SSL Certificates

Product Introduction

Copyright Notice

Trademark Notice

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

Product Introduction
Overview

Last updated: 2023-09-27 21:33:18

Overview

SSL Certificates, also known as digital certificates, are provided in collaboration with Tencent Cloud and renowned digital certificate authorities (CA, Certificate Authority). Tencent Cloud platform offers a one-stop management service for the application, management, and cloud deployment of both free and paid SSL certificates. SSL certificates provide a comprehensive HTTPS solution for your websites, mobile apps, Web APIs, and other applications, including identity verification and encrypted data transmission.

Introduction to the Principles of HTTPS

The following video will further explain the principles of the SSL protocol:
Watch video

SSL and HTTPS

An encrypted HTTP protocol based on the SSL certificate for secure data transmission enables a site to be switched from Hypertext Transfer Protocol (HTTP) to Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS).
After you purchase an SSL certificate via Tencent Cloud, you can ask CA to sign and issue it through the SSL Certificate Service console. Once the certificate is issued, you can download and deploy it to the web service of your server. Alternatively, you can deploy it to your Tencent Cloud resources with one click. In this way, your web services or cloud resources can transfer data over HTTPS.

Advantages of HTTPS

Advantages	Note
Anti-hijacking, Anti-tampering, Anti-eavesdropping	HTTPS encrypts data transferred between the server and client for your websites, apps, and web APIs to prevent your data from being hijacked, tampered, or listened to.
Improving rankings in SEO	HTTPS websites are more trusted by search engines. Therefore, your websites can be collected faster and rank higher.
Increasing PV	Users trust HTTPS websites more. Therefore, they will feel

	securer to visit your websites and thus your PV can be increased.
Avoiding phishing websites	It aids users in identifying phishing websites, safeguarding the interests of both users and businesses, and bolstering user trust.

Introduction to Tencent Cloud SSL Certificates

Last updated: 2023-10-13 10:07:45

This document introduces the types of SSL certificates supported by Tencent Cloud, domain name types, brand introductions, industry selection cases, and encryption algorithms.

SSL Certificate Types

Tencent Cloud SSL Certificates supports the purchase of three types of SSL certificates: DV, OV, and EV. The security, supported certificate brands, and applicable website types vary among these different types of certificates, as detailed in the table below.

Certificate type	Applicable Website Types	Trust Level	Authentication Strength	Security	Supported Brands
DV (Domain Validation)	Personal website	Minor	The certification authority only verifies the authenticity of the website, not the enterprise information. The certificate can be issued once the domain name verification is successful.	Minor	• DNSPod (Tencent Cloud's proprietary brand) • TrustAsia • Wotrus
OV (Organization Validated)	Government organizations, enterprises, educational institutions, etc.	Strong	The CA will verify the authenticity of the website, as well as the authenticity of the enterprise information.	High	• SecureSite (same as DigiCert) • GeoTrust • GlobalSign • DNSPod (Tencent Cloud's proprietary brand) • TrustAsia

					• Wotrus
EV (Enhanced Enterprise)	Large Enterprises and Financial Institutions	Highest	The most stringent authentication standards, where the CA verifies the authenticity of the website and the veracity of the enterprise information.	Highest	• SecureSite (also known as DigiCert) • GeoTrust • GlobalSign • DNSPod (Tencent Cloud's proprietary brand) • TrustAsia • Wotrus

SSL Certificate Validity Period

The default validity period for SSL certificates is one year, and the period does not commence until the certificate is actually issued after purchase. Once the SSL certificate is successfully issued, it is considered effective and the validity period begins to be calculated (the effective date cannot be specified).

SSL Certificate Domain Types

The table below illustrates the differences between the various types of domain names that SSL certificates can be bound to.

Domain Type	Note
Single-domain	A single-domain refers to a certificate that can only protect one main domain, one sub-domain, or one public IP address.
Multi-domain	Multi-domain refers to a single certificate bound to multiple single-domain names (which need to be bound simultaneously, as domain names cannot be added after the certificate is issued).
Wildcard (Wildcard Domains)	A wildcard domain refers to a primary domain and all its subdomains at the secondary level. For instance, `*.tencent.com`; If you purchase a `*.tencent.com`, `tencent.com` is offered by default. The wildcard `*.tencent.com` can also match the next-level subdomain (such as `www.tencent.com`,

	`example.tencent.com` ...), but it does not support **cross-level subdomains**, such as `www.example.tencent.com` .

