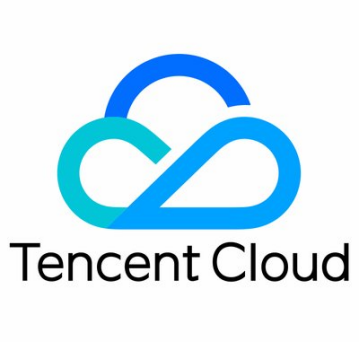
SSL Certificates

Certificate Application



©2013–2023 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Trademark Notice

Tencent Cloud

This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Certificate Application
Formal Certificate Submission Process
Domain Validation (DV) SSL Certificate Submission Process
OV (Organization Validated) and EV (Extended Validation) SSL Certificate Material Submission Process
Information Submission Process for Wotrus OV and EV SSL Certificates
DNSPod GM (SM2) OV and EV SSL Certificate Material Submission Process
Guide to Using Free SSL Certificates
Overview of Free SSL Certificate
Free SSL Certificate Application Process

©2013–2023 Tencent Cloud. All rights reserved.

Certificate Application
Formal Certificate Submission Process
Domain Validation (DV) SSL Certificate Submission Process

Last updated: 2023-09-27 21:52:50

Scenario

Upon successful purchase of a Domain Validation (DV) SSL Certificate, relevant documents must be submitted. Please refer to the Purchase Process for the certificate acquisition procedure. Once the Certificate Authority (CA) has approved the authentication review, the certificate will be officially issued, and you can download and install the certificate.

Preparations

1. Log in to the SSL Certificate Service console and navigate to the **Pending Submission** management page.
2. Select the purchased certificate and click on **Submit Materials**.

Instructions

> **Note**
> The information required varies slightly depending on the type of domain certificate. This operation uses the Wotrus brand Domain Validation (DV) certificate for multiple domains as an example.

Step 1. Enter a domain name

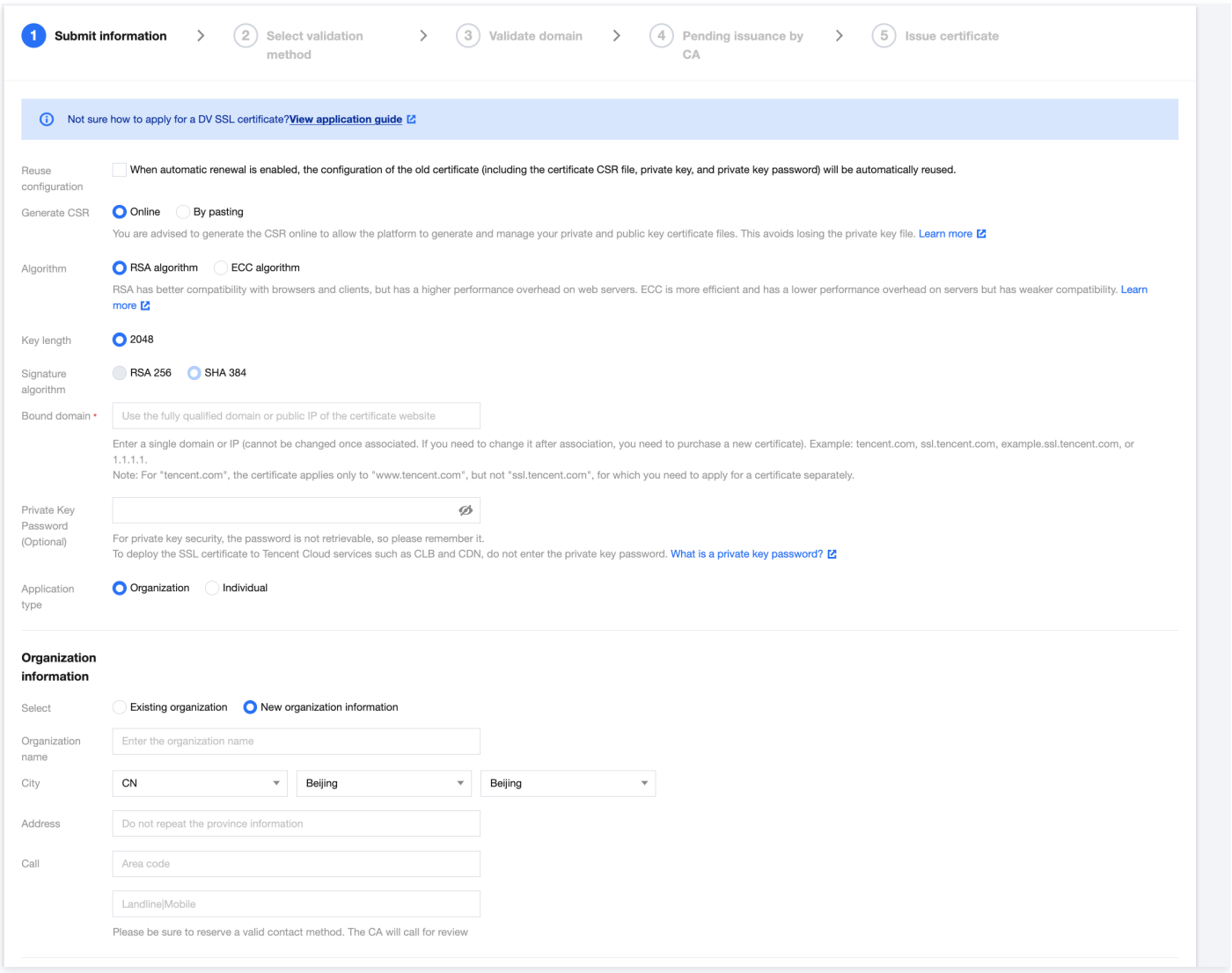
Select one of the following CSR generation methods as needed.

- Choose the "Generate CSR Online" method and execute the operation to generate CSR online (**We recommend generating the CSR online, allowing the platform to generate and manage your private and public key certificate files, thus preventing the loss of private key files**).
- Choose the "Paste CSR" method and perform the Paste CSR operation (**self-upload, private key cannot be generated**).

Generating the CSR online

1. Enter the domain information as shown below:

©2013-2023 Tencent Cloud. All rights reserved.



The main parameter information is as follows:

- **Algorithm**: Choose the certificate encryption algorithm based on your actual requirements.
- **Key Length**: Select the key length for your certificate based on your actual requirements.
- **Bound domain**: Enter a single domain to bind the certificate to, such as `tencent.com` or `ssl.tencent.com`.
- **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.

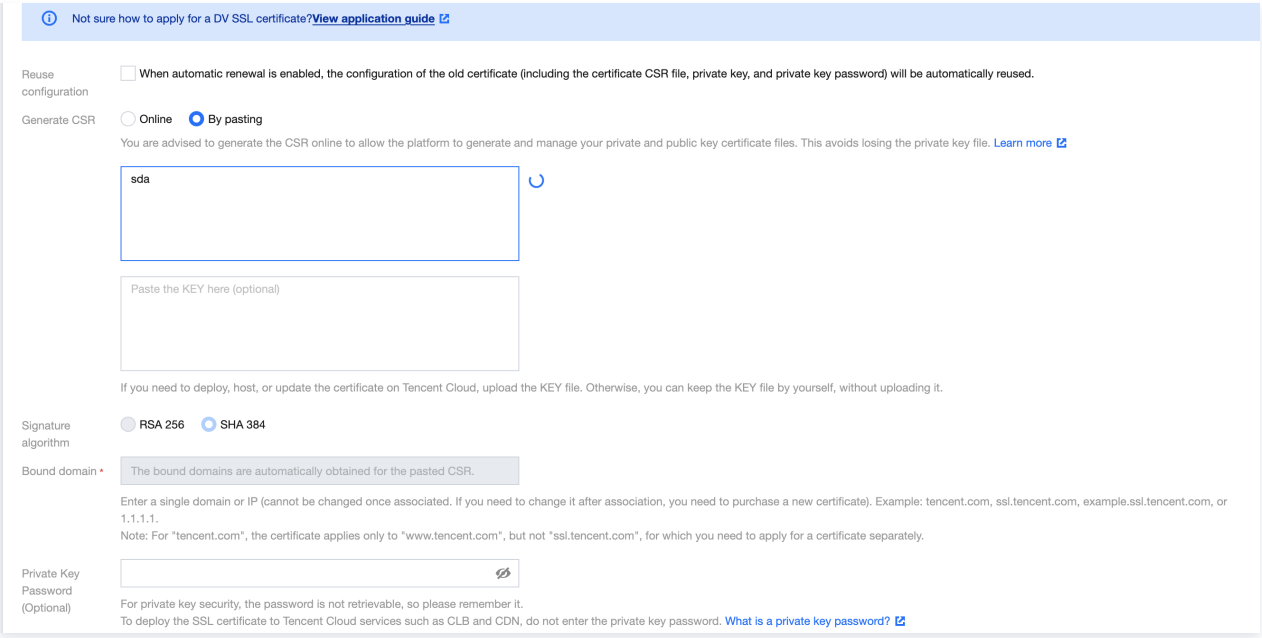
2. Enter your organization information.
   - **Existing Organization**: Select **Existing Organization** to directly use the organization's information.
   - **New Organization information**: Enter full name, department, city, address, and landline number of your organization.
3. Enter the Admin information.
   - **Existing Admin**: Select **Existing Admin** to directly use the administrator's information.
   - **New Admin Information**: Please provide the accurate name, position, phone number, and email of the administrator.
4. Enter contact information. You may select **Same as the admin**.
5. Click **Next** to proceed to Step 2.

