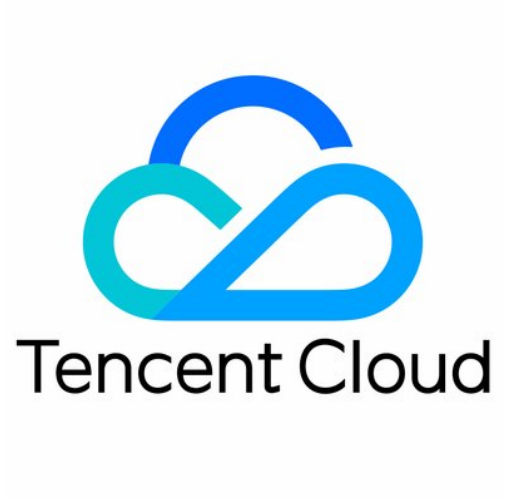
SSL Certificate Service

Purchase Guide

Product Documentation



Contents

Purchase Guide
Pricing

Last updated：2019-07-22 12:31:39

Note:

- **Single-domain Name** Only one domain name can be bound, which can be a second-level domain name like example.domain.com, a third-level domain name like example.example.domain.com, or a first-level domain name like domain.com. But all sub-domains under the first-level domain name are not supported. Up to 100 levels of domain name can be supported.
- **Multi-domain name** One single certificate can be bound to multiple domain names, subject to the maximum number of supported domain names displayed in the sale information at Tencent Cloud's official website.
- **Wildcard domain name** Only one wildcard domain name with only one wildcard can be bound, such as *.domain.com and *.example.domain.com (up to 100 levels). Multi-wildcard domain names like *.*.domain.com are not supported.
- **Multi-wildcard domain name** Multiple wildcard domain names with only one wildcard can be bound, such as *.domain.com and *.example.domain.com (up to 100 levels). Multi-wildcard domain names like *.*.domain.com are not supported.

All the unit prices below are based on one year of purchase.

Certificate Brand	Supported Domain Name Types	Certificate Model	Unit Price (only for the first year of purchase and subject to any discounts for subsequent years displayed in the sale information at Tencent Cloud's official website)	Remarks
Symantec	Single-domain name	OV SSL certificate	809 USD/year	-
	Single-domain name	OV Pro SSL certificate	1294 USD/year	-
	Single-	EV SSL	1294 USD/year	-

	domain name	certificate		
	Single-domain name	EV Pro SSL certificate	2071 USD/year	-
	Multi-domain name	OV SSL certificate for multi-domain name	809 USD/year	The total price is calculated by multiplying the unit price by the number of domain names
	Multi-domain name	OV Pro SSL certificate for multi-domain name	1294 USD/year	The total price is calculated by multiplying the unit price by the number of domain names
	Multi-domain name	EV SSL certificate for multi-domain name	1294 USD/year	The total price is calculated by multiplying the unit price by the number of domain names
	Multi-domain name	EV Pro SSL certificate for multi-domain name	2071 USD/year	The total price is calculated by multiplying the unit price by the number of domain names
	Wildcard domain name	OV SSL certificate for wildcard domain name	6471 USD/year	-
GeoTrust	Single-domain name	OV SSL certificate	461 USD/year	-
	Single-domain name	EV SSL certificate	785 USD/year	-

	Wildcard domain name	OV SSL certificate for wildcard domain name	1108 USD/year	-
	Multi-domain name	OV SSL certificate for multi-domain name	903 USD/year; an additional domain name is priced at 105 USD/year	5 domain names are supported by default, and an additional domain name is priced at 105 USD/year
	Multi-domain name	EV SSL certificate for multi-domain name	1561 USD/year; an additional domain name is priced at 235 USD/year	5 domain names are supported by default, and an additional domain name is priced at 235 USD/year
TrustAsia	Single-domain name	OV SSL certificate	728 USD/year	-
	Single-domain name	EV SSL certificate	1537 USD/year	-
	Multi-domain name	OV SSL certificate for multi-domain name	1051 USD/year	2 domain names are supported by default, and an additional domain name is priced at 324 USD/year
	Multi-domain name	EV SSL certificate for multi-domain name	2103 USD/year	2 domain names are supported by default, and an additional domain name is priced at 566 USD/year
	Wildcard domain name	DV SSL certificate for	323 USD/year	-

		wildcard domain name		
	Wildcard domain name	OV SSL certificate for wildcard domain name	2184 USD/year	-
	Multi-wildcard domain name	OV SSL certificate for multi-wildcard domain name	4368 USD/year	2 domain names are supported by default, and an additional domain name is priced at 2184 USD/year
GlobalSign	Single-domain name	OV SSL certificate	603 USD/year	-
	Single-domain name	EV SSL certificate	1598 USD/year	-
	Multi-domain name	OV SSL certificate for multi-domain name	923 USD/year	2 domain names are supported by default, and an additional domain name is priced at 320 USD/year
	Multi-domain name	EV SSL certificate for multi-domain name	2080 USD/year	2 domain names are supported by default, and an additional domain name is priced at 482 USD/year
	Wildcard domain name	OV SSL certificate for wildcard domain name	2111 USD/year	-

	Multi-wildcard domain name	OV SSL certificate for multi-wildcard domain name	4221 USD/year	2 domain names are supported by default, and an additional domain name is priced at 2111 USD/year

Purchase Procedure

Last updated：2019-10-30 10:05:53

1. Select a certificate brand and model

Tencent Cloud provides four brands of SSL certificates for sale, as shown below:

Symantec

Symantec, the world's largest information security service producer and provider and the most authoritative digital certification authority. It offers a wide range of content and network security solutions to businesses, individual users and service providers. 93% of the Fortune 500 companies choose VeriSign SSL digital certificates. Symantec acquired VeriSign in August 2010, and since then has provided the verification services of VeriSign. In April 2012, Symantec changed VeriSign's product name and brand logo.

GeoTrust

GeoTrust, the world's second-largest digital certification authority (CA) and a leader in authentication and trust certification, provides state-of-the-art technologies that enable organizations and companies of all sizes to deploy SSL digital certificates securely and cost-effectively and achieve a wide range of authentications. GeoTrust was founded in 2001, and to 2006, it has takes 25% of global market share. VeriSign acquired GeoTrust with USD 125 million in May-September 2006, which is now also a **cost-effective** SSL certificate brand of Symantec.

From a technical point of view, the differences between Symantec (formerly VeriSign) and GeoTrust are as shown below:

1. Symantec (supporting RSA, DSA and ECC) is superior to Geotrust (supporting RSA and DSA) on algorithm.
2. Symantec is superior to Geotrust on compatibility. Symantec is compatible with all browsers on the market, and also shows very good compatibility for mobile devices.
3. Symantec is superior to Geotrust on OCSP response.
4. Symantec is superior to Geotrust on CA security. As an internationally renowned security vendor, Symantec provides the number one CA security in the world.
5. In addition to encrypted data transfer, Symantec certificates provide malware scanning and vulnerability assessment features.
6. A maximum of USD 1.75 million in certificate commercial insurance compensation is provided by Symantec, while the number of GeoTrust is USD 1.5 million.

TrustAsia

TrustAsia is a brand of Yashu Information Technology (Shanghai) Co., Ltd in the field of information security. It is a platinum partner of Symantec™. TrustAsia specializes in providing businesses with all network security services including digital certificates. TrustAsia SSL certificates are issued by the Symantec root certificates.