Introduction to Tencent Cloud SSL Certificate Brands

Certificate Provider	Brand Introduction
SecureSite	SecureSite, a brand under DigiCert (formerly Symantec), is the world's largest information security manufacturer and service provider, and the most authoritative digital certificate issuing authority. It provides a wide range of content and network security solutions for enterprises, individual users, and service providers. 93% of Fortune Global 500 companies have chosen VeriSign SSL digital certificates. SecureSite certificates offer advantages such as security, stability, and excellent compatibility.
GeoTrust	GeoTrust, the second-largest digital certificate issuing authority (CA) globally, is a leader in the field of identity and trust authentication. From its establishment in 2001 to 2006, it captured 25% of the global market share. VeriSign acquired GeoTrust for $125 million from May to September 2006. Currently, it is also a cost-effective brand under SecureSite's SSL certificates.
GlobalSign	Established in 1996, GlobalSign is a distinguished and trusted Certificate Authority (CA) and provider of SSL digital certificates, having issued over 20 million certificates globally. The professional prowess of GlobalSign has won the favor of numerous servers, domain registrars, and system service providers in the Chinese network market, making it their partner for digital certificate services.
DNSPod	DNSPod, a proprietary brand of Tencent Cloud, is supported by well-known domestic CA institutions for basic setup. Designed with the characteristics of the Chinese market in mind, DNSPod certificates feature domestically customized OCSP for fast access speeds.
TrustAsia	TrustAsia, a brand in the field of information security by Asiasoft Information Technology (Shanghai) Co., Ltd., professionally provides all network security services, including digital certificates, for enterprises. TrustAsia

	brand SSL certificates are issued by Sectigo root certificates.
WoTrus	WoTrus, operated by WoTrus CA Limited, is an internationally verified CA that has also obtained the electronic certification service license (issued by the MIIT) of China. It provides third-party digital identity verification for organizations and issues globally trusted digital certificates.
CFCA (Domestic)	The China Financial Certification Authority (CFCA) has passed the international WebTrust certification and is one of the members of the international CA Browser Alliance. It provides globally trusted certificates, independently developed by China's authoritative digital certificate certification authority, denoting it as a purely domestic certificate. Note: CFCA certificates currently do not support Apple iOS 10.1 and earlier versions, nor Android 6.0 and previous versions.

Brand Differences

The most significant difference between certificates of different brands lies in their root certificates:

- SecureSite is issued by SecureSite root certificates, all of which are under the DigiCert umbrella.
- GeoTrust is issued by the GeoTrust root certificate.
- GlobalSign is issued by a GlobalSign root certificate.
- DNSPod is issued by the Sectigo root certificate.
- A TrustAsia wildcard certificate is issued using a Sectigo root certificate.
- WoTrus is issued by a Sectigo root certificate.

From a technical perspective, the differences between SecureSite (formerly Verisign) and GeoTrust are as follows:

- The compatibility of SecureSite surpasses that of GeoTrust, as SecureSite is universally compatible with all browsers on the market and provides excellent support for mobile devices.
- In terms of OCSP response speed, SecureSite outperforms GeoTrust.
- In terms of CA security, SecureSite surpasses GeoTrust. SecureSite is a globally recognized security manufacturer, and its CA security level is ranked as the world's top safety factor.

- In addition to facilitating encrypted transmission, SecureSite certificates also offer additional features such as malware scanning and vulnerability assessment.
- Both SecureSite and GeoTrust offer commercial insurance compensation for their certificates. SecureSite provides a maximum compensation of 1.75 million USD, while GeoTrust offers up to 1.5 million USD.

SSL Certificates Supporting IP Address Binding

Certificate Provider	OV	OV Pro	DV	EV	EV Pro
SecureSite	**Single-domain/Multi-domain Support** Other domain types are not supported	**Single-domain/Multi-domain Support** Other domain types are not supported	Unavailable	Unavailable	Unavailable
GeoTrust	**Single-domain/Multi-domain Support** Other domain types are not supported	–	–	Unavailable	–
TrustAsia	**Single-domain/Multi-domain Support** Other domain types are not supported	–	Unavailable	Unavailable	–
GlobalSign	**Single-domain/Multi-domain Support**	–	–	Unavailable	–

	Other domain types are not supported				
Wotrus	Unavailable	–	Unavailable	Unavailable	–
DNSPod (SM)	**Single-domain/Multi-domain Support** Other domain types are not supported	–	–	**Single-domain/Multi-domain Support** Other domain types are not supported	–
DNSPod (International)	**Single-domain/Multi-domain Support** Other domain types are not supported	–	**Single-domain/Multi-domain Support** Other domain types are not supported	Unavailable	–
CFCA	**Support for Single/Multiple Domains** Other domain types are not supported.	–	–	Unavailable	–

SSL Certificate Industry Cases

The table below provides examples of certificate selection for certain industries, serving as a reference for your certificate selection:

Industry Classification	Recommended	Case Type	Industry Requirement

	Certificate Type		
Finance and Banking	EV certificate	Bank of China	• Enterprise identity information must be displayed in the website address bar. • Data transmission must be highly secure.
Education, government, and internet	OV wildcard certificate	• Ministry of Foreign Affairs of the People's Republic of China • Jingdong • Tencent News • Shanghai Gold Exchange • State Grid Corporation of China • Yonyou Network Technology Co. Ltd. • Langchao • Tencent Cloud	• New sites will be added in the later stage of the website project. • The government or company name does not need to be displayed in the website address bar.
Individual Business	DV certificate	Personal Blogs and the like	• No data transmission. • Websites that purely display information or content

Supported Encryption Algorithms for SSL Certificates

Certificate	Certificate	Certificate	Encryption Algorithms			Signature Algorithms	
			RSA	ECC	SM	RSA	ECDSA

standard	type	Provider	2048	4096	prime256v1	secp384r1	sm2withSM4	SHA256	SHA384	SHA256	SHA384
International Standard	Free certificate (DV)	TrustAsia	This feature is supported.	Unavailable	This feature is supported.	Unavailable	Unavailable	Unavailable	This feature is supported.	This feature is supported.	This feature is supported.
	OV	SecureSite	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.
		Geotrust	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.

		TrustAsia	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	Unavailable	This feature is supported.	This feature is supported.	This feature is supported.
		GlobalSign	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.
		Wotrus	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	This feature is supported.	Unavailable	Unavailable	Unavailable
		CFCA	This feature is	Unavailable	Unavailable	Unavailable	Unavailable	This feature is sup	Unavailable	Unavailable	Unavailable

		supported.					ported.			
OV Pro	SecureSite	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.
DV	TrustAsia	This feature is supported.	Unavailable	This feature is supported.	Unavailable	Unavailable	Unavailable	This feature is supported.	This feature is supported.	This feature is supported.
	Wotrus	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	This feature is supported.	Unavailable	Unavailble	Unavailable
EV	Se	Th	Thi	Th	Un	Un	Thi	Un	Th	Th

		cureSite	is feature is supported.	s feature is supported.	is feature is supported.	available	available	s feature is supported.	available	is feature is supported.	is feature is supported.
		Geotrust	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.
		TrustAsia	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	Unavailable	This feature is supported.	This feature is supported.	This feature is supported.
		GlobalSign	This feature is su	This feature is supported.	This feature is su	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is su	This feature is su

			pported.	ted.	pported.					pported.	pported.
	EV Pro	SecureSite	This feature is supported.	This feature is supported.	This feature is supported.	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.
Chinese SM Standard	OV	DNSPod	Unavailable	Unavailable	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.	This feature is supported.
	DV		Unavailable	Unavailable	Unavailable	Unavailable	This feature is supported.	Unavailable	This feature is supported.	This feature is supported.	This feature is supported.
	EV		Una	Unava	Una	Unava	This	Unava	This	This	This

			va ila bl e	ilab le	va ila bl e	ilab le	fea tur e is sup por ted .	ilab le	feat ure is sup por ted.	fe at ur e is su pp or te d.	fe at ur e is su pp ort ed .

Strengths

Last updated: 2023-09-27 21:41:18

Supports international certificates from major renowned brands

Tencent Cloud SSL Certificates are issued by top international Certificate Authorities (CAs), ensuring security. A Certificate Authority (CA) is a network organization responsible for managing and issuing security credentials and encryption security keys, and for verifying the legality of public keys in the public key system. It is crucial for a CA to verify the authenticity of users and businesses, and its authority and impartiality are of utmost importance. Tencent Cloud only collaborates with top-tier, authoritative CAs to provide secure SSL certificates. Currently, certificates from DigiCert, GeoTrust, GlobalSign, TrustAsia, and Wotrus can be purchased through Tencent Cloud.

Supports Chinese Cryptography Standard (SM2) certificates

Tencent Cloud's proprietary DNSPod brand SSL certificates support the SM2 Chinese Cryptography Standard, meeting the domestic transformation and cryptography standard compliance requirements of government agencies, public institutions, large state-owned enterprises, and financial banks.

Support for multi-year SSL certificates

SSL certificate processes are simplified and automated in the entire lifecycle covering application, validation, review, issue, and renewal.