Pasting the CSR

1. Paste the prepared CSR information into the text box, enter the "Domain Information", and fill in the organization information (you can select "Existing organization"), admin information (you can select "Existing Admin"), and contact information (you can

©2013–2023 Tencent Cloud. All rights reserved.

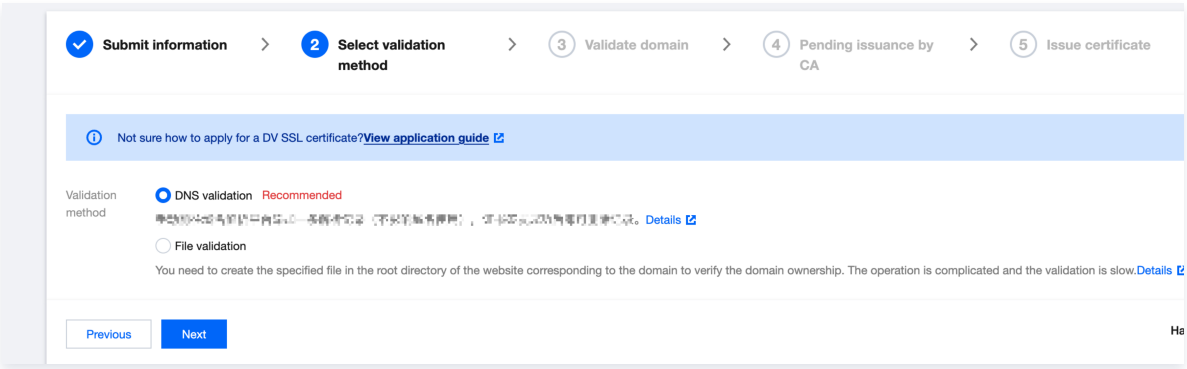
check **Same as Admin**). As shown in the figure below:



2. Click **Next** to proceed to Step 2.

Step 2. Select the validation method

1. On the "Select Verification Method" page, the system will provide available domain verification methods based on the type of certificate you purchased, its validity period, and whether the domain is on DNSPod for DNS resolution, among other conditions.
   - Apply for a one-year Domain Validation (DV) certificate: DNS Verification/File Verification. As shown in the image below:

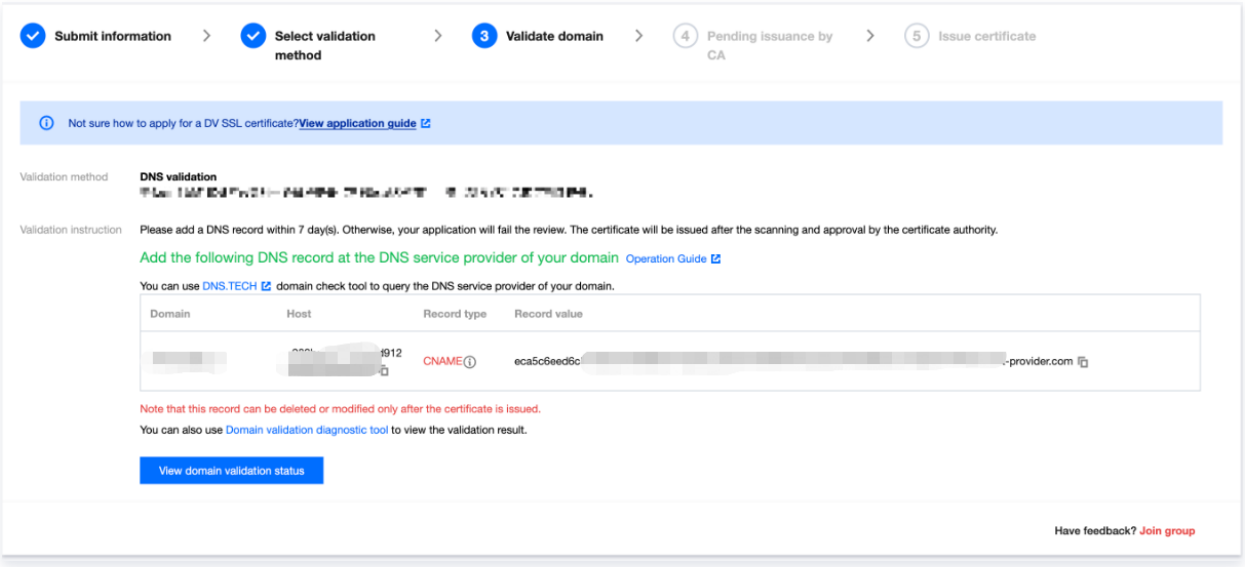


   - To apply for a TrustAsia Domain Validation (DV) certificate (2-year or 3-year wildcard domain): Automatic DNS Verification/Automatic File Verification.
2. Click **Next**.

Step 3. Validate your domain

1. On the "validate domain" page, please carry out the domain verification operation according to the information provided on the page. For instance, if you have chosen the DNS verification method, the following information will be displayed, as shown in the figure below:

©2013-2023 Tencent Cloud. All rights reserved.



- Applying for a one-year Domain Validation (DV) certificate:
  - **DNS Validation**: For domain validation operations, please refer to DNS Validation.
  - **File Validation**: For domain validation procedures, please refer to File Validation.
- Applying for a TrustAsia Domain Validation (DV) certificate (2-year or 3-year wildcard domain):
  - **Automatic DNS Validation**: For domain validation operations, please refer to Automatic DNS Validation.
  - **Automatic File Validation**: Please refer to Automatic File Validation for domain validation operations.

2. After completing the domain verification operation, you can click **View Domain Ownership Validation Status** to check whether the domain verification operation was successful.

> **Note**
> - For the DNSPod GM (SM2) DV certificate, once the domain name verification is passed for the first time, the verification will be retained for 13 months.
> - If a DNSPod GM (SM2) DV certificate has been applied for the same domain name under the same company name within the past 13 months, domain validation will not be required.

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.

©2013-2023 Tencent Cloud. All rights reserved.

OV (Organization Validated) and EV (Extended Validation) SSL Certificate Material Submission Process

Last updated: 2023-12-13 18:02:45

Scenario

Upon successful purchase of the OV (including OV Pro Edition) and EV (including EV Pro Edition) SSL certificates (see Purchase Process for details), relevant materials need to be submitted. Once the CA organization's certification review is approved, the certificate will be officially issued, and you can download the paid certificate for installation.

Preparations

1. Log in to the SSL Certificate Service console and navigate to the **Pending Submission** management page.
2. Select the certificate for which you need to submit materials and click **Submit Materials**.

Instructions

> **Note**
> The information required varies slightly depending on the type of domain certificate. This operation uses a multi-domain certificate as an example.

Step 1. Enter a domain name

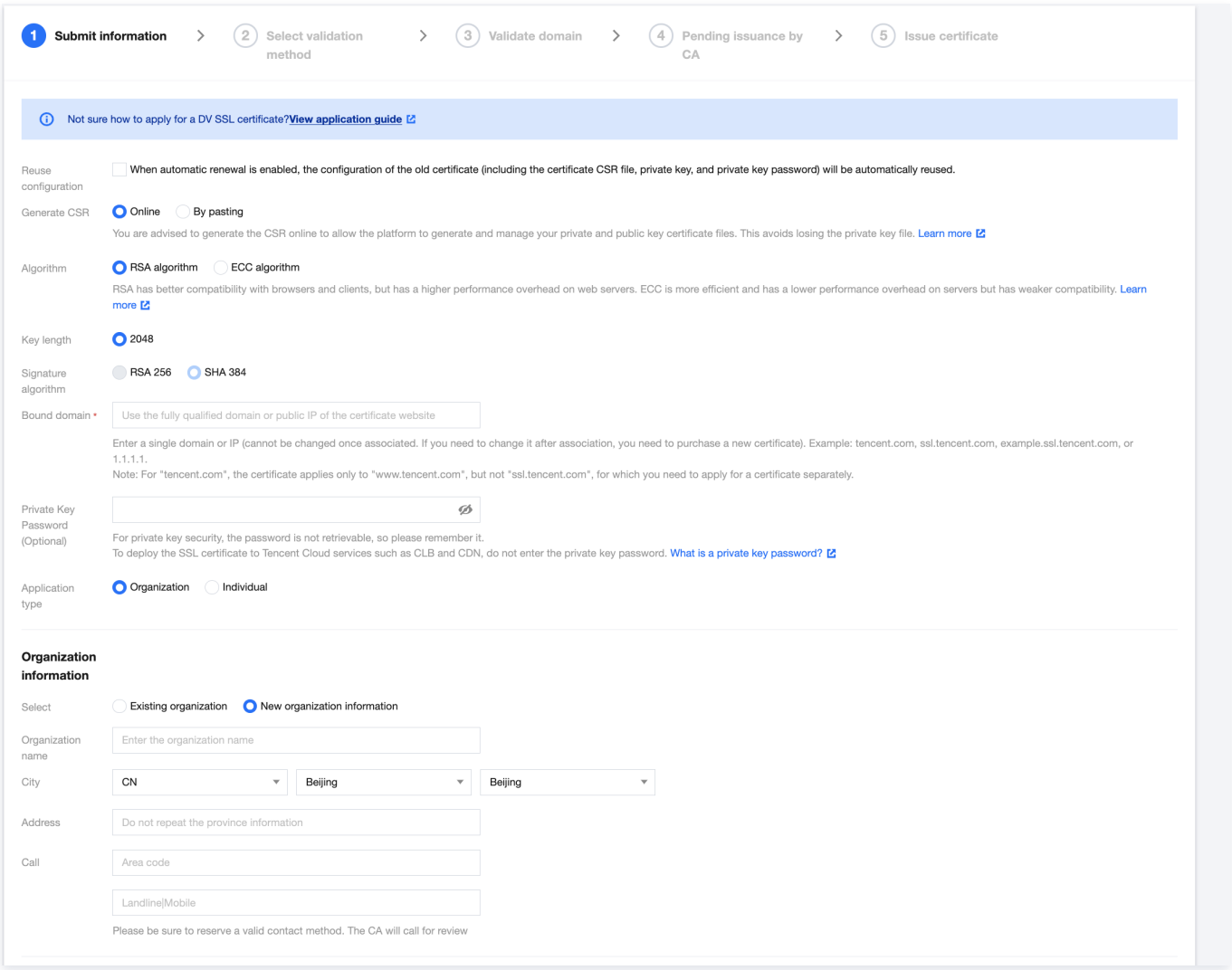
Select one of the following CSR generation methods as needed.