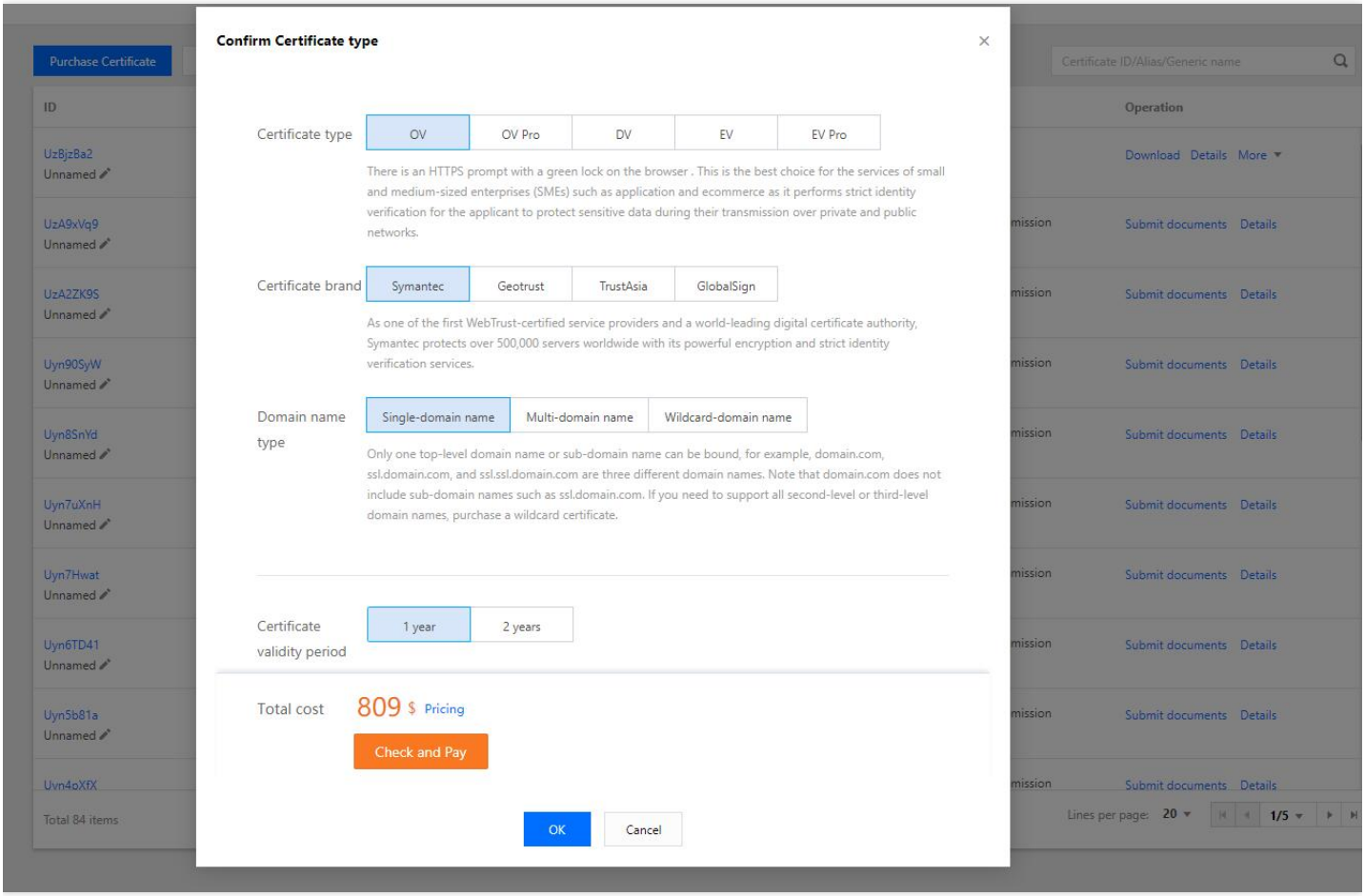
GlobalSign

Founded in 1996, GlobalSign is a reputable and trusted CA and provider of SSL and digital certificates with more than 20 million digital certificates issued worldwide. It supports a great number of server providers, domain name registrars, and system service providers in the Chinese market thanks to its professional strengths as their digital certificate service partner.

Brand Differences

Certificates of different brands vary on browser address bar, encryption level, and guaranteed compensation. The most important difference lies in root certificates. For example, a Geotrust wildcard certificate is issued by Geotrust root certificate, while a Symantec wildcard certificate is issued by Symantec root certificate which is compatible with all browsers on the market and also supports mobile devices best. TrustAsia's wildcard certificates are issued by Symantec root certificates, and GlobalSign's wildcard certificates are issued by its own root certificates.

For more information, see parameters comparison provided in SSL Certificate Service Console.



2. Select the number of supported domain names

Single-domain name

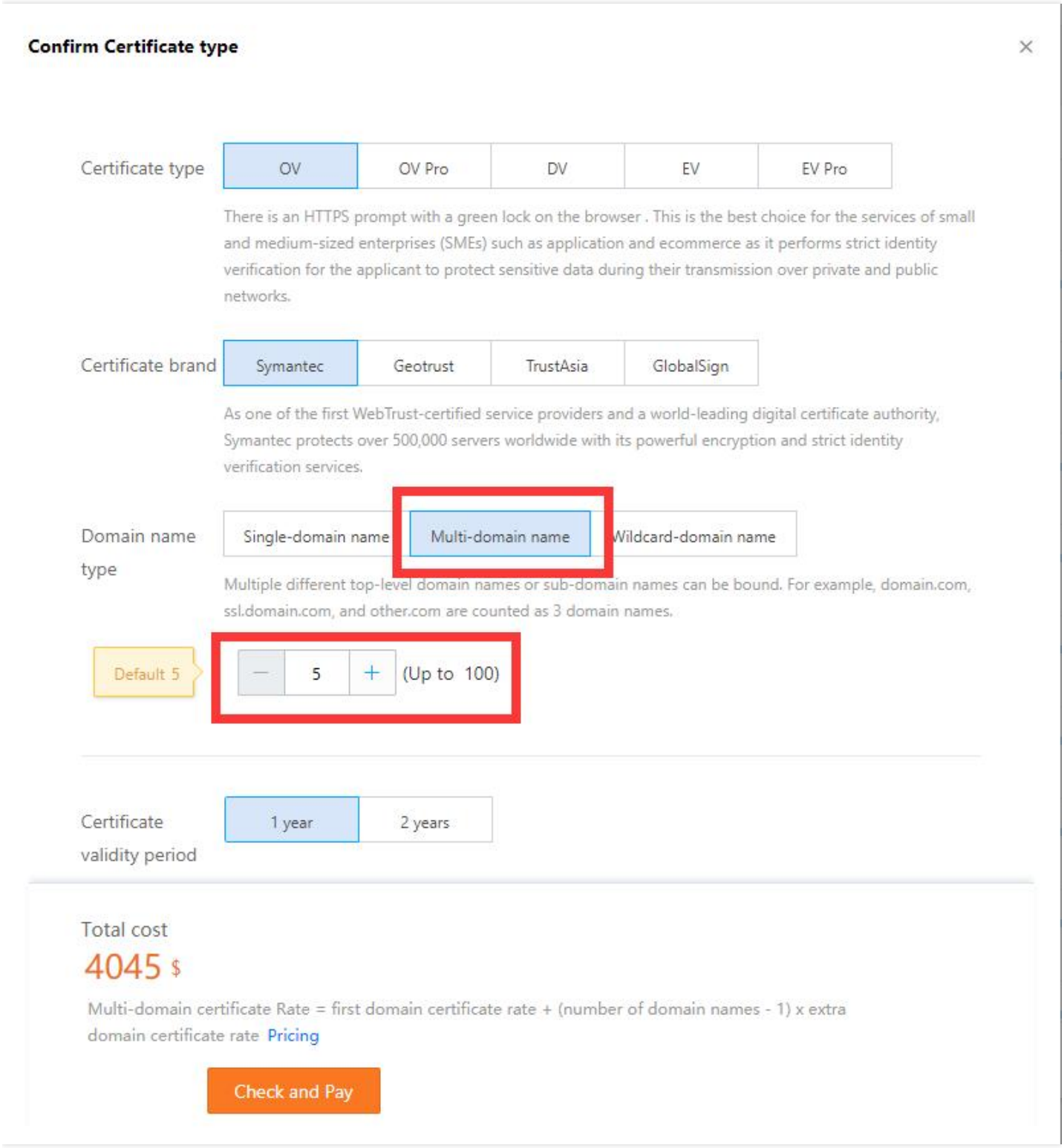
It only allows to bind one domain name, which can be a second-level domain name like example.domain.com, a third-level domain name like example.example.domain.com, or a first-level domain name like domain.com. **But all sub-domains under the first-level domain name are not supported**. Up to 100 levels of domain name can be supported.

