

SSL Certificate Service

Certificate Application

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Certificate Application

- Information Submission Process for Paid SSL Certificates

 - Information Submission Process for Wotrus OV and EV SSL Certificates

 - Information Submission Process for SSL Certificates of Other Brands

Certificate Application Information Submission Process for Paid SSL Certificates Information Submission Process for Wotrus OV and EV SSL Certificates

Last updated : 2024-03-06 17:20:20

Overview

After purchasing a Wotrus SSL certificate (OV or EV), you need to submit relevant information. For more information, please see [Purchasing Process](#).

Prerequisites

1. You have logged in to the [SSL Certificate Service console](#) and clicked **Pending Submission**.
2. You have selected the desired certificate and clicked **Submit Information**.

Directions

Note:

The information required varies by certificate type. This document uses a multi-domain OV certificate as an example.

Step 1. Enter the domain name

Select one of the following CSR generation methods as needed.

Select **Generate CSR Online** and then perform operations described in [Generate a CSR online](#) (this option is recommended. Your private key and public key certificate information is generated and managed by the platform to prevent private key loss).

Select **Paste CSR** to [paste the CSR](#) (no private key can be generated with this option).

Generate a CSR online

1. Enter the domain name information, as shown below:

Note:

You can go to the **SSL Certificate Service console** > [My Profile](#) to manage the information of **Existing Organization** or **Existing administrator** if it does not meet your requirements.

Main parameters are described as follows:

Algorithm: Select an encryption algorithm for your certificate.

Key Length: Select the key length for your certificate.

Bound Domain: Enter a single domain to bind to the certificate, such as `tencent.com` or `ssl.tencent.com`.

Other Domains: Enter other domains to bound to the certificate. Note that they cannot be the same as the common name and cannot be modified after submitted to the CA.

Private Key Password: This field is optional and cannot be modified or restored once entered. Please keep the password in mind.

Note:

If you need to deploy Tencent Cloud services such as CLB or CDN, don't set the private key password.

2. Enter your organization information.

Existing Organization: You can use the information of an existing organization directly.

New organization information: Enter your organization's full name, department, city, address, and landline number.

3. Enter the administrator information.

Existing administrator: You can use the information of an existing administrator directly.

New administrator information: Enter the administrator's name, position, phone number, and email.

4. Enter the contact information. You can check **Same as the administrator**.

5. Click **Next** to go to [Step 2](#).

Paste the CSR

1. Paste the CSR information into the text box (your domain information will be detected), enter or select the existing organization information, administrator information, and contact information, as shown in the following figure.

2. Click **Next** to go to [Step 2](#).

Step 2. Select the domain validation method

1. On the **Select Validation Method** page, select the domain validation method, as shown in the following figure.

2. Click **Next** to go to the **Pre-review** page.

Step 3. Wait for the pre-review to complete

After you submit the information and select the domain validation method, your certificate will be pre-reviewed, which usually takes **10 minutes–72 hours**.

Step 4. Validate your domain

1. Validate the domain ownership by referring to the message displayed on the **Validate Domain** page. For example, if you have selected manual DNS validation, the following message will be displayed. Please go to the corresponding DNS hosting provider to add the DNS record, as shown in the following figure.

You can validate your domain as follows:

DNS validation: For detailed directions, please see [Domain Ownership Verification](#).

File validation: For detailed directions, please see [Domain Ownership Verification](#).

2. After the domain validation is completed, you can click **View Domain Validation Status** to see whether the validation is successful or not.

Step 5. Wait for the manual review to complete

After your domain is validated, the CA will review the information submitted and call you to complete the validation.

Note:

It takes 3–5 business days to review OV certificates, and 5–7 business days to review EV certificates.

Step 6. Wait for CA to issue the certificate

After the review is completed, the CA will issue your certificate. You can download and install it.

Note:

The certificate will be issued only if both the manual review and domain validation are passed.

After you applied, there will be a manual review, during which you will receive a call from the US to your organization's business registration number.

Information Submission Process for SSL Certificates of Other Brands

Last updated : 2024-03-06 17:20:20

Overview

If you purchase an OV (including OV Pro) or EV (including EV Pro) SSL certificate (see [Purchasing Process](#) for details), you need to submit materials as required.

After CA approves the materials, the certificate will be issued. You can download and install the paid certificate.

Preparations

1. Log in to the [SSL Certificate Service console](#) and click **Pending Submission**.
2. Select the desired certificate and click **Submit Materials**.

Directions

Note:

The information required varies by certificate type. A multi-domain certificate is taken as an example here.

Step 1. Enter a domain name

Select one of the following CSR generation methods as needed.

Select **Generate a CSR online** to [generate a CSR online](#) (**Recommended, with a CSR and a private key generated**).

Select **Paste CSR** to [paste the CSR](#) (**CSR uploaded automatically, with no private key generated**).

Generate a CSR online

1. Enter domain information.

The main parameters are described as follows:

Algorithm: Select an encryption algorithm type for your certificate as needed.

Key Length: Select the key length for your certificate.

Bound Domain: Enter a single domain to be bound to the certificate, such as `tencent.com` or `ssl.tencent.com`.

Note:

Some certificate brands support binding IP addresses. For details, see [SSL Certificates Supporting IP Address Binding](#).

Other Domains: Enter other domains to be bound to the certificate. They cannot be common names or be modified after submission to CA.

Note:

This parameter is not available for single-domain certificates.

Private Key Password: Optional. The password cannot be modified once entered or recovered, so please keep it in mind.

Note:

If you need to deploy Tencent Cloud services such as CLB or CDN, don't set the private key password.

2. Enter your organization information.

Existing Organization: Use the information of an existing organization.

New Organization: Enter full name, department, city, address, and landline number of your organization.

3. Enter the administrator information.

Existing administrator: Use the information of an existing administrator.

New administrator: Enter the administrator's name, position, phone number, and email.

4. Enter contact information. You may select **Same with the administrator**.

5. Click **Next** to go to [Step 2](#).

Paste the CSR

1. Paste the CSR information into the text box (to detect domain information), enter organization information (or select **Existing Organization**), administrator information (or select **Existing administrator**), and contact information (or select **Same with the administrator**).

2. Click **Next** to go to [Step 2](#).

Step 2. Upload the confirmation letter

Note:

If you use the organization and administrator information in [My Profile](#) that has been reviewed, the confirmation letter can be omitted.

For GlobalSign certificates, the confirmation letter is always required.

For GlobalSign EV certificates, the CA will email you the documents required for review in 2–3 business days after you submit the information, and you do not need to upload them to the console.

1. Click **Download the confirmation letter template** and enter information required in the confirmation letter.

2. Fill out, attach your organization's official seal on and scan the confirmation letter.

3. Click **Upload** and **Next**.

Note:

The confirmation letter can be a JPG, PNG, or PDF file of up to 1.4 MB.

During the manual review of the confirmation letter, you can re-upload it to modify the information.

4. In the **Confirmation letter uploaded successfully** pop-up window, click **OK**. Then, you can wait for the CA to confirm and review your information.

Step 3. Wait for CA to review

After you upload the confirmation letter, the CA will contact you via your email and phone calls for identity verification.

Note:

It takes 3–5 business days to review OV certificates, and 5–7 business days to review EV certificates.

Step 4. Wait for CA to issue the certificate

After the review is completed, the CA will issue your certificate. You can download and install it.