- Choose the "Generate CSR Online" method and perform the operation to generate CSR online (**recommended, as it can generate both CSR and private key**).
- Choose the "Paste CSR" method and perform the Paste CSR operation (**self-upload, private key cannot be generated**).

Generating the CSR online

1. Enter the domain information as shown below:

©2013-2023 Tencent Cloud. All rights reserved.



The main parameter information is as follows:

- **Algorithm**: Choose the type of encryption algorithm for your certificate based on your actual needs.
- **Key Length**: Select the key length for your certificate based on your actual needs.
- **Bound domain**: Enter the single domain name to which the certificate is bound. For example, tencent.com or ssl.tencent.com.

> **Note**
> Some certificate brands support binding IP addresses. For details, see SSL Certificates Supporting IP Address Binding.

- **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.

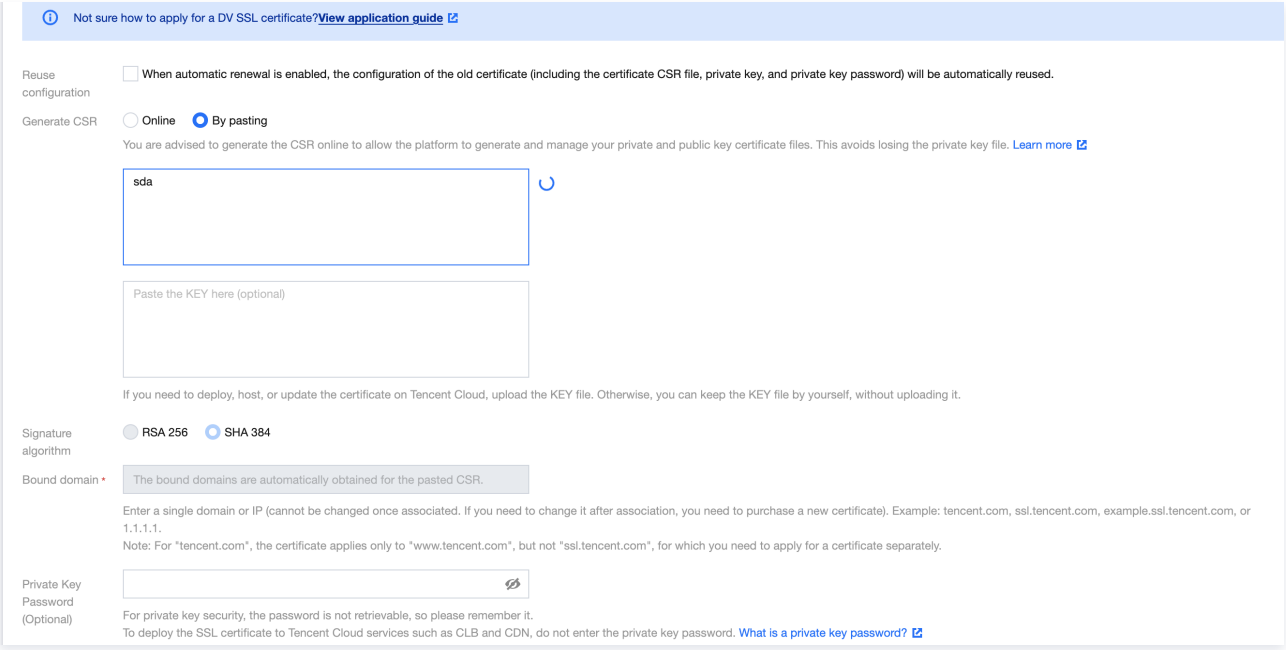
2. Enter your organization information.
   - **Existing Organization**: Select **Existing Organization** to directly use the organization's information.
   - **New Organization information**: Enter full name, department, city, address, and landline number of your organization.
3. Enter the Admin information.
   - **Existing Admin**: Select **Existing Admin** to directly use the administrator's information.
   - **New Admin Information**: Please provide the accurate name, position, phone number, and email of the administrator.
4. Enter contact information. You may select **Same as the admin**.

©2013–2023 Tencent Cloud. All rights reserved.

5. Click **Next** to proceed to Step 2.

Pasting the CSR

1. Paste the prepared CSR information into the text box to identify your domain information. Then, fill in the organization information (you can select "Existing Organization"), administrator information (you can select "Existing Administrator"), and contact information (you can check **Same as Administrator**). As shown in the figure below:



2. Click **Next** to proceed 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 still needs to be uploaded when you submit the information.
> - 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 Confirmation Letter Template** and fill in the necessary information.
2. Fill out, attach your organization's official seal on and scan the confirmation letter.
3. Click **Upload** to upload the confirmation letter, then click **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 pop-up window indicating "Upload Confirmation Letter Successful", click **Confirm** and wait for the business personnel and the CA organization to confirm and review the submitted materials offline.

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.

©2013–2023 Tencent Cloud. All rights reserved.

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.

©2013–2023 Tencent Cloud. All rights reserved.

Information Submission Process for Wotrus OV and EV SSL Certificates

Last updated: 2023-09-28 09:53:43

Scenario

After successfully purchasing the Wotrus brand's Organization Validation (OV) and Extended Validation (EV) SSL certificates, relevant documents need to be submitted. Please refer to Purchase Process for the certificate purchase procedure.

Preparations

1. Log in to the SSL Certificate Service console and navigate to the **Pending Submission** management page.
2. Select the purchased certificate and click on **Submit Materials**.

Instructions

> **Note**
> The information required varies slightly depending on the type of domain certificate. This operation uses the Organization Validation (OV) certificate for multiple domains as an example.

Step 1. Enter a domain name

Select one of the following CSR generation methods as needed.

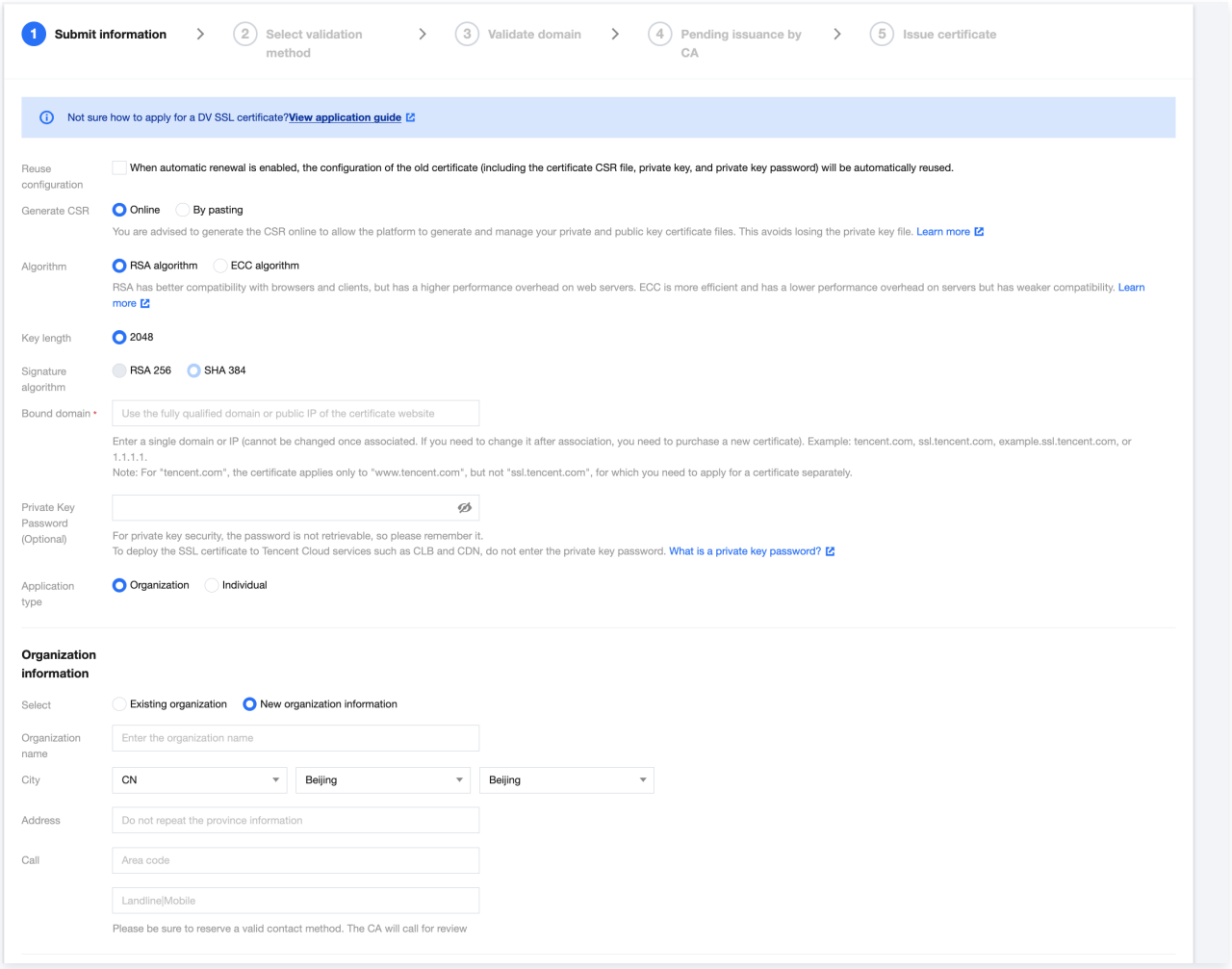
- Choose the "Generate CSR Online" method and execute the operation to generate CSR online (**We recommend generating the CSR online, allowing the platform to generate and manage your private and public key certificate files, thus preventing the loss of private key files**).
- Choose the "Paste CSR" method and perform the Paste CSR operation (**self-upload, private key cannot be generated**).