Comprehensive automated management features for SSL certificates

The automated management features provided by Tencent Cloud SSL Certificates are as follows:

Service name	Service description
Quick deployment to cloud services	SSL certificates can be swiftly deployed to Tencent Cloud services such as Cloud Load Balancer, CDN, Cloud Live, COS, and Anti-DDoS among 12 other cloud services, with support for batch deployment.
Certificate auto-	Assists in alleviating the hassle of manually renewing SSL certificates annually.

renewal service	
Certificate Hosting Service	Upon enabling the certificate hosting service, you will not need to manually redeploy the new certificate to the services on the cloud resources after the old certificate is renewed. This means the new SSL certificate will be automatically deployed to the Tencent Cloud resources where the original SSL certificate was deployed, such as Load Balancer, CDN, Cloud Live, DDOS, etc. **This helps you reduce operational costs incurred due to repeated deployments caused by certificate validity periods.**
Extended service	Supports the application and management of certificates via API calls, freeing you from the constraints of solely using the certificate console for application and management.

Tencent Cloud SSL Certificate Browser Compatibility Test Report

Last updated: 2023-09-27 14:47:56

Note:

- CT (Certificate Transparency) provides a policy for Google browsers to monitor and audit HTTPS certificates, hence the term 'CT error' is often used to describe certificate incompatibility.
- Different certificate brands have varying levels of compatibility. The test report is as follows (this report is for reference only).

Browser Version	International Standard						Chinese SM Standard	
	SecureSite	Geotrust	TrustAsia	GlobalSign	DNSPod	Wotrus	DNSPod SM	WoTrus SM2
IE6 (with the SHA-2 patch)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
IE (8+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
QQ (9.5.1/9.5.2)	CT Error	CT Error	CT Error	CT Error	CT Error	This feature is supp	CT Error	CT Error

						orted.		
QQ (7+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Baidu (6+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Maxthon (4.4+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
360 (8.1)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
360 (6+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is sup	This feature is supported.	CT Error	CT Error

					ported.			
UC (5+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Sogou (6+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Liebao (3+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
2345 (7.1+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
CoolNovo (2+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is sup	This feature is supported.	CT Error	CT Error

					ported.			
TheWorld (3.6+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Opera (34+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Safari (5+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Edge	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
Firefox (25+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is sup	This feature is supported.	CT Error	CT Error

					ported.			
Chrome (53/54)	CT Error	CT Error	CT Error	CT Error	CT Error	This feature is supported.	CT Error	CT Error
Chrome (46+)	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	CT Error	CT Error
MeSign	CT Error	CT Error	CT Error	CT Error	CT Error	CT Error	This feature is supported.	This feature is supported.
360 Chinese SM	CT Error	CT Error	CT Error	CT Error	CT Error	CT Error	This feature is supported.	This feature is supported.
Honglianhua (Haitai)	CT Error	CT Error	CT Error	CT Error	CT Error	CT Error	This feature is supported.	This feature is supported.

Note:

Due to a bug in the Chrome (53/54) version kernel, all certificates from the SecureSite CA organization issued after June 1, 2016, will be affected by this issue, resulting in CT errors. Chrome addressed this issue promptly through an automatic patch and fixed it in version 55. Users who can connect to Chrome's servers will not be affected by this issue. However, as most users in China cannot access Chrome's servers, it is recommended to upgrade to version 55 or later to resolve this issue. The QQ browser, which uses the Chromium (53/54) version kernel, is also affected.

Multi-Year SSL Certificate and Automatic Review Overview

Last updated: 2023-09-27 21:44:54

Multi-year certificate

- A multi-year certificate is a type of certificate that users can purchase for several years in one go. As the expiration of the certificate approaches each year, Tencent Cloud automatically submits the certificate information to the CA institution for review, eliminating the need for users to initiate the application themselves.
- SSL certificate processes are simplified and automated in the entire lifecycle covering application, validation, review, issue, and renewal.
- Upon purchasing a multi-year certificate for more than one year from Tencent Cloud and completing the review, Tencent Cloud will automatically apply for a second SSL certificate for you **within 30 natural days before the expiration of the previous SSL certificate**. If your organization and domain name review are valid, the second certificate will be issued without the need for you to reapply.

Note

- Upon successful automatic review of the certificate, a new certificate will be issued. You are required to replace the existing certificate with the new one. For information on certificate installation, please refer to the relevant certificate installation documentation.
- "-" indicates certificates not available for now.