> An SSL certificate bound to the domain name www.domain.com (subdomain is www) supports the first-level domain name domain.com.

Multi-domain name

One single certificate can be bound to multiple domain names, subject to the maximum number of supported domain names displayed in the console.

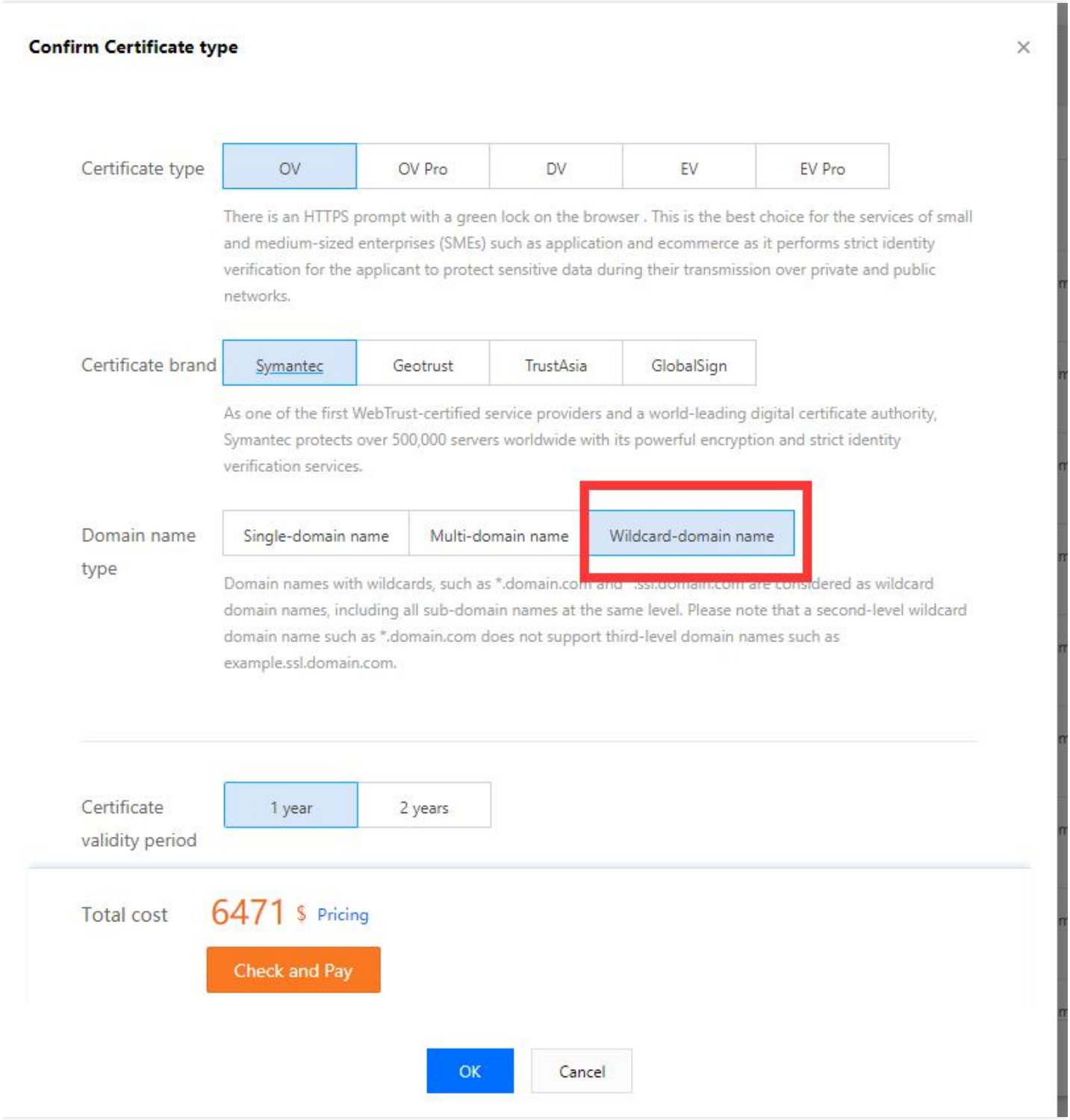
- The price of Symantec multi-domain name certificates are calculated based on the number of domain names.
- GeoTrust, TrustAsia, and GlobalSign multi-domain name certificates in excess of the default number of supported domain names are charged additionally.



Wildcard domain name

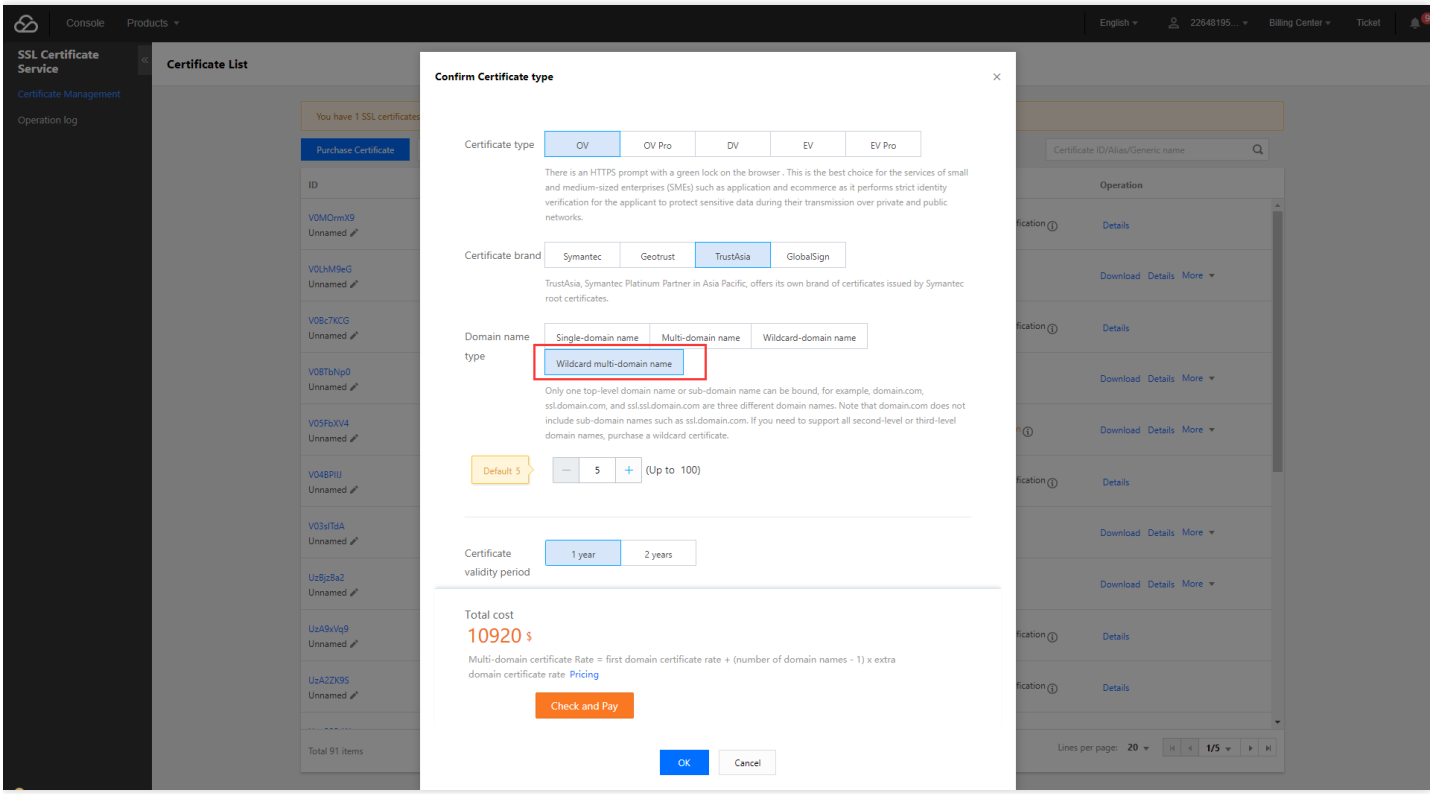
Only one wildcard domain name with only one wildcard can be bound, such as *.domain.com and *.example.domain.com (up to 100 levels). Multi-wildcard domain names like *.*.domain.com are not supported.