Generating the CSR online

1. Enter the domain information as shown in the image below.

> **Note**
> If the existing company and administrator information does not meet the requirements for your current certificate application, you can manage it by going to **SSL Certificate Service Console >** My Profile.

©2013-2023 Tencent Cloud. All rights reserved.



Main parameters are as described below:

- **Algorithm**: Check the required certificate encryption algorithm.
- **Key Length**: Check the required key length for the certificate.
- **Bound domain**: Enter a single domain to bind the certificate to, such as `tencent.com` or `ssl.tencent.com`.
- **Private Key Password**: Optional. The password cannot be modified once entered or recovered, so please keep it in mind.

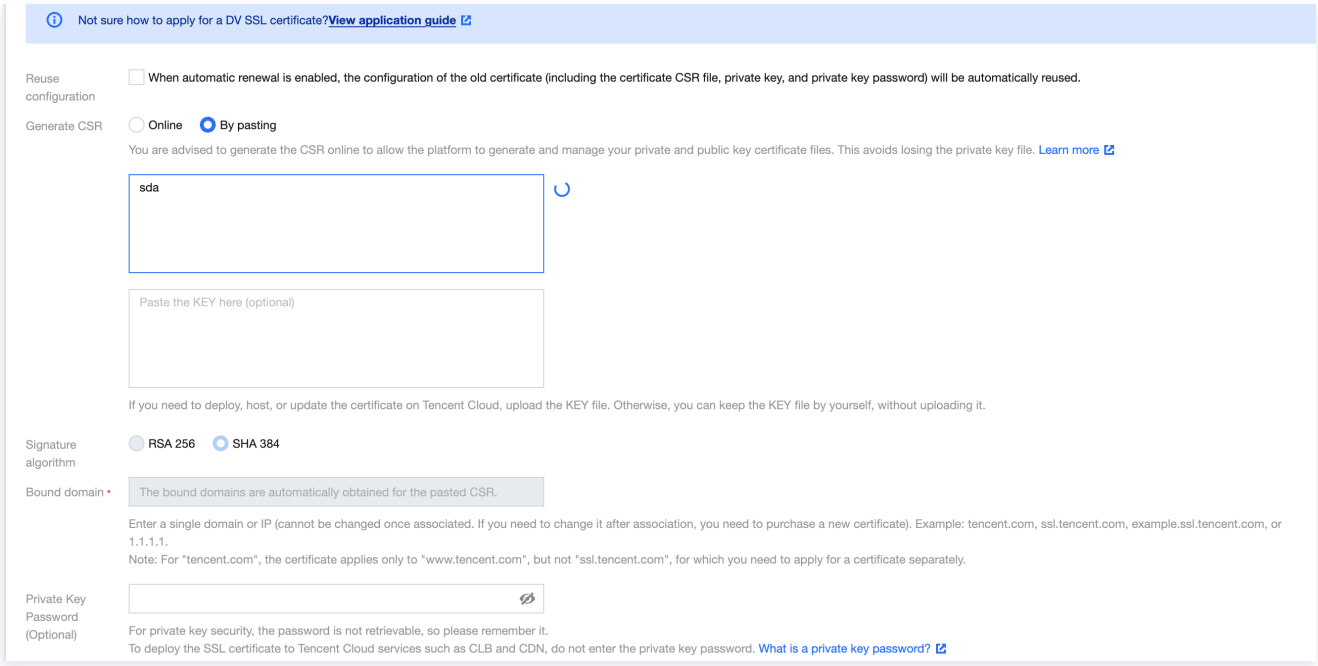
> **Note**
> If you need to deploy Tencent Cloud services such as CLB or CDN, don't set the private key password.

2. Enter your organization information.
   - **Existing Organization**: Select **Existing Organization** to directly use the organization's information.
   - **New Organization information**: Enter full name, department, city, address, and landline number of your organization.
3. Enter the Admin information.
   - **Existing Admin**: Select **Existing Admin** to directly use the administrator's information.
   - **New Admin Information**: Please provide the accurate name, position, phone number, and email of the administrator.
4. Enter contact information. You may select **Same as the admin**.
5. Click **Next** to proceed to Step 2.

Pasting the CSR

1. Paste the prepared CSR information into the text box to identify your domain information, and fill in or select the existing company information, administrator information, and contact information, as shown in the following figure:

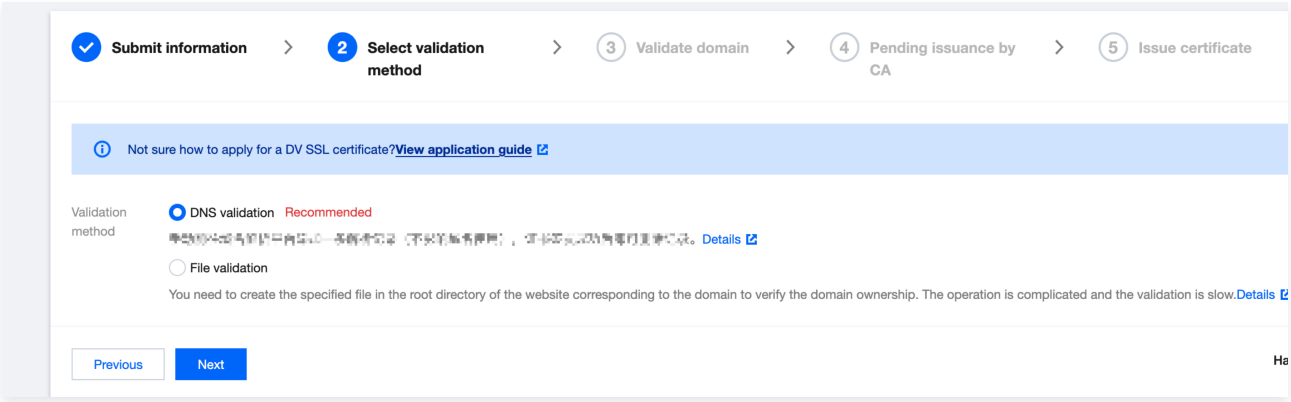
©2013–2023 Tencent Cloud. All rights reserved.



2. Click **Next** to proceed to Step 2.

Step 2: Select the domain authentication method

1. On the "Select Verification Method" page, choose the Domain Verification method. See the figure below:



2. After selecting the verification method, click **Next** to proceed to the "Pre-Review" page.

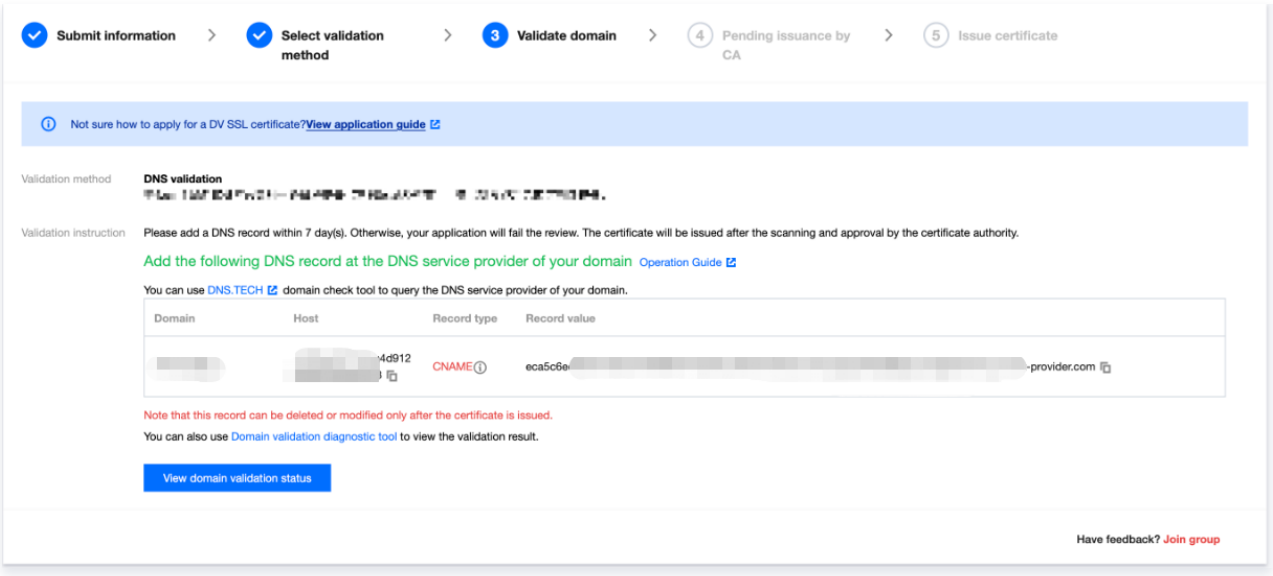
Step 3. Wait for the pre-review to complete

After submitting the materials and choosing the domain verification method, you need to wait for the reviewer to preliminarily review your certificate. The review time is expected to be between **10 minutes and 72 hours**. Please be patient.