Available multi-year international standard certificates

Certificate Provider	Organization validated (OV)	OV Pro	Domain-validated (DV)	Free DV	EV	EV Pro
Secure Site	This feature is supported.	This feature is supported.	-	Unavailable	This feature is supported.	This feature is supported.
GeoTr	This	-	-	-	This	-

ust	feature is supported.				feature is supported.	
TrustAsia	Unavailable	-	Unavailable	-	Unavailable	-
GlobalSign	Unavailable	-	-	-	Unavailable	-
Wotrus	Unavailable	-	Unavailable	-	Unavailable	-

Automatic information submission for review

The automatic submission feature provided by Tencent Cloud SSL Certificate Service allows you to pre-fill application information such as company details and domain names in the SSL Certificate Service Console > **My Information**, and complete domain validation and company information review. When you apply for an SSL certificate, Tencent Cloud will help you automatically complete the domain validation for specific brand SSL certificates and submit them for review, achieving simplified management.
Automatic review will submit OV enterprise and EV enhanced certificates, CS code signing and EV_CS enhanced certificates to the root CA institution. After the review is passed, the company information review will be skipped when applying for the corresponding certificate and type on Tencent Cloud (if the review is not passed, a specialist will actively contact the reserved contact method for the certificate).

International standard certificates for which automatic information submission for review is supported

The following table lists international standard certificates for which automatic information submission for review is supported.

> **Note**
> When applying for a domestic encryption certificate or an international standard certificate that does not support automatic submission for review, domain validation and automatic submission for review cannot be skipped. However, you can quickly fill in the information using the existing organization information in **My Profile**.

Certificate Provider	Organization validated (OV)	OV Pro	Domain-validated (DV)	Free DV	EV	EV Pro

Secure Site	This feature is supported.	This feature is supported.	–	Unavailable	This feature is supported.	This feature is supported.
GeoTrust	This feature is supported.	–	–	–	This feature is supported.	–
TrustAsia	This feature is supported.	–	Unavailable	–	This feature is supported.	–
GlobalSign	Unavailable	–	–	–	Unavailable	–
Wotrus	Unavailable	–	Unavailable	–	Unavailable	–

Introduction to Tencent Cloud's National Cryptography Scheme Introduction to the Government and Enterprise SM Solution

Last updated: 2023-09-27 21:47:42

Tencent Cloud's Government and Enterprise SM product suite offers domestically encrypted services throughout the entire network transmission process. The suite includes International/SM dual certificates, SM adaptive gateway, SM browser, and SM DoH, along with a comprehensive construction and deployment plan, providing you with end-to-end application services.
Should you require related solution construction, please click on Apply Now. Upon receipt of your application, the Tencent Cloud Government and Enterprise SM Solution Team will get in touch with you.

Background Description

In the Global Trust Root Certification Program published by Microsoft in the CA/B Forum, "Trade Sanctions" were listed for the first time as one of the evaluation criteria for Microsoft's Global Trust Root Certification Program.
As early as 1999, the State Council issued the "Commercial Cryptography Management Regulations". Up to now, the state has successively issued several regulations to standardize and guide the domestication of data security in relevant fields. The most critical message conveyed is: the security of critical information infrastructure must be guaranteed by applying cryptographic technology.

The Cybersecurity Multi-Level Protection Scheme 2.0 explicitly stipulates that the entire process of message or session in network communication must be encrypted (Level 3), one of the cryptographic technology standards is the SM2 algorithm.
Based on national policies and requirements, DNSPod has launched Tencent Cloud's Government and Enterprise SM product, using the SM (SM2) certificate and related ecosystem construction, to address the compliance needs of government and enterprise customers during network transmission.

Solution Description

Tencent Cloud's Government and Enterprise SM product suite comprises three main modules: International + SM dual SSL certificates, SM algorithm browser, and SM adaptive gateway. Through the combination of these three, the SM link in the complete network transmission is achieved.

Users request to visit sites through different browsers. The SM security gateway will make a judgment: if the system adaptively recognizes that the browser supports the SM algorithm, it can use the SM standard HTTPS for access and transmission. If a regular browser is used, the international algorithm certificate supported by the regular browser is used for HTTPS access and transmission.
Even if the international standard certificate is no longer supported, it can quickly switch to the SM standard, ensuring the continuity and stability of the business.

Solution Features

Target Customers

- Government Agency Units.
- Educational institutions such as universities.
- Telecommunication networks and other units providing public information network services.
- Broadcasting stations, news agencies, and other news organizations.
- Public service units such as healthcare, finance, and transportation.
- Other major governments and enterprises that need to undertake domestic cryptographic construction and meet compliance requirements.

Chinese SM (SM2) Certificate

Proprietary Brand
Tencent Cloud is a proprietary brand that complies with national standards, possesses full intellectual property rights, meets monitoring requirements, is immune to certificate supply disruption risks, and guarantees service and after-sales support.
Superior Performance

- According to a foreign research report on the performance of the ECC encryption algorithm: By adopting the ECC algorithm, the response time of a Web server is more than ten times faster than that of RSA.
- Simultaneously, the encryption strength of SM2 is significantly superior to that of RSA 3072.