An SSL certificate bound to the domain name *.domain.com (which must be a second-level wildcard domain name) supports the first-level domain name domain.com.



Multi-wildcard domain name

Multiple wildcard domain names can be bound. For example, *.domain.com, *.ssl.domain.com, and *.another.com are counted as three wildcard domain names in total, including all the sub-domain names at the same level, subject to the maximum number of supported domain names displayed in the console.



3. Select certificate validity

OV and EV certificates can be valid for up to 2 years, while DV certificates can be valid for up to 1 year.

4. Payment

After selecting the brand, model, supported domain name, and certificate validity, you can submit the order and proceed with the payment process.

5. Submit the application

After purchasing a certificate, you need to submit approval materials in SSL Certificate Service Console for certificate application. The certificate will be issued upon approval by the CA. For more information, see Material Submission for OV/EV SSL Certificate.

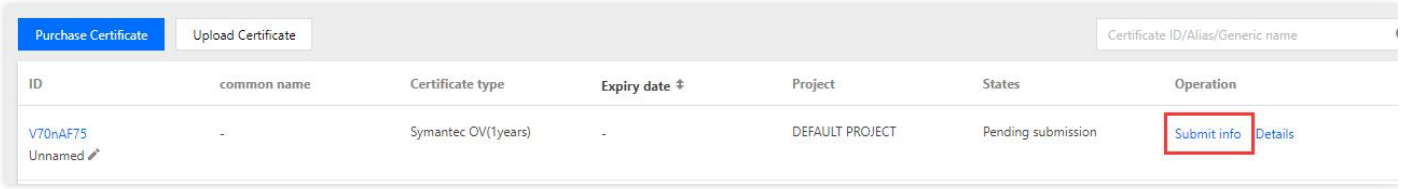
Material Submission for OV/EV SSL Certificates

Last updated：2019-10-31 17:13:11

After you successfully purchase an OV, OV Pro, EV, or EV Pro SSL certificate (see purchase process for details), you need to submit relevant information for review.
After the CA approves the information, the official certificate will be issued and you can download the paid certificate for installation.

Information Submission Portal

1. Log in to the SSL Certificates Service Console.
2. On the "Certificate List" page, select a certificate you have purchased and click "Submit info", as shown below:



Entering the Domain Name

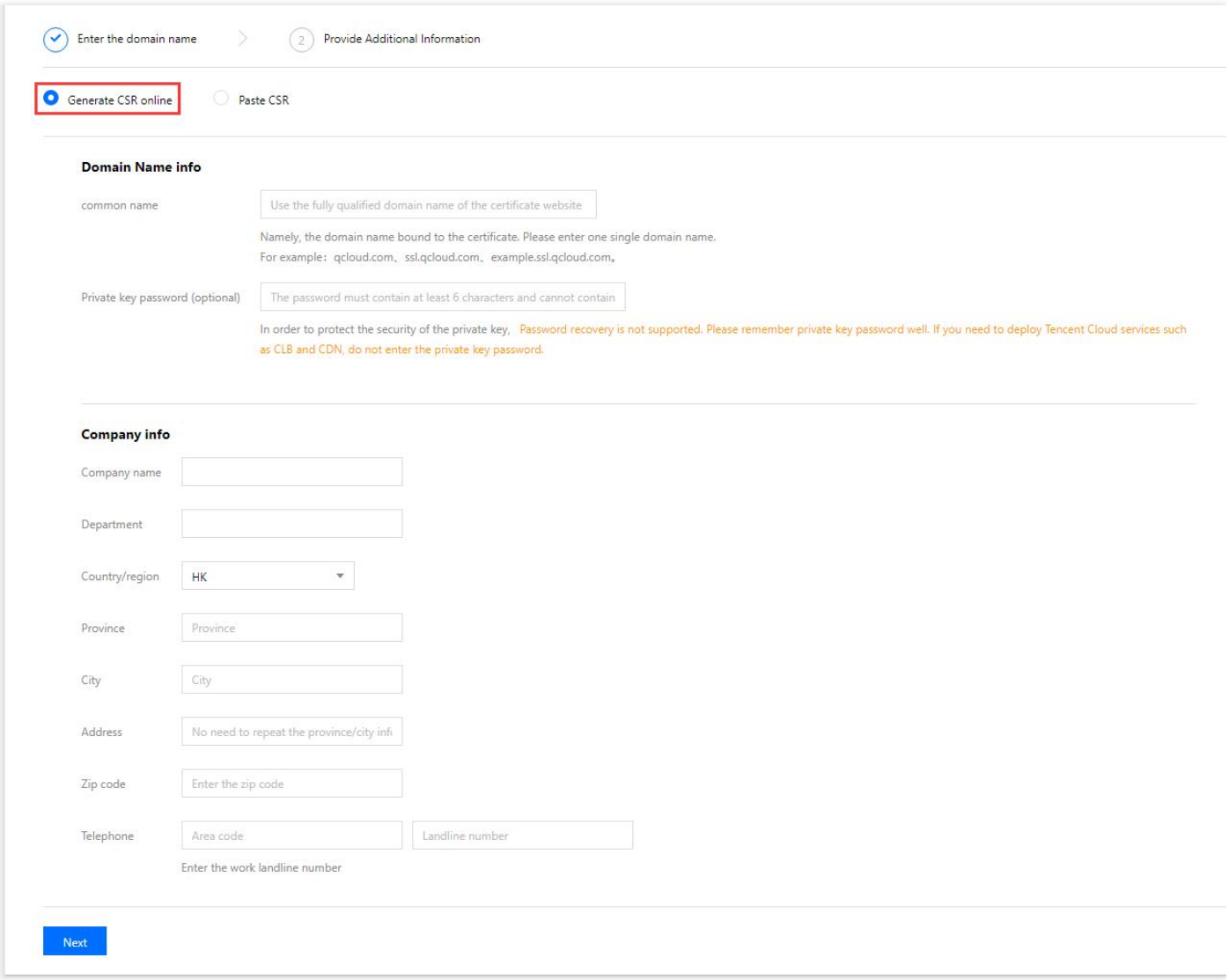
Select the CSR generation method based on your actual needs.

- Select "Generate CSR online" to generate the CSR online.
- Select "Paste CSR" to paste the CSR.

Generate CSR online

> The information required varies by certificate type. Below is an example with a multi-domain name certificate.

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



Key parameters are as follows:

- Generic Name: Enter the domain name/wildcard domain name to be bound to the certificate.
- Domain Name: Enter domain names/wildcard domain names other than the generic name.

> This parameter is not available for single-domain name certificates.

- Private Key/Passphrase: This is optional and cannot be modified once entered.