Step 4. Validate your domain

1. Please follow the instructions on the "Validate Domain" page to verify domain ownership. For instance, if you have chosen manual DNS validation, the following information will be displayed. You should add the resolution on the corresponding domain name resolution platform as shown below:

©2013-2023 Tencent Cloud. All rights reserved.



You can verify according to the following operation instructions:

- **DNS Validation**: For domain validation operations, please refer to DNS Validation.
- **File Validation**: For domain validation procedures, please refer to File Validation.

2. After completing the domain verification operation, you can click **View Domain Ownership Validation Status** to check whether the domain verification operation was successful.

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.

©2013–2023 Tencent Cloud. All rights reserved.

DNSPod GM (SM2) OV and EV SSL Certificate Material Submission Process

Last updated: 2023-09-28 10:00:47

Scenario

After successfully purchasing the DNSPod GM (SM2) OV and EV SSL certificates, it is necessary to submit relevant materials.
Please refer to the purchase process for the certificate purchase procedure.
Once the CA organization's certification review is passed, the certificate will be officially issued, and you can download and install it.

Preparations

1. Log in to the SSL Certificate Service console and navigate to the **Pending Submission** management page.
2. Select the purchased GM certificate and click on **Submit Materials**.

Instructions

> **Note**
> The information required varies slightly depending on the type of domain certificate. This operation uses the Organization Validation (OV) certificate for multiple domains as an example.

Step 1. Enter a domain name

Select one of the following CSR generation methods as needed.

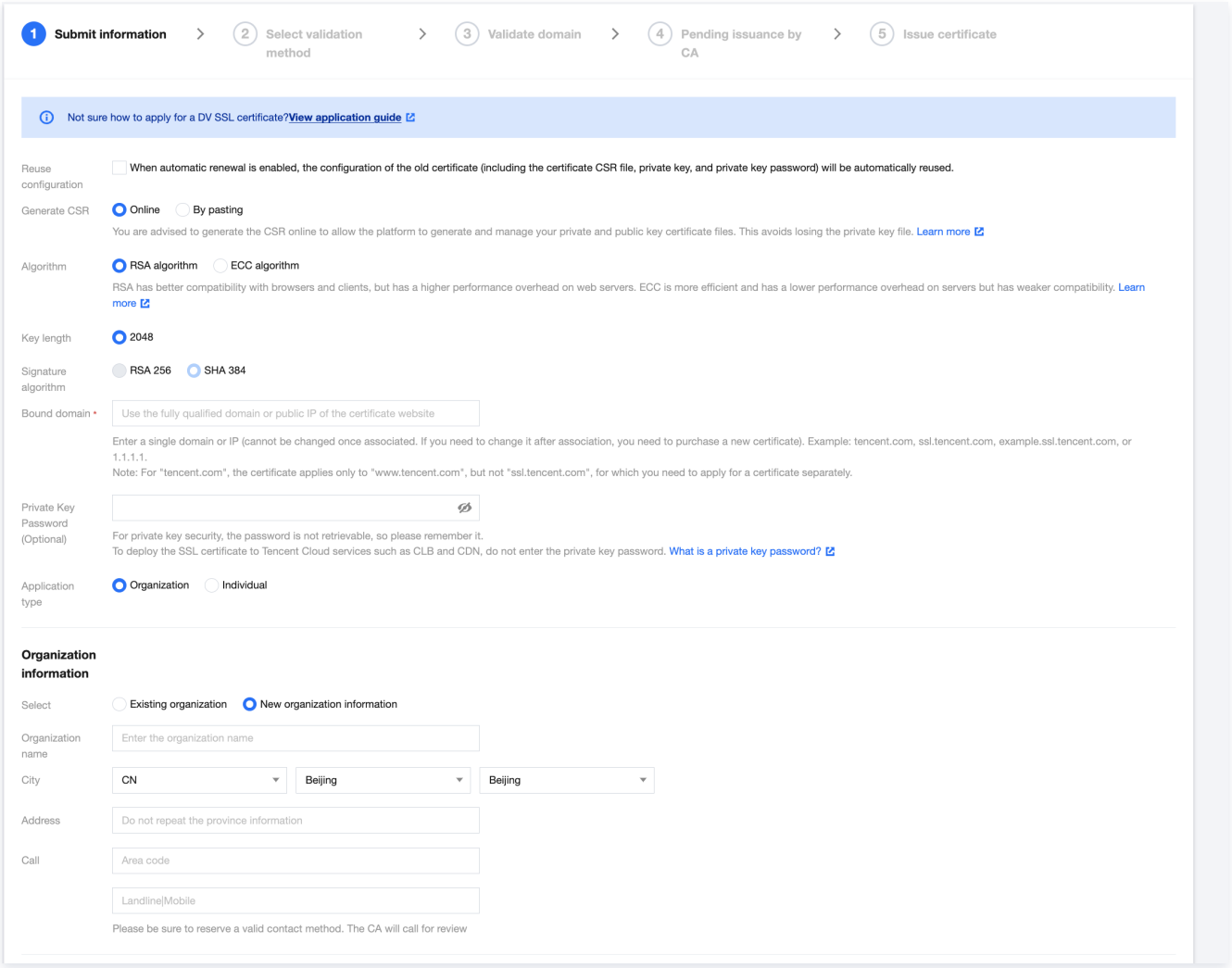
- Choose the "Generate CSR Online" method and execute the operation to generate CSR online (**We recommend generating the CSR online, allowing the platform to generate and manage your private and public key certificate files, thus preventing the loss of private key files**).
- Choose the "Paste CSR" method and perform the Paste CSR operation (**self-upload, private key cannot be generated**).

Generating the CSR online

1. Enter the domain information as shown in the image below.

> **Note**
> If the existing company and administrator information does not meet the requirements for your current certificate application, you can manage it by going to **SSL Certificate Service Console** > My Profile.

©2013-2023 Tencent Cloud. All rights reserved.



Main parameters are as described below:

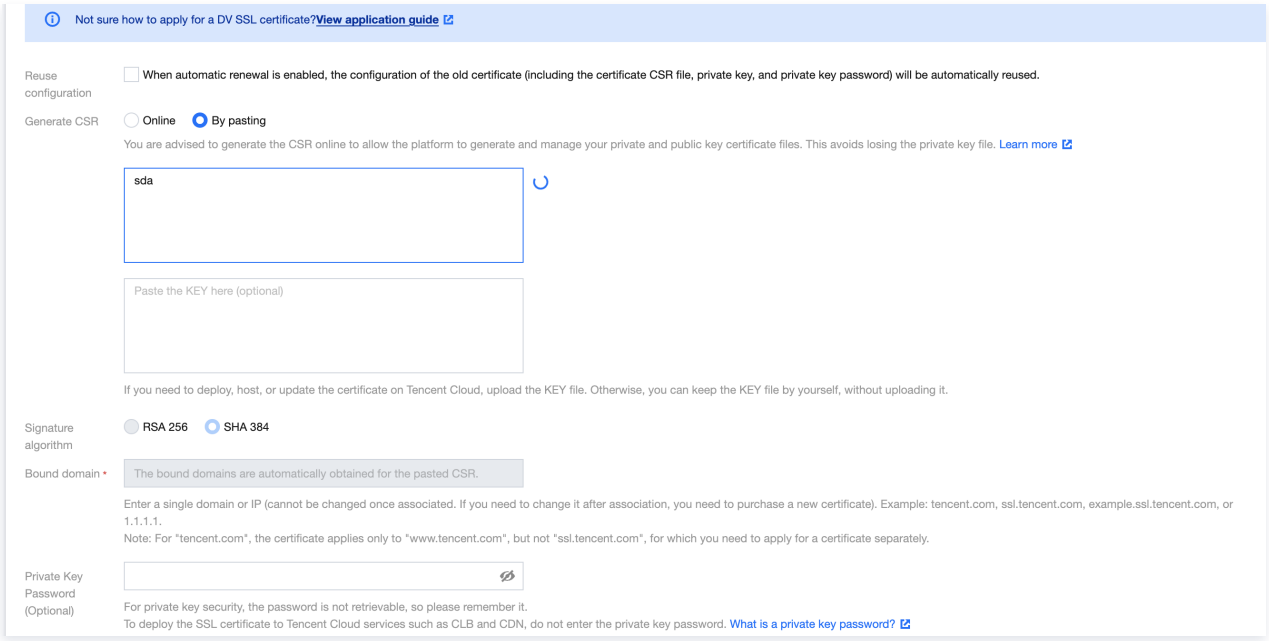
- **Bound domain**: Enter a single domain or public IP address to bind to the certificate. For example, tencent.com, ssl.tencent.com, example.ssl.tencent.com, 1.1.1.1.
- **Private Key Password**: Optional. The password cannot be modified once entered or recovered, so please keep it in mind.

2. Enter your organization information.
   - **Existing Organization**: Select **Existing Organization** to directly use the organization's information.
   - **New Organization information**: Enter full name, department, city, address, and landline number of your organization.
3. Enter the Admin information.
   - **Existing Admin**: Select **Existing Admin** to directly use the administrator's information.
   - **New Admin Information**: Please provide the accurate name, position, phone number, and email of the administrator.
4. Enter contact information. You may select **Same as the admin**.
5. Click **Next** to proceed to Step 2.