SM Browser

SM Browser

- Supports both SM and International dual certificates.
- Supports access via both Chinese SM (SM2) and international standard SSL certificates.

Excellent Compatibility

- Complies with GB/T 38636-2020 (GM/T 0024-2014) standards (TLCP).
- Versions for both Windows and Mac systems are provided.

Deep Customization

- Tencent Cloud's SM browser supports enterprise-level deep customization solutions, allowing for in-depth customization of various browser configurations based on different user needs.

SM Gateway

Cloud Load Balancer

Deeply optimizes web applications, supports IP session persistence, application session persistence, deep health checks, URL redirection, and dual hot standby.

Web Acceleration

Supports acceleration technologies such as dynamic compression, object storage, and connection reuse, along with threshold limit and alert capabilities. It also supports user certificate passthrough and intelligent page preloading.

SSL Acceleration

Supports RSA/ECC/SM2 acceleration, SSL v3.0, TLS v1.0-V1.3 protocols, SM dual certificates, SM algorithms SM1/2/3/4, and SM browser.

SM DoH

- Supports DNSPod's SM DoH Service.
- DNS over HTTPS (abbreviated as DoH) is a secure domain name resolution scheme. Its significance lies in making DNS resolution requests over the encrypted HTTPS protocol, preventing the user's DNS resolution requests in the original DNS protocol from being intercepted or modified (such as in a man-in-the-middle attack), thereby achieving the goal of protecting user privacy.

- Both the SM Gateway and the Browser DoH module support the SM2 encryption algorithm, thereby providing users with a complete domain name resolution SM link.

Release notes

Category		Enterprise Edition	Premium Edition	Premium Edition	Description
Price		400000	700000	1200000	All solutions include the delivery of SM/International Standard Certificates, SM Gateway, and SM Browser as a complete package.
					All solutions include implementation, deployment, and maintenance costs.
					Billing can be individually tailored based on the additional configurations or services utilized by the user.
Certificate	International Standard SSL Certificate (OV Wildcard)	5	10	15	Utilizes DigiCert's top-level root certificate, ensuring security and reliability.
	SM Standard SSL Certificate (OV Wildcard)	5	10	15	Tencent Cloud's proprietary brand, DNSPod Intermediate Root, ensures reliable after-sales service.
Gateway	T100 Model	✓	–	–	• Max Concurrency: 30000 • SSL Throughput: 1 Gbps • SSL Creation

					(RSA2048): 5500 • SSL Creation (SM): 3000 • Size: 2 U • Power Supply: Dual Power
	T200 Model	–	✓	–	• Max Concurrency: 50,000 • SSL Throughput: 1 Gbps • SSL Creation (RSA2048): 15000 • SSL Creation (SM): 13000 • Size: 2 U • Power Supply: Dual Power
	T500 Model	–	–	✓	• Maximum Concurrency: 100,000 • SSL Throughput: 10 Gbps • SSL Creation (RSA2048): 40000 • SSL Creation (SM): 30000 • Size: 2 U • Power Supply: Dual Power
Exclusive SM Browser	SM + International Dual Certificate Access	✓	✓	✓	Dual Certificate Access Supported
	Customization of Browser Icons	–	✓	✓	Exclusive Icon
	Custom Browser	–	✓	✓	Exclusive Name

	Naming				
	Customization of Browser Color Scheme	–	–	✓	Custom Color Scheme
	Dedicated Installation Page	–	–	✓	Custom UI Installation
	Custom Development Services	Dependent on Circumstances	Dependent on Circumstances	Dependent on Circumstances	User's Customization Requirements
Government and Enterprise SM Support Services	SM System Deployment	✓	✓	✓	One-stop deployment of the SM solution.
	SM Product Training	✓	✓	✓	Training for the use and maintenance of the SM Solution products.
	SM Technology Support	✓	✓	✓	Offers 12/7 technical support services.
	SM Product VIP Service	–	–	✓	The VIP service of the SM product will have shorter problem response and resolution times, along with dedicated one-on-one technical support.

Basic Concept of DNSPod SM2 SSL Certificate

Last updated: 2023-09-27 21:49:04

Introduction to DNSPod SM2 certificate

The Chinese cryptographic algorithm is a crucial foundation for ensuring the autonomous and controllable network security of our country. The application of "HTTPS encryption" in the field of network information security is gradually popularizing the Chinese cryptographic algorithm SM2. The SM2 algorithm, through autonomous and controllable cryptographic technology, safeguards the data security of important information flow on the Internet, which holds significant strategic importance in enhancing our country's network information security and autonomous control level. Our country has already issued numerous policies, demanding vigorous promotion of the application of Chinese cryptographic algorithms in finance and other critical fields.
The DNSPod SM2 certificate not only meets the domestic transformation and cryptographic algorithm compliance requirements of industry customers such as government agencies, public institutions, large state-owned enterprises, and financial banks. Simultaneously, through the "SM2/RSA" dual certificate service, it assists website systems to adaptively comply with all browsers, considering both cryptographic compliance and global universality.