2. Enter your organization information.

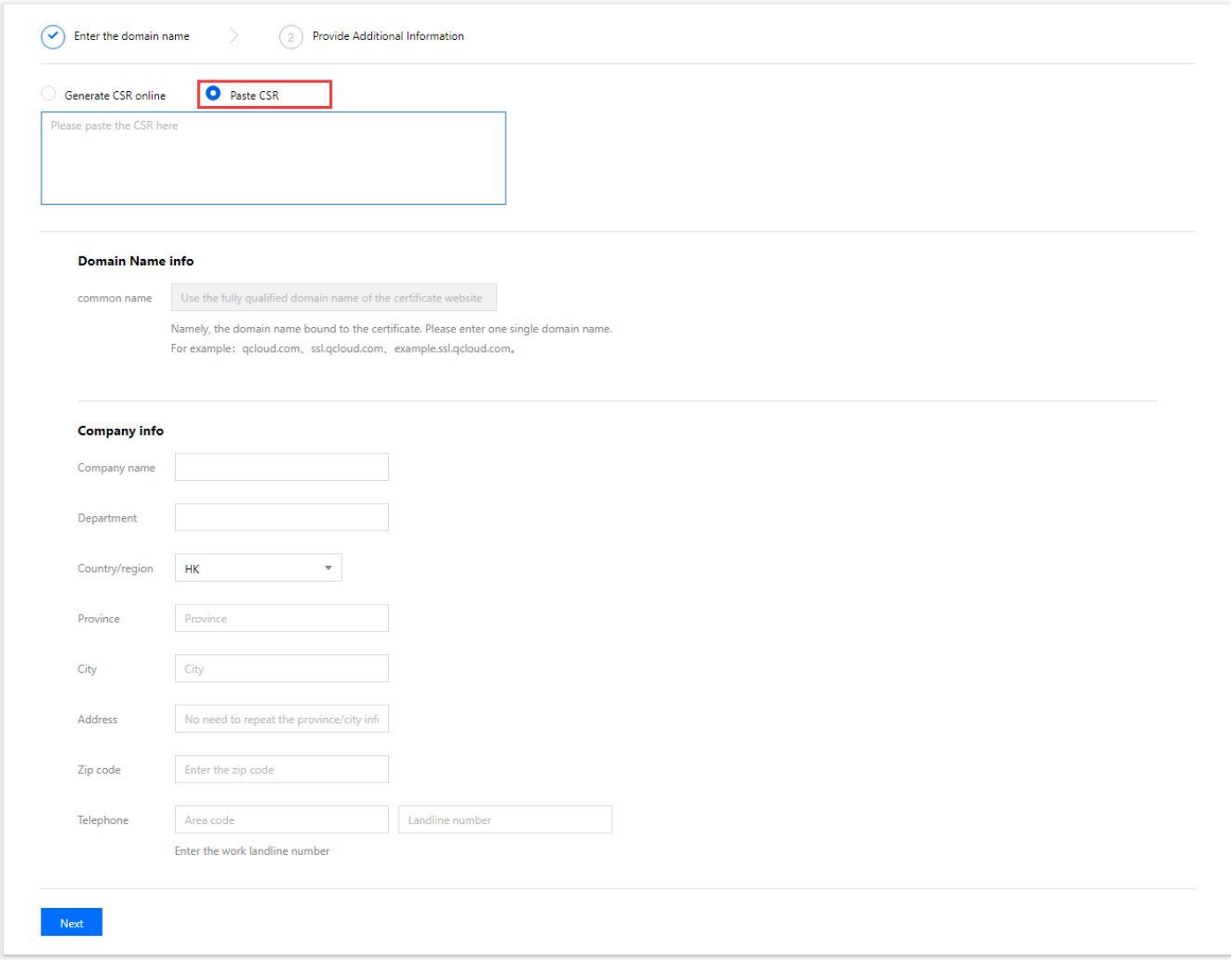
> Please enter the company name (full name), departments, city, address, and telephone number.

3. Click **Next** to provide additional information.

Paste CSR

> The information required varies by certificate type. Below is an example with a single-wildcard domain name certificate.

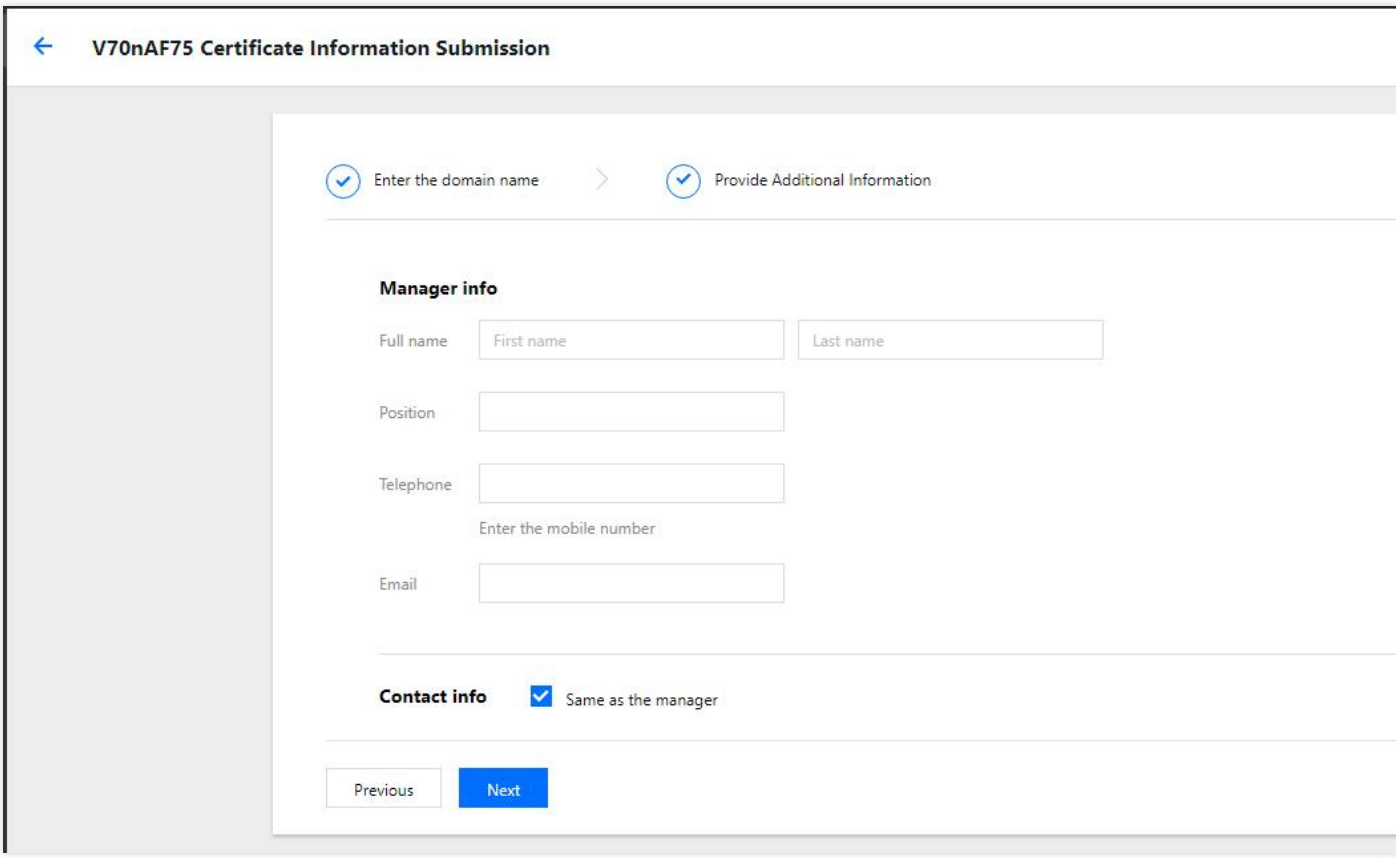
1. Paste the prepared CSR information into the text box, enter the domain name information, and enter the company name (full name), departments, city, address, and telephone number as shown below:



2. Click **Next** to provide additional information.

Providing Additional Information

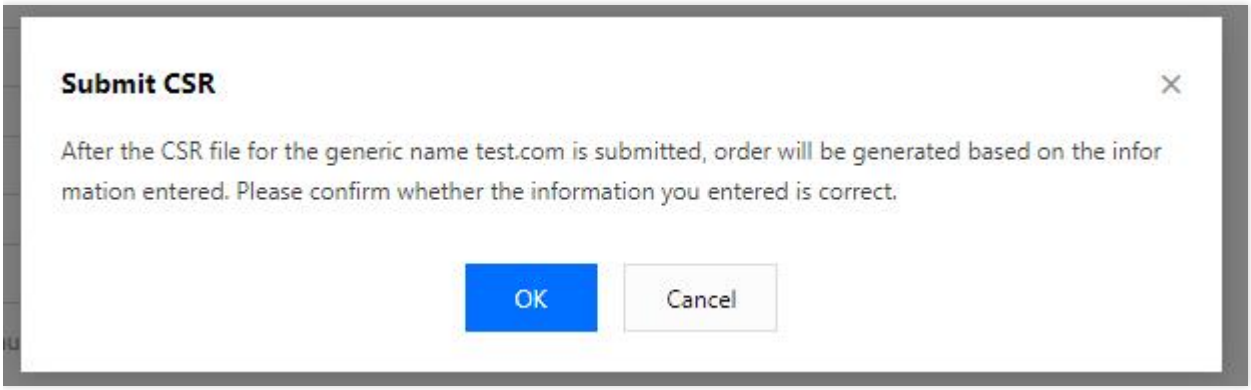
1. Fill in the administrator and contact information. If they are the same, you can check "Same as the administrator", as shown below:



2. Click **Next**.

Uploading for Review

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.