Pasting the CSR

1. Paste the prepared CSR information into the text box to identify your domain information, and fill in or select the existing company information, administrator information, and contact information, as shown in the following figure:

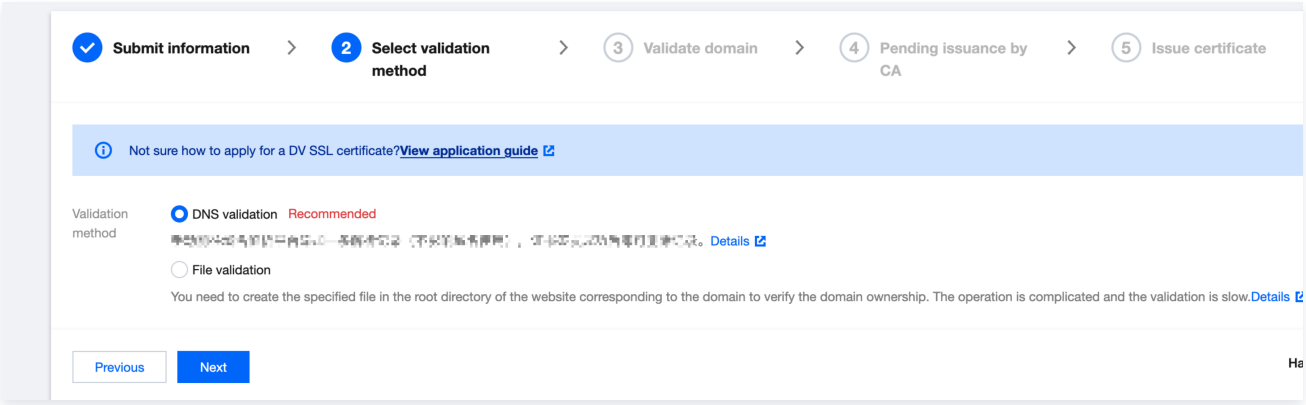
©2013–2023 Tencent Cloud. All rights reserved.



2. Click **Next** to proceed to Step 2.

Step 2: Select the domain verification method

1. On the "Select Verification Method" page, you can choose the domain verification method, as shown below:



2. After selecting the verification method, click **Next** to proceed to the "Upload Confirmation Letter" page.

Step 3: Upload the Confirmation Letter

1. On the "Upload Confirmation Letter" page, click **Download Confirmation Letter Template** and fill in the application information.
2. After completing the application form, affix your organization's official seal, scan or take a clear photo, and upload it.
3. Click **Upload** to submit the confirmation letter.

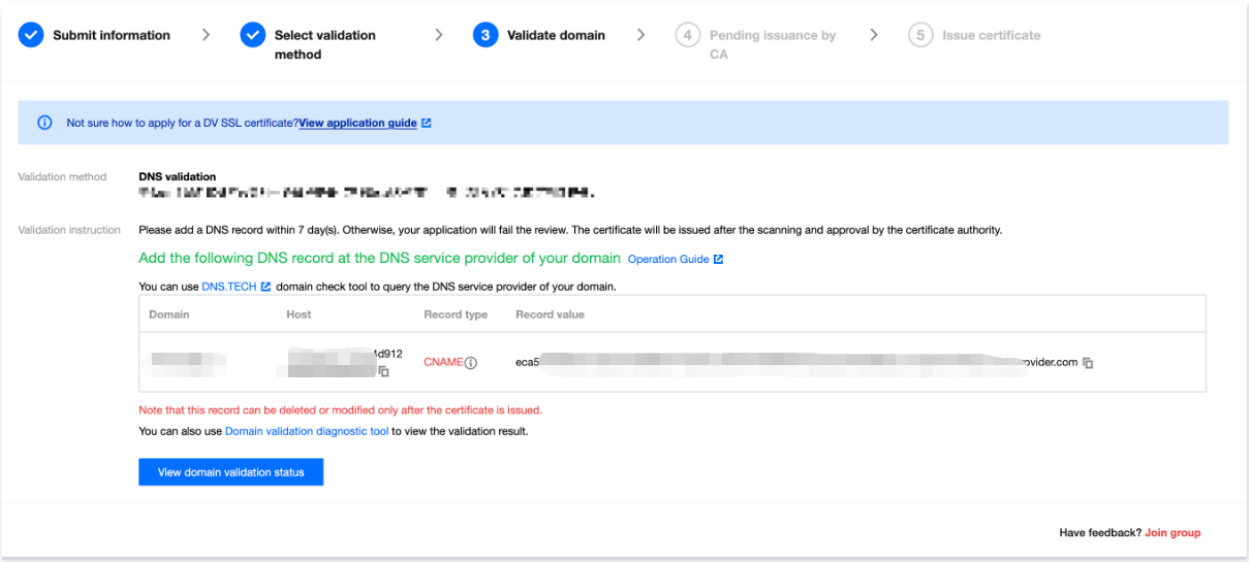
> **Note**
> - The application form supports .jpg, .gif, and .pdf formats, with a size limit of 1.4 MB.
> - After the application file is uploaded, it cannot be uploaded again. Ensure that the application file is uploaded correctly.

4. Click **Next** to proceed to the "Validate Domain" page.

Step 4. Validate your domain

1. Follow the instructions on the "Validate Domain" page to verify domain ownership. For instance, if you choose manual DNS verification, the following information will be displayed. See the image below:

©2013–2023 Tencent Cloud. All rights reserved.



- **DNS Validation**: For domain validation operations, please refer to DNS Validation.
- **File Validation**: For domain validation procedures, please refer to File Validation.

2. After completing the domain verification operation, you can click **View Domain Ownership Validation Status** to check whether the verification operation was successful.

Step 5: Undergo manual review

Once the domain validation is successful, it will proceed to the manual review stage. After the manual review is passed, the certificate will be officially issued.

> **Note**
> - Once the domain verification is successful, the verification will be retained for 13 months. Within these 13 months, if the same domain applies for DNSPod GM (SM2) OV and EV SSL certificates under the same organization name, the domain verification process will not be executed.
> - The certificate will be issued only after manual approval and domain validation.
> - It takes 3–5 business days to review OV certificates, and 5–7 business days to review EV certificates.
> - Manual approval will not be required if you apply for a certificate with the same information after having successfully applied for a certificate of the same type.

Step 6. Wait for CA to issue the certificate

After the official issuance of the certificate, you can download and install it.

©2013–2023 Tencent Cloud. All rights reserved.

Guide to Using Free SSL Certificates
Overview of Free SSL Certificate

Last updated: 2023-09-28 10:02:37

Overview of Free SSL Certificate

Tencent Cloud offers a complimentary SSL certificate primarily intended for preliminary testing, catering to users' needs for HTTPS communication during the early stages of website development.

Differences Between Free SSL Certificates and Formal SSL Certificates

> ⚠ **Note:**
> The compatibility of an official certificate is superior to that of a free certificate. For the stability of your business, it is imperative to use an official certificate for formal projects. Click here to select and purchase an official certificate.

Certificate Features	Free Certificate	Official Certificate
Domain Quota	Subject to Quota Limitations	No limit
Certificate Provider	TrustAsia	• SecureSite (DigiCert) • DNSPod • GeoTrust • GlobalSign • TrustAsia • WoTrus
Supports binding to wildcard domains (wildcards)	Unavailable	This feature is supported.
Support binding IP	Unavailable	This feature is supported.
Multi-domain	Unavailable	This feature is supported.
Installation Consultation Services	Unavailable	This feature is supported.
After-sales service	Unavailable	This feature is supported.

Rules for Free Certificate Quota

Previously, individual accounts could apply for a maximum of 20 free certificates. Now, individual accounts can apply for up to 50 free certificates, of which 20 free certificates can be bound to domain names across the internet, and 30 free certificates can be bound to Tencent Cloud domain names. Becoming a Tencent Cloud V2 member will increase the quota for binding domain names across the internet. If you wish to become a member, please proceed to Claim Tencent Cloud Membership.

Authentication Type	Account Type	Number of Free Certificates	Can be bound to Tencent Cloud domain names	Can be bound to domain names across the internet
Individual	Standard/V1 Member Account	50 certificates	30	20
	V2 Member Account	50 certificates	-	50
Enterprise	Standard/Membership Account	10	You can bind any 10 domain names.	

©2013-2023 Tencent Cloud. All rights reserved.

Remark: As of 0:00 on March 20, 2023, corporate accounts without any free certificates are only entitled to a quota of 10 free certificates. Corporate accounts with valid free certificates will continue to maintain a quota of 20 free certificates.