Note

- Currently, the SM2 certificate does not support deployment on Tencent Cloud products **CLB Load Balancer, CDN Content Delivery Network, T-Sec DDoS Protection, T-Sec Web Application Firewall, and CSS Live Streaming**. For support information on other products, please consult customer service at 4009100100 or confirm by browsing the relevant product documentation.
- Currently, the SM2 certificate does not support deployment on **Tomcat servers**, **GlassFish servers**, **JBoss servers**, **Jetty servers**, **IIS servers**, and **Weblogic servers**.

SSL certification and encryption implementation of SM algorithms

The SSL handshake process of an SM certificate is as follows:

1. Exchange of Hello messages to negotiate a cipher suite, exchange of random numbers, and determination of session reuse.
2. Exchange necessary parameters to negotiate a pre-master key.
3. Exchange of certificate information for the purpose of verifying the other party.

4. Generate the master key using the pre-shared key and the exchanged random number.
5. It provides secure parameters to the record layer.
6. Verifying the consistency of the security parameters calculated by both parties, as well as the authenticity and integrity of the handshake process.

To implement the above handshake process, both the client (browser) and the server need to support the Chinese cryptographic algorithm. Although the SM2/SM3/SM9 algorithms have been successively incorporated into the international standard system, a lengthy process is still required to achieve widespread compatibility between the client and the server. During this period, technical solutions are needed to enable both the browser and the server to support the Chinese cryptographic algorithm and the Chinese cryptographic SSL certificate, thereby promoting the widespread application of the Chinese cryptographic algorithm. Therefore, to implement SSL authentication and HTTPS encryption based on the Chinese cryptographic algorithm on the server, website operators need to apply to an authoritative electronic certification authority licensed by the Ministry of Industry and Information Technology (such as DNSPod) for a Chinese cryptographic SSL certificate that complies with the Chinese cryptographic standard, and deploy the certificate on a web server that supports the Chinese cryptographic standard certificate.
When a Chinese cryptographic browser is used to access a site that has deployed a Chinese cryptographic standard certificate, the browser and the server will use the Chinese cryptographic algorithm to encrypt the transmitted data, achieving Chinese cryptographic algorithm SSL authentication and encryption.

Browser Issues with DNSPod GM (SM2) SSL Certificates

Last updated: 2023-09-27 21:49:32

Browsers Supporting DNSPod GM (SM2) Certificates

Browsers such as 360, MeSign, and Haitai support Chinese cryptographic algorithms.

Resolving Browser Compatibility Issues with DNSPod GM (SM2) Certificates

Websites using SSL certificates with Chinese cryptographic algorithms can be accessed normally on browsers that support these algorithms. However, as these algorithms are not yet widely compatible with all mainstream browsers, some browsers that only support international algorithms may report errors with Chinese cryptographic SSL certificates. You can resolve this issue by using the 'Dual Certificate Deployment' and 'Adaptive Browser Compatibility' solutions. These solutions are compatible with both browsers that support Chinese cryptographic algorithms and those that only support international algorithms. With these solutions, you can access the website normally with any browser, meet the compliance requirements for deploying Chinese cryptographic SSL certificates, and also meet the requirements for website availability, usability, and global applicability, thus overcoming the technical barriers to the application of Chinese cryptographic SSL.

> **Note**
> Tencent Cloud offers a free DV SSL certificate to users who have purchased DNSPod GM (SM2) certificates to smoothly resolve browser compatibility issues. For specific deployment methods, please refer to Installation of GM Certificates.

Browser Differences Among Different Types of DNSPod GM (SM2) Certificates

Certificate type	OV	DV	EV
Supporting wildcard domain names	This feature is supported.	This feature is supported.	Unavailable
Multi-domain	Supported (up to 100 domain names)		
Cryptographic	Adopting the Chinese cryptographic algorithm system SM2 to		

algorithms	deliver better key strength than international cryptographic standards
Browser Compatibility	Compatible with browsers supporting Chinese cryptographic algorithms, such as 360, MeSign, and Haitai

Address Bar Differences for DNSPod GM (SM2) Certificates

- DV: displays the security lock icon in browsers supporting Chinese cryptographic algorithms.
- OV: displays the security lock icon and the organization name in browsers supporting Chinese cryptographic algorithms.
- EV: displays the green address bar and the organization name in browsers supporting Chinese cryptographic algorithms.

Automated Management Solution

Last updated: 2023-09-27 21:50:03

If you are applying for a certificate for the first time, it is essential to familiarize yourself with the various brands and types of certificates. Then, based on your actual needs, apply for the certificate that best suits you. For more details, please refer to Tencent Cloud SSL Certificate Overview.
This document primarily details the process of automating certificate management.

> **Note:**
> To achieve automated certificate management, simply enable the three services: **Automatic DNS Addition, Certificate Auto-Renewal, and Certificate Hosting**, and ensure that your account has sufficient balance.

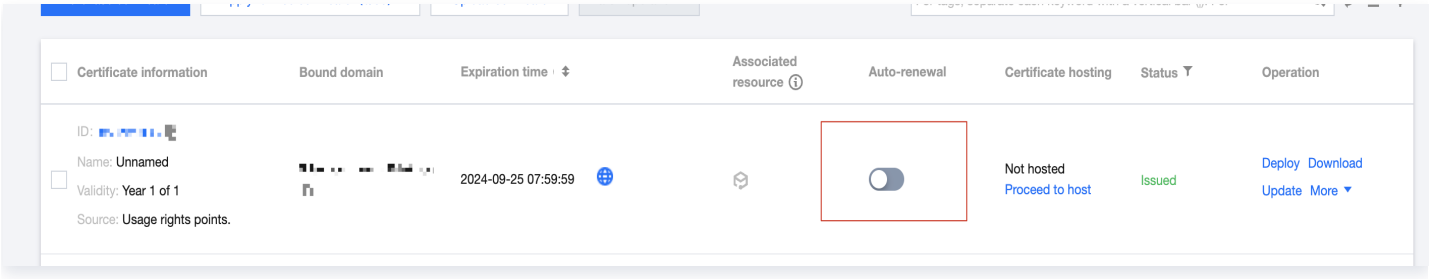
Implications of not renewing an SSL certificate on time

If an SSL certificate is not renewed after its expiration, users will encounter a warning message stating "The website's security certificate has expired" when they attempt to access the website. This could deter users from visiting the website due to security concerns. Furthermore, malicious entities could exploit expired SSL certificates to tamper with or steal information and data transmitted between the browser and the server, compromising user data security.

Enabling auto-renewal for SSL certificates

Please navigate to SSL Certificate Service Console > **My Certificates**. On the **My Certificates** page, enable auto-renewal. For more details, please refer to SSL Certificate Auto-Renewal Guide.

> **Note:**
> Auto-renewal is only available for formal certificates; free certificates do not support this feature.

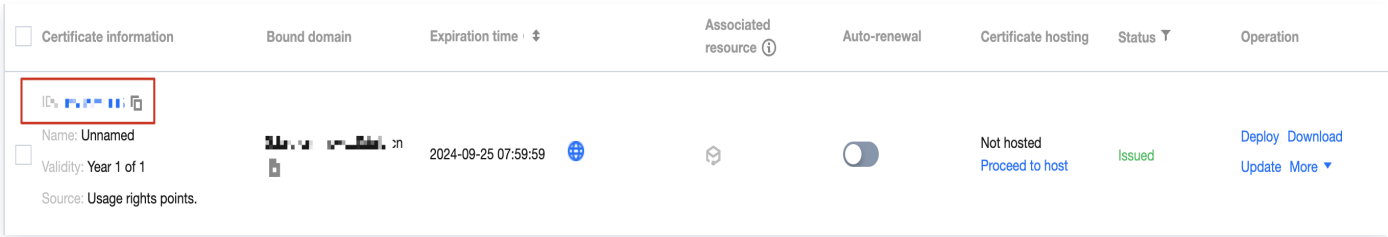


Automatic replacement of old resources after SSL certificate renewal

By enabling the certificate hosting service, you won't need to redeploy the certificate to the cloud resources after successfully renewing the SSL certificate. This service will automatically deploy the new SSL certificate to the Tencent Cloud resources where the original SSL certificate was deployed, such as Load Balancer, Content Delivery Network, etc. For more details, please refer to Cloud Resource Hosting Guide.

Note:
Upon issuance of an SSL certificate, you can initiate cloud resource hosting and bind the relevant cloud resources. When the SSL certificate is renewed, generating a new certificate, the cloud resources associated with the original certificate will automatically be bound to the new one.

1. Please navigate to the SSL Certificate Service Console, proceed to **My Certificates**, and on the **My Certificates** page, click on the **ID.**



2. On the opened page, activate the certificate hosting service as required.