OV/EV SSL Certificates Renewal

Last updated：2019-10-31 17:13:34

Renewing an SSL certificate is equivalent to applying for a new certificate in the console, so you need to install and deploy the new certificate to the server. The new certificate does not affect the normal use of the existing one.

> If you need to modify the certificate information, please apply for a new one.

Advantages of Renewal

Renewing the existing certificate shows the following advantages over purchasing a new one:

Simplified renewal procedure

Instead of entering the application information again, you only need to confirm the original certificate's application data pulled automatically by the system to enter the payment process. After making the payment, please upload the confirmation letter and wait for certificate review.

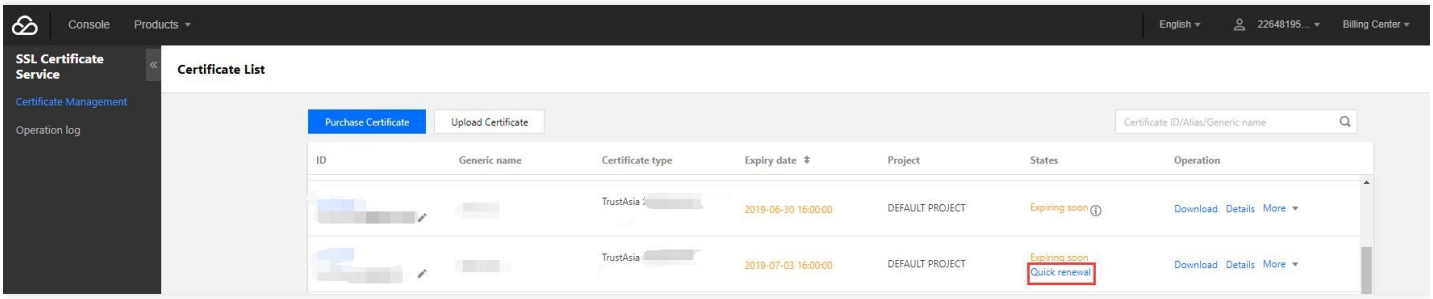
Extra-prolonged certificate validity after renewal

After renewal, the unused time of the original certificate and a complimentary period of 1 to 90 days will be added to the validity of the new certificate. You will not suffer any loss in terms of certificate validity period due to renewal.

Certificate Renewal Procedure

Enter the certificate renewal entry

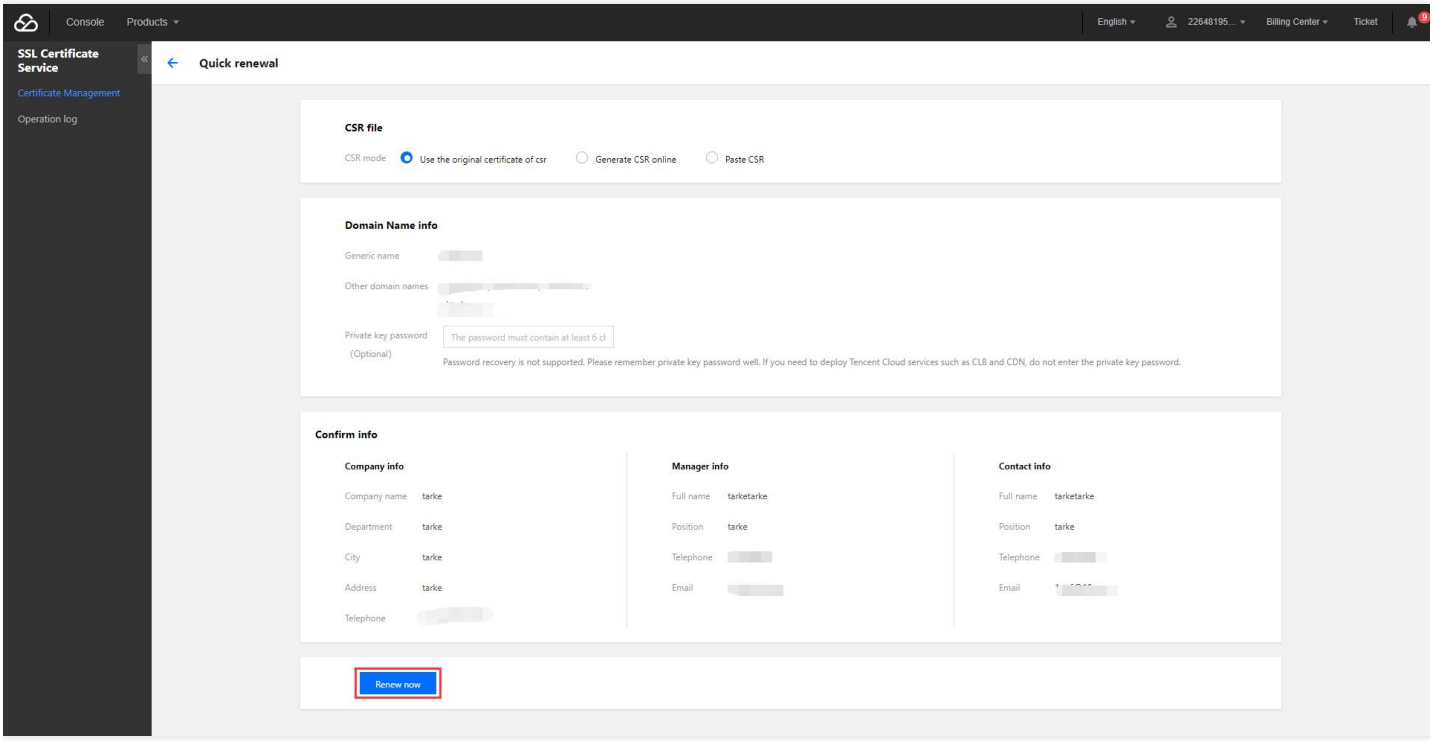
(1) For a paid DV certificate, the fast renewal option will become available 3 months before its expiration date. You can open the fast renewal window by clicking **Fast Renewal** in the "Status" column of the certificate in the certificate list in the SSL Certificate Service Console.



(2) In the SSL certificate renewal prompt page, confirm the information and click **Go to Renewal** to enter the renewal page.

Confirm the renewal information and make the payment

(1) For certificate renewal, you do not need to enter the information again. As a new certificate will be generated after the renewal, you need to set the CSR file for the new certificate. You can automatically generate a CSR file through the system or upload a CSR file on your own.
(2) After confirming the information, you can select the renewal period and click **Quick Pay** to enter the payment process.