Note:

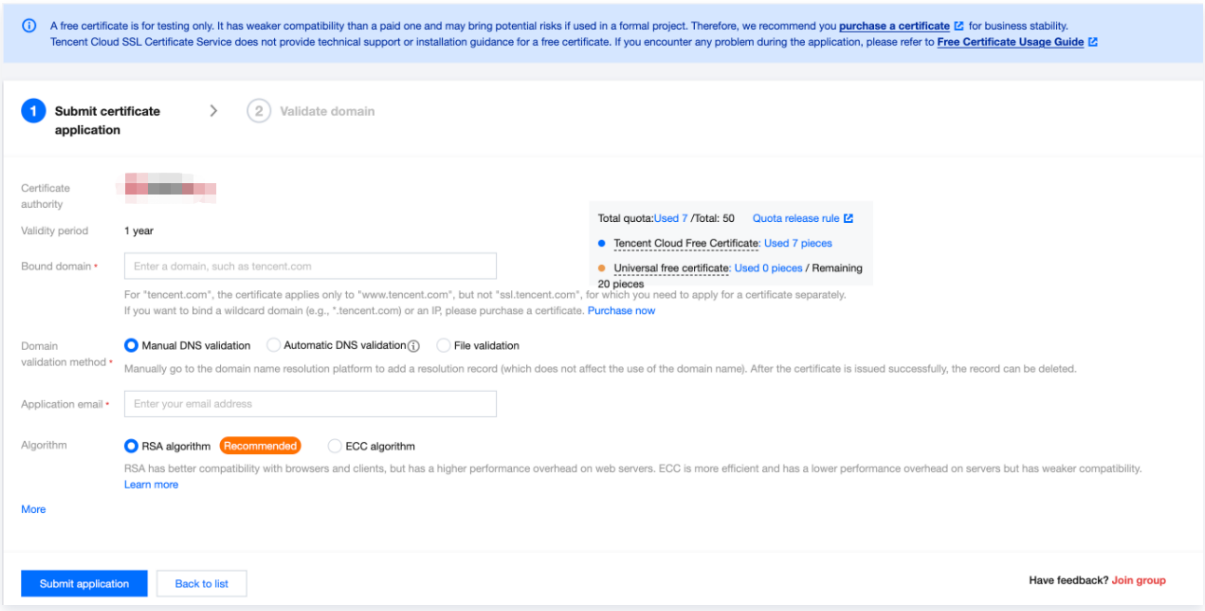
- Tencent Cloud Domains: Domains registered with Tencent Cloud or transferred into Tencent Cloud.
- Global domains: Domains registered either with Tencent Cloud or with other domain registrars.
- Quota deduction rules: If the domain you are applying for belongs to Tencent Cloud, one Tencent Cloud domain quota will be deducted first. Only when the Tencent Cloud domain quota is insufficient will the global domain quota be deducted.

Usage Restrictions of Free SSL Certificates

1. A free certificate only supports binding to a single domain and does not support binding to a wildcard domain or an IP. It also does not support domains with special suffixes applying for a free certificate. These special suffixes include, but are not limited to: .edu, .gov, .org, .ru, .jp, .pay, .bank, .live, and .nuclear.
2. Free certificates do not come with manual technical support or installation guidance. Please follow the guidance document for certificate installation and deployment.

Steps to Apply for a Free SSL Certificate

1. Log in to the SSL Certificate Service Console, navigate to the **My Certificates** page, and click on **Apply for Free Certificate**.
2. Fill in the application as required and click **Submit application**. Once the verification is complete, the review will be finalized within one business day. You will be notified of the review results via text message, email, and in-site messages. As shown in the figure below:



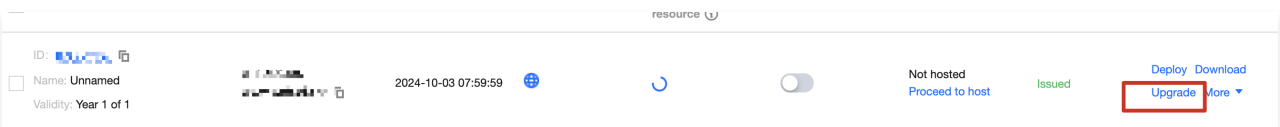
3. For a detailed application process, please refer to Free SSL Certificate Application Process.

How to Upgrade to an Official Certificate

Free SSL certificates do not support renewal and are recommended for testing purposes only. To achieve a higher level of security and enjoy human customer service support, you can upgrade to a paid SSL certificate in the following two ways.

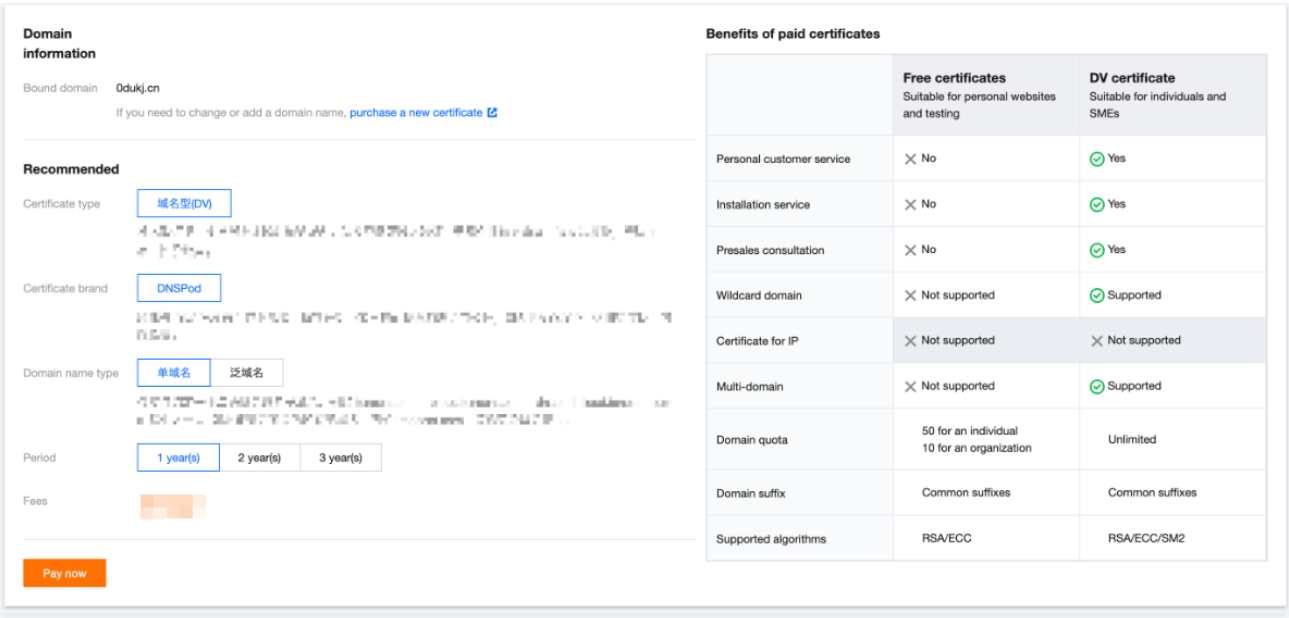
Method One: Upgrade via the Certificate Service Console

1. Log in to the SSL Certificate Service Console, navigate to the "My Certificates" management page, select the certificate that needs to be upgraded, and click on **Upgrade**. As illustrated below:



©2013-2023 Tencent Cloud. All rights reserved.

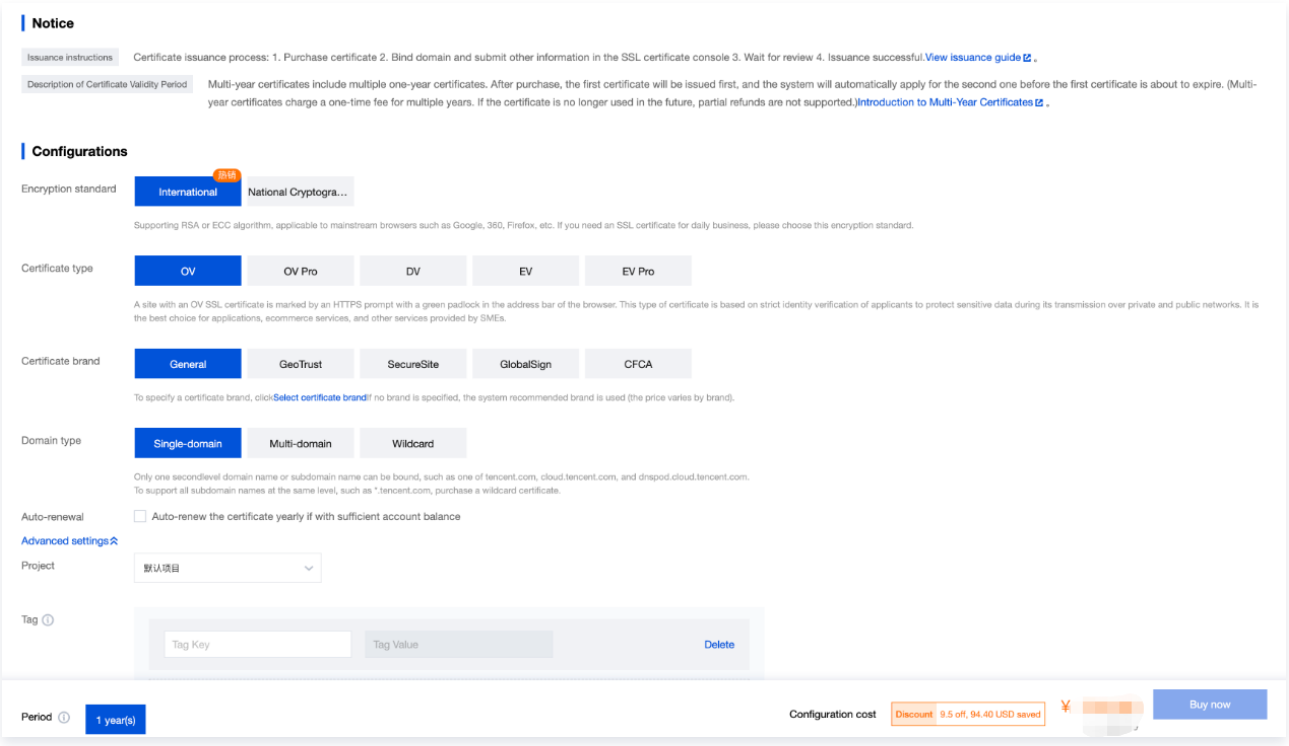
2. In the pop-up window, after confirming the certificate specifications, click **Proceed to Payment** as shown below:



Method Two: Proceed to the certificate purchase page to buy a paid certificate

Taking the purchase of a **custom configuration** paid certificate as an example.

