificados, uno para **ovh.es** y otro para **www.ovh.es**

#### **Paso 2/4. Verificación de datos**

La siguiente pantalla mostrará todos los posibles problemas que puede dar el certificado respecto a los datos que figurarán en el certificado.

#### **A- Corrección de datos del propietario**

El cuadro superior le permitirá corregir los datos del propietario del dominio.

El certificado, estará **obligatoriamente** a nombre del propietario (particular o empresa) del dominio registrado en OVH.

Si es necesario corregir los datos del propietario, pulse el botón **Corregir datos**

**B– Duración del certificado**

Seleccione la validez deseada del nuevo certificado :

El certificado puede solicitarse con una validez de

- 12 meses
- 24 meses
- 36 meses

**C– Verificación de la identidad del propietario**

Si el propietario no puede verificar su identidad por sí mismo, el contacto administrador necesitará la autorización correspondiente para poder verificarla en su lugar.

En ese caso, indique la persona que va a actuar como persona autorizada.

**D– Verificación de la empresa**

Si el propietario del dominio y/o del certificado es una empresa, deberá identificarla con su número de NIF correspondiente.

También es necesario indicar una persona de contacto para la validación telefónica así como indicar su puesto en la empresa.

Indique los datos que se le solicitan y pulse **Aceptar**

**Paso 3/4. Gestión de claves**

Debe generar una clave privada RSA así como la clave pública CSR correspondiente, necesarias para la obtención de un certificado electrónico.

Por razones de seguridad, es conveniente generarlas desde su ordenador, de todos modos, puede seleccionar que nuestro asistente las genere automáticamente. En ese caso, OVH declinará toda responsabilidad por la privacidad de los datos tratados.

Existen dos formas de realizar la generación de claves :

- Generar la clave usando el asistente (indicado para no–expertos)
- Generar la clave de forma manual (indicado para obtener un máximo de seguridad)

## A – Creación automática

- Tiene que registrar su llave privada

Haga clic en **Descargar la clave privada**

Podrá guardar el archivo **private.key** en su ordenador.

**Nota** : Por lo general, es conveniente guardar todos los archivos en el mismo directorio.

En nuestro ejemplo guardamos el fichero como **private.key**.

- Marque el mensaje de advertencia

[ ] Reconozco que este método automático está desaconsejado y que he guardado la clave privada en un entorno en el cual sólo las personas de confianza tienen acceso.

- Una vez guardado el fichero pulse el botón **Aceptar**

## B – Creación manual

Genere la Clave privada y pública a través de SSH en su servidor de Linux, con ayuda de los comandos indicados en la página.

```
# openssl genrsa -des3 -out private.key 2048
# openssl -req -new -key private.key -out request.csr -days 365 -sha1
-batch
```

Obtendrá dos ficheros **private.key** y **request.csr**.

Copie el contenido de "request.csr" en el campo de texto de la página y guarde el archivo de la clave privada **private.key** en un lugar seguro.

- Una vez introducido el contenido pulse el botón **Aceptar**

### **C – Verificación del sitio web**

Adicionalmente el Manager puede solicitarle que le añada un fichero de texto de verificación a su sitio web generalmente **ovh-cert.txt**.

Para ello cree un fichero de texto con la secuencia de texto que le indica el Manager y colóquelo en la raíz del sitio web a certificar.

#### **ovh-cert.txt**

```
w?%oyt$%)/y+9yq;9'6*Y'9;0y9%/>
```

Una vez emplazado dicho fichero en su alojamiento, haga clic en el botón **Verificar**.

### **Paso 4/4. Creación de la orden de pedido**

En el último paso, se le muestra la orden de pedido para el pago :

#### **Contratar una autenticación para un certificado SSL**

Acaba de contratar el certificado SSL para el sitio web **www.mi\_sitio.com**.

Su orden de pedido es la BC XXXXXX.

Una vez pagada la orden de pedido, el procedimiento de verificación de datos comienza.

- Deberá proporcionar una serie de documentos solicitados
- Deberá atender una llamada telefónica para verificar sus datos

Una vez terminado el procedimiento de verificación, el certificado aparecerá en el Manager.

## Tramitación del certificado y envío de documentos

Los certificados Standard, de baja certificación (Low assurance) no necesitan envío de documentos ni verificación telefónica. Basta con que siga las instrucciones del email que recibirá para verificar el código de certificación a través de su página web.

Si contrató un certificado Business de alta certificación (High assurance) deberá enviar los documentos justificantes del propietario del dominio (ya sea particular o empresa), que serán validados por una auditoría. Una vez validados los datos del propietario en el WHOIS, se verificará manualmente la identidad con una llamada telefónica al número de teléfono de contacto del propietario.

### Documentos a proporcionar

Si el propietario del dominio es :		
Particular	Asociación	Empresa
<ul style="list-style-type: none"> <li>– Una copia de su carné de identidad, NIF o Pasaporte</li> <li>– Una prueba de domicilio o la inscripción en el censo de su ayuntamiento.</li> </ul>	<ul style="list-style-type: none"> <li>– Una copia del recibo de declaración de constitución</li> </ul>	<ul style="list-style-type: none"> <li>– Un extracto del registro de comercio (CIF)</li> </ul>
Una copia de su factura de teléfono/contrato de internet donde aparezca su número de teléfono.		

### Transmisión a través del Manager

Puede transmitir sus documentos justificativos a través de su espacio de cliente Manager. Para ello, vaya a su espacio manager,

Haga clic en *Mis Productos*

**Mis Productos**

Seleccione *Operaciones en curso*

**Operaciones en curso**

Elija la operación en cuestión :

Nueva **Autenticación SSL** en espera...

Consulte el estado de su solicitud :

### Seguimiento :

Su certificado está en fase de tratamiento...

**Detalles :**

Verificación del teléfono – En curso...

Verificación de la concordancia entre el solicitante y el propietario del dominio – **Terminado**

Verificación de la existencia de la sociedad / documentos de identidad y prueba de domicilio para un particular – **Terminado**

Verificación de los documentos – En curso...

**Documentos requeridos:**

Esta sección le permite cargar y enviar los documentos requeridos para la auditoría de su certificado SSL. Puede utilizar los siguientes formatos : imágenes JPEG, PNG, GIF y documentos PDF

**El tamaño máximo de un fichero es de 1000 KB**

- Copia de su factura de teléfono

Cargar el fichero

- Carta de autorización ( Descargar el modelo )

Cargar el fichero

Para completar el procedimiento, deberá escanear los documentos. A continuación cargue y envíe los archivos requeridos.

Volver a las guías sobre SSL en OVH : [GuiaSSL](#)

Más información