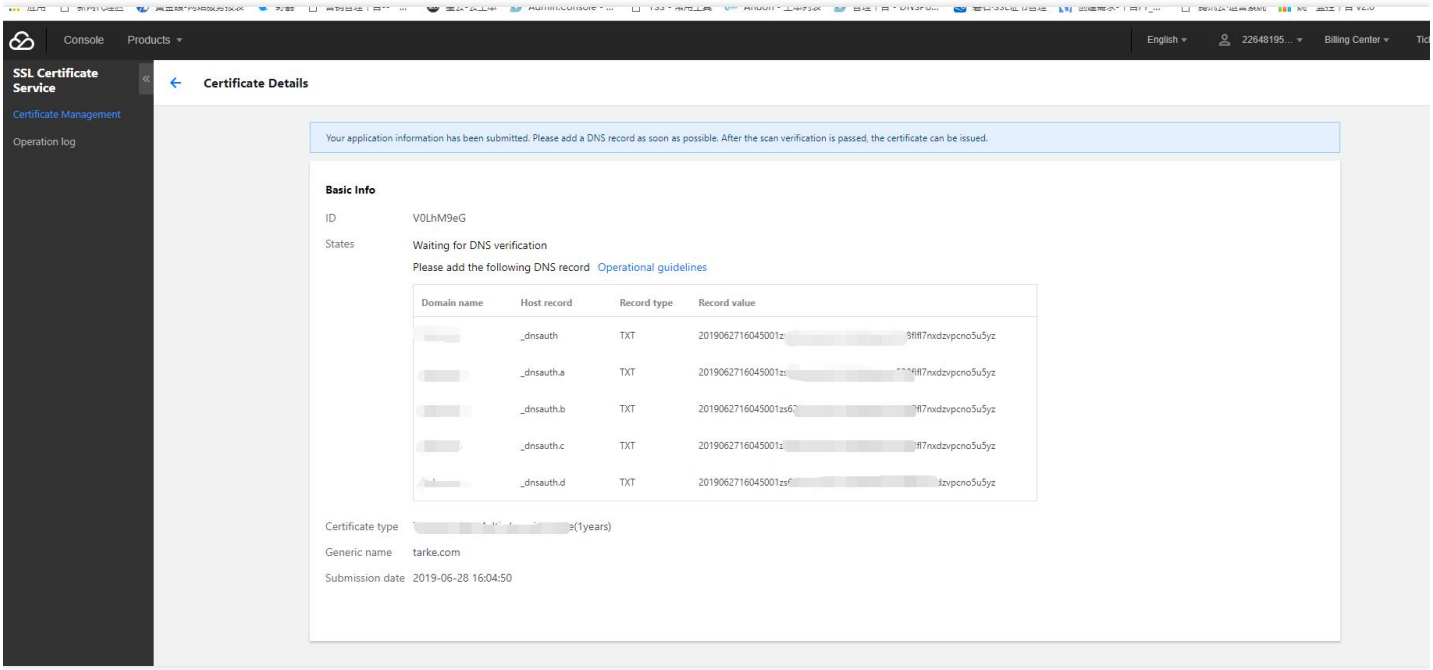
(3) Confirm the certificate information and click **Purchase** for payment.

Complete domain name authentication

(1) After purchasing a certificate successfully, you can find a new certificate generated in the certificate list of the SSL Certificate Service Console, with the status of **To be verified**. Then you can click **Details** to go to

the certificate details page.

(2) The DNS verification value will be generated in the certificate details. You need to add that DNS record and wait for scan and verification by the CA. The certificate will be issued immediately after approval.



Paid DV SSL Certificates Renewal

Last updated：2019-10-31 17:13:41

Renewing an SSL certificate is equivalent to applying for a new certificate in the console, so you need to install and deploy the new certificate to the server. The new certificate does not affect the normal use of the existing one.

> If you need to modify the certificate information, please apply for a new one.

Advantages of Renewal

Renewing the existing certificate shows the following advantages over purchasing a new one:

Simplified renewal procedure

Instead of entering the application information again, you only need to confirm the original certificate's application data pulled automatically by the system to enter the payment process. After making the payment, please upload the confirmation letter and wait for certificate review.

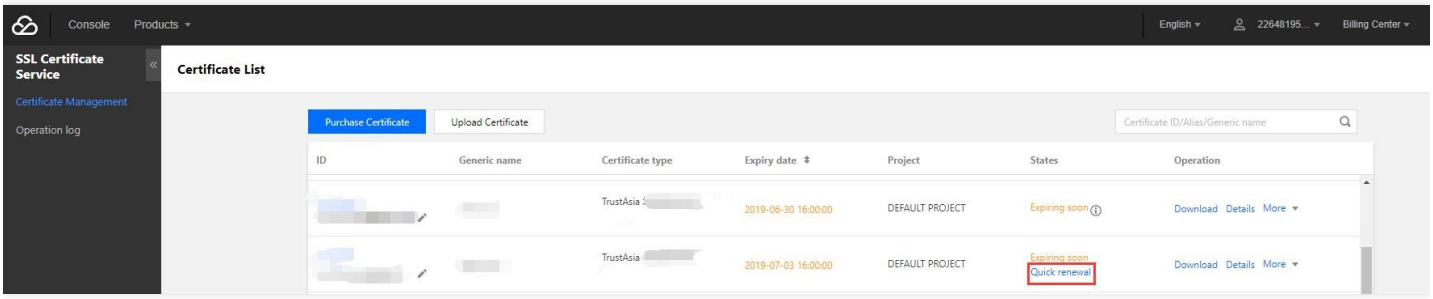
Extra-prolonged certificate validity after renewal

After renewal, the unused time of the original certificate and a complimentary period of 1 to 90 days will be added to the validity of the new certificate. You will not suffer any loss in terms of certificate validity period due to renewal.

Certificate Renewal Procedure

Enter the certificate renewal entry

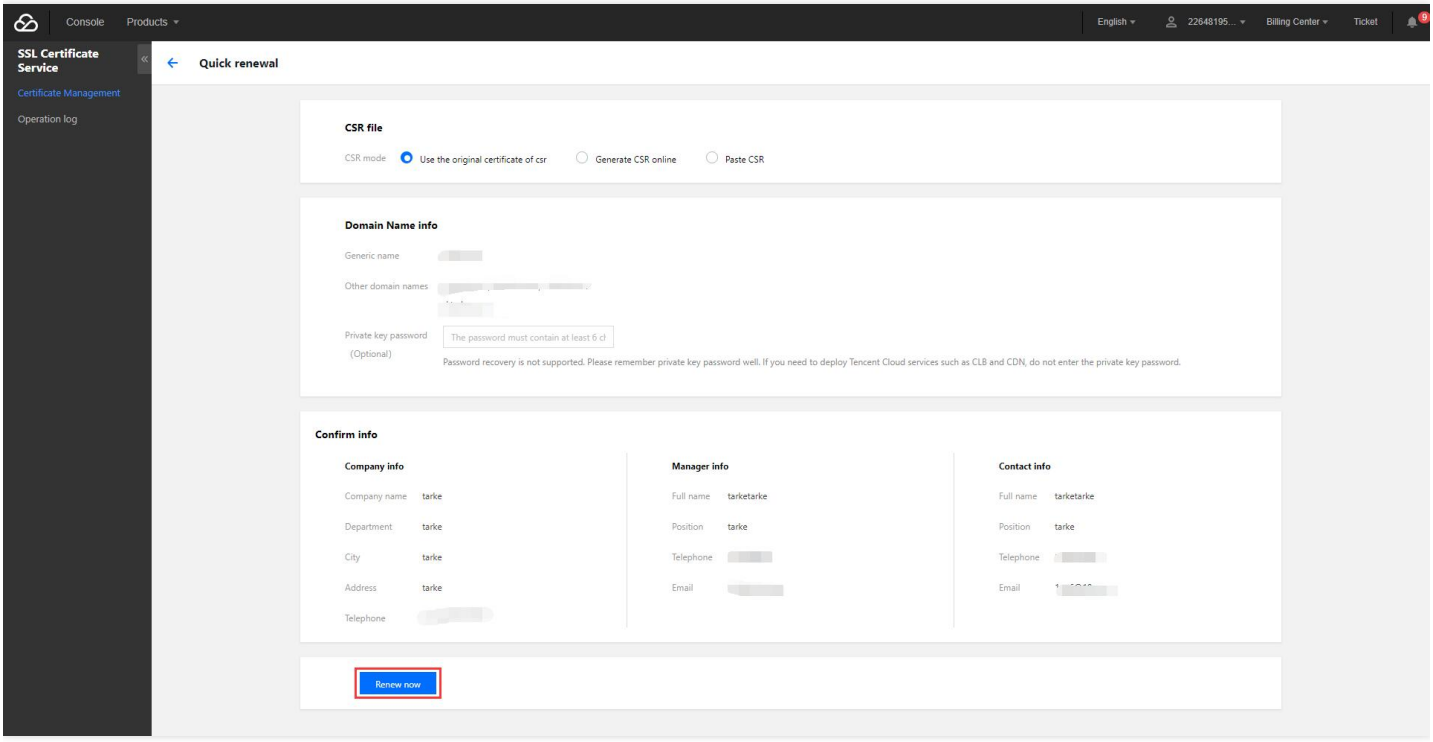
(1) For a paid DV certificate, the fast renewal option will become available 3 months before its expiration date. You can open the fast renewal window by clicking **Fast Renewal** in the "Status" column of the certificate in the certificate list in the SSL Certificate Service Console.