1. Purchase a paid certificate on the SSL Certificate Purchase Page. For detailed information, please refer to the parameter comparison provided on the official website, as shown below:



2. Choose the appropriate certificate type and brand based on your industry and actual needs. For certificate types, refer to SSL Certificate Type Cases, and for certificate brands, see Introduction to SSL Certificate Brands.
3. Choose the domain name type and the number of domain names supported as needed.
4. Choose the certificate validity period as per your requirements.
5. Click **Buy Now** to proceed to the order management page and finalize the payment by clicking **Submit Order**.

©2013-2023 Tencent Cloud. All rights reserved.

Free SSL Certificate Application Process

Last updated: 2023-09-28 10:12:14

Registering an account

To apply for a certificate on Tencent Cloud, first you need to register a Tencent Cloud account and complete identity verification.

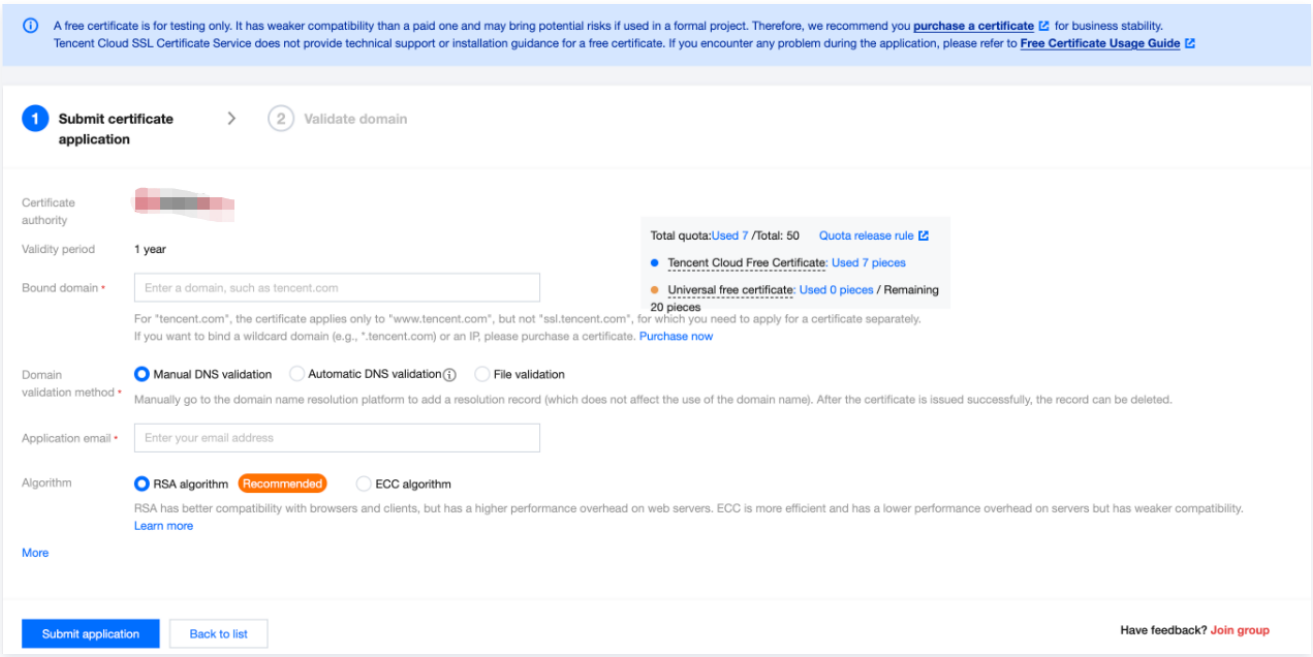
1. New users, please click Tencent Cloud's official website and select **Sign Up for Free** in the top right corner to access the registration page.
2. Please register a Tencent Cloud account to access the Tencent Cloud Console.
3. Complete identity verification before proceeding with the certificate application.

Applying for a Free Certificate

Note

- Free certificates are only available for second-level domain names and their subdomains, and do not support IP or wildcard domain applications. For example, `dnspod.cn` and `docs.dnspod.cn`.
- Within the scope of TrustAsia (not necessarily applied through Tencent Cloud), a maximum of 20 free certificates can be applied for the same primary domain. When applying, please check whether the domain has TrustAsia certificates on other service provider platforms to avoid reaching the application limit. For more details, please refer to Free Certificate Quota Related Questions.
- If you wish to continue using a free certificate after its expiration, please reapply and install it.

1. Log in to the SSL Certificate Service Console, navigate to the **My Certificates** page, and click on **Apply for a Free Certificate**.
2. Fill out the certificate application form as shown below:



- **Bound domain:** Enter a single domain, such as `tencent.com` or `ssl.tencent.com`.
- **Domain Validation Method:**

  Note

  - Automatic DNS Verification: For the verification method, please refer to Automatic DNS Addition.

    If the domain name applied for is successfully hosted on the DNSPod DNS Console, automatic DNS addition is supported.
  - Manual DNS verification: For the verification method, please refer to DNS Validation.
  - File Verification: For the verification method, see File Verification.

©2013-2023 Tencent Cloud. All rights reserved.

- **Application Email** : Please enter your email address.
- **Algorithm**: Choose the desired encryption algorithm for your certificate. For more information about the algorithms, refer to What are the differences between RSA and ECC encryption algorithms?
- **Certificate Name**: Optional, please enter a remark for the certificate, not exceeding 200 characters.
- **Private Key Password**: Optional. To ensure the security of your private key, **password recovery is NOT supported**, so please remember the password.

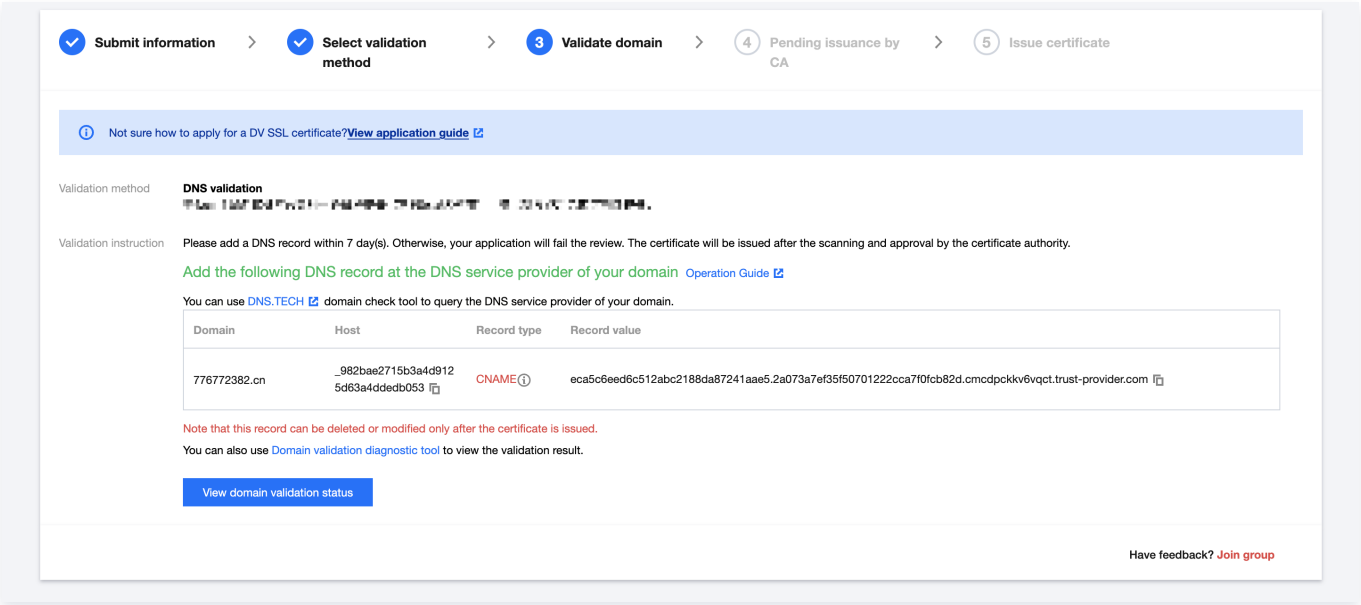
> **Note**
> If you need to deploy Tencent Cloud services such as Cloud Load Balance or CDN, do not enter the private key password.

- **Tag**: Select your tag key and tag value to better manage existing Tencent Cloud resources by category.

> **Note**
> To add tags, please refer to Managing Tags.

- **Project**: Please select the project to which your certificate belongs, making it convenient for you to manage your certificates through the project.

3. Follow the **verification instructions** to complete domain identity validation, and click **Finish**. As shown in the image below:



4. Once the domain verification is approved, the CA will issue the certificate within 24 hours. Please be patient.

> **Note**
> The submitted domain failed the security review by the certificate authority. For specific reasons, please refer to Reasons for Security Review Failure.

Download and Deployment

After completing the domain verification, you can click **Download** to obtain the issued certificate for local installation and deployment, or deploy it to relevant Tencent Cloud services. For related operations, please refer to How to choose the SSL certificate installation and deployment type?

FAQs

- Queries Related to Free SSL Certificate Quota
- Can the TXT records for domain name resolution configured in the SSL certificate be deleted?
- What should I do if I forget my private key password?
- What should I do if the free SSL certificate remains unverified?

©2013–2023 Tencent Cloud. All rights reserved.