SSL Certificate Service

Product Introduction

Product Documentation

Tencent Cloud

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

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

Contents

Product Introduction
Overview

Last updated：2024-03-06 16:57:28

Overview

SSL Certificates are also known as digital certificates. Tencent Cloud works with well-known Certificate Authorities (CA) to allow users to apply for, manage, and deploy free/paid SSL certificates, which enable HTTPS to identify identities and encrypt data for your websites, apps, and web APIs.

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

Advantage	Description
Anti-hijacking/tampering/listening	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	The green icon on the HTTPS address bar helps users identify phishing websites, protecting user and business interests and enhancing user trust.

Introduction to Tencent Cloud SSL Certificates

Last updated：2024-03-06 16:57:28

Certificate Issuance

DV certificates are reviewed and verified automatically by DigiCert for fast issuance.
As a world-leading digital certificate provider, DigiCert offers the best certificate services to its global customers. It has remained a reliable partner with many top businesses around the world, providing trusted SSL, private and managed PKI deployment, and device certificates for the emerging IoT market.
TrustAsia is a brand of TrustAsia Technologies, Inc. in the field of information security. It is a platinum partner of DigiCert.TrustAsia specializes in providing businesses with all network security services including the digital certificates.

Quick Application

Simplified processes: Tencent Cloud certificate service supports automatic generation of CSR online. The domain name is automatically verified by DNS, and the application is submitted in one step. The verification and issuance process is fully automatic.

Centralized Management

Multi-platform management: upload and manage certificates issued by any agency, with centralized validity monitoring of each certificate.
Private key hosting: for a certificate with CSR generated online and a private key password set, the password is used for encrypted certificate hosting to ensure information security.

Strengths

Last updated：2024-03-06 16:57:28

Top CAs

SSL certificates are issued by leading global CAs and are safe and reliable.
Certificate Authorities (CAs) are network agencies which manage and issue secure credentials and encryption information keys. The credibility and fairness of CAs are very important as they are responsible for public key validity verification in the public key system as well as user and enterprise identity verification. Therefore, Tencent Cloud only works with the most reputable CAs to provide secure SSL certificates.

Encrypted data transfer

Encryption secures the data transfer between the browsers/Apps and servers.
Encrypted App and webpage communication via HTTPS can prevent data from being stolen and tampered in the course of transmission and guarantee data integrity; prevent traffic hijacking and advertisement inserting by ISPs, and effectively resist man-in-the-middle attacks, greatly improving the security.

100% compatibility (international standard certificates)

SecureSite root certificates can be issued for all browsers and mobile devices.
Compatibility determines whether security reminders will properly pop out when users access sites via browsers. SecureSite root certificates rank top in browser compatibility, supporting all mainstream browsers and mobile devices.

Improved search ranking

HTTPS can help improve sites' search rankings and credibility.
Google adjusted the search engine algorithm in 2014, as a result, HTTPS-encrypted websites rank higher in search results than HTTP sites. Search engine vendors in Mainland China are also stepping up their focus on HTTPS to fuel SEO.

Support for multi-year SSL certificates

SSL certificate processes are simplified and automated in the entire lifecycle covering application, validation, review, issue, and renewal, relieving you of the concern that global CAs won't issue SSL certificates with a validity period greater than 13 months.

Comprehensive services

The following value-added services are supported:

Quick deployment to Tencent Cloud services: SSL certificates can be quickly deployed to Tencent Cloud services such as CLB, CDN, CSS, and Anti-DDoS.

Extended service: Certificates can be applied for and managed via APIs besides the console.

Hosting service: With Tencent Cloud resource hosting, a new SSL certificate can be automatically deployed to the same Tencent Cloud resources such as CLB, CDN, CSS, and Anti-DDoS as the original certificate after renewal and issue. This reduces Ops costs caused by repeated deployment due to the validity period of the certificate.

Fast refund

If you have paid for an SSL certificate order, but the application failed, the approval process was suspended, and the SSL certificate was not issued, you can request a refund at any time by performing a few simple operations in the console.

Advantages of HTTPS

Last updated：2024-03-06 16:57:28

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).

Preventing traffic hijacking

Applying HTTPS to the whole website is a solution for eliminating ISPs or intermediary induced