(2) In the SSL certificate renewal prompt page, confirm the information and click **Go to Renewal** to enter the renewal page.

Confirm the renewal information and make the payment

(1) For certificate renewal, you do not need to enter the information again. As a new certificate will be generated after the renewal, you need to set the CSR file for the new certificate. You can automatically generate a CSR file through the system or upload a CSR file on your own.
(2) After confirming the information, you can select the renewal period and click **Quick Pay** to enter the payment process.



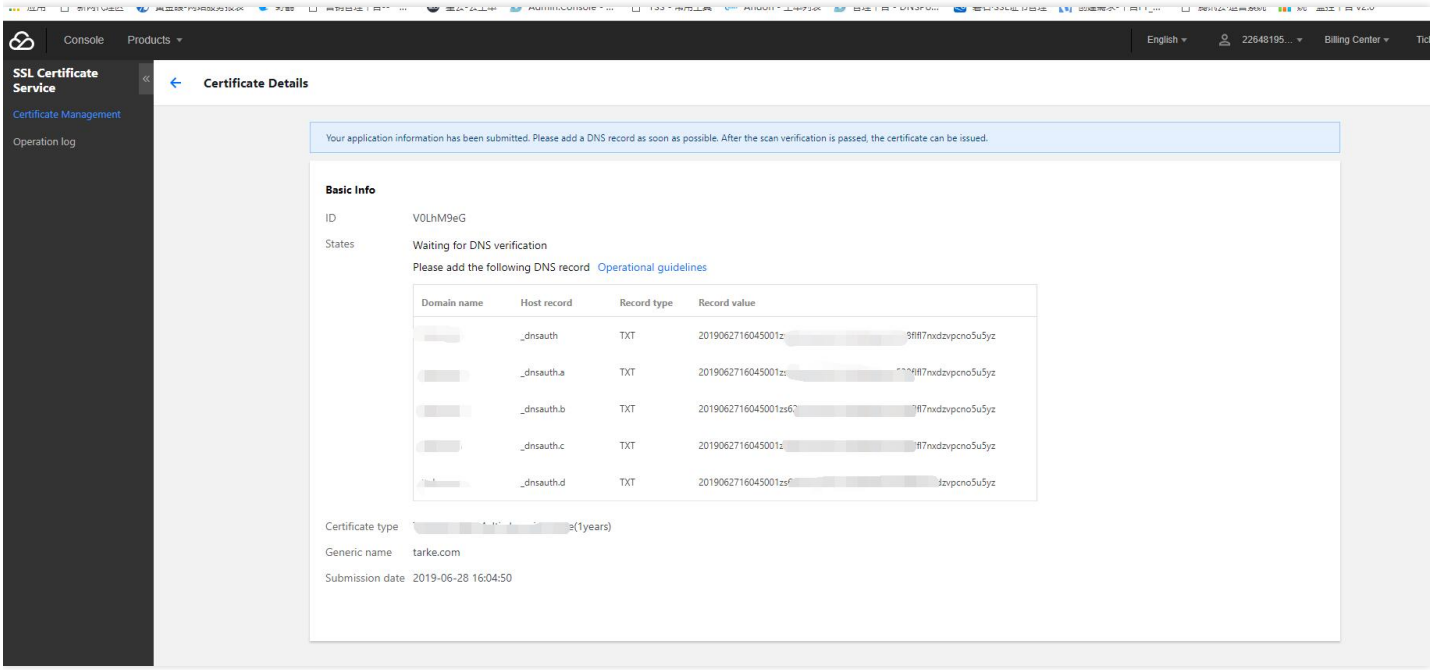
(3) Confirm the certificate information and click **Purchase** for payment.

Complete domain name authentication

(1) After purchasing a certificate successfully, you can find a new certificate generated in the certificate list of the SSL Certificate Service Console, with the status of **To be verified**. Then you can click **Details** to go to

the certificate details page.

(2) The DNS verification value will be generated in the certificate details. You need to add that DNS record and wait for scan and verification by the CA. The certificate will be issued immediately after approval.



Refund

Last updated：2019-07-22 12:40:42

1. Refund conditions

No refund for free DV SSL certificates;
No refund for SSL certificates that have been successfully issued by CAs;
Refund can be applied for SSL certificates in a terminated verification process after successful payment.

2. Refund method

Submit a ticket offline to apply for refund, and Tencent Cloud engineers will help you complete the refund process.

Symantec SSL Certificates Clarification Announcement

Last updated：2019-10-31 17:12:59

"Google No Longer Trusts Symantec Certificates" recently spreading on the Internet is not a true story. We hereby clarify that:

1. Symantec PKI system for issuing SSL Certificates will undergo a security upgrade. In order to urge Symantec to update, Google plans to distrust **certificates issued by non-updated Symantec PKI system** instead of all Symantec SSL certificates since October 23, 2018 when Chrome70 will be released. The fake news above is a serious misinterpretation.
2. Symantec plans to enable the new PKI system on December 1, 2017. SSL certificates that are issued prior to December 1, 2017 by the non-updated PKI system and will expire after October 23, 2018 will be reissued to users for free. Therefore, Symantec's PKI system update is absolutely safe and will not affect users.
3. “Symantec is selling the CA certificate business” is also a rumor without any official response.

There will be a detailed official clarification from Symantec soon. Please feel free to purchase Symantec SSL Certificates and not get misled by fake news.

August 2, 2017

Browser Compatibility Test Report

Last updated：2019-07-22 12:41:03

Certificates sold on Tencent Cloud official website are compatible with the mainstream browser versions. Here is the detailed compatibility test report:

Browser	Symantec EV	Geotrust EV	Symantec OV	Geotrust OV	TrustAsia G5 DV	Geotrust DV
IE6 (SHA2 patched)	Supported	Supported	Supported	Supported	Supported	Supported
IE (8+)	Supported	Supported	Supported	Supported	Supported	Supported
QQ browser (9.5.1/9.5.2)	CT error	CT error	CT error	CT error	CT error	CT error
QQ browser (7+)	Supported	Supported	Supported	Supported	Supported	Supported
Baidu browser (6+)	Supported	Supported	Supported	Supported	Supported	Supported
Maxthon browser (4.4+)	Supported	Supported	Supported	Supported	Supported	Supported
360 browser (8.1)	Supported	Supported	Supported	Supported	Supported	Supported
360 browser (6+)	Supported	Supported	Supported	Supported	Supported	Supported
UC browser (5+)	Supported	Supported	Supported	Supported	Supported	Supported
Sogou browser (6+)	Supported	Supported	Supported	Supported	Supported	Supported
CM browser (3+)	Supported	Supported	Supported	Supported	Supported	Supported
2345 browser (7.1+)	Supported	Supported	Supported	Supported	Supported	Supported
ChromePlus browser (2+)	Supported	Supported	Supported	Supported	Supported	Supported

Browser	Symantec EV	Geotrust EV	Symantec OV	Geotrust OV	TrustAsia G5 DV	Geotrust DV
TheWorld browser (3.6+)	Supported	Supported	Supported	Supported	Supported	Supported
Opera browser (34+)	Supported	Supported	Supported	Supported	Supported	Supported
Safari browser (5+)	Supported	Supported	Supported	Supported	Supported	Supported
Edge browser	Supported	Supported	Supported	Supported	Supported	Supported
Firefox browser (25+)	Supported	Supported	Supported	Supported	Supported	Supported
Chrome browser (53/54)	CT error	CT error	CT error	CT error	CT error	CT error
Chrome browser (46+)	Supported	Supported	Supported	Supported	Supported	Supported

CT (Certificate Transparency) is a policy of Google Chrome that monitors and verifies HTTPS certificates. Due to a kernel bug of Chrome 53/54, CT error occurs in all certificates of Symantec CA issued after June 1, 2016. Chrome handles this problem with automatic patch in first time, and fixes this problem in version 55. Users who can connect to Chrome's server will not be affected by this issue. But most users in China cannot access Chrome's server, it is recommended to upgrade to version 55+ to solve this problem. And QQ browser using kernel of Chromium 53/54 version is also affected.
Click here to check specific issues and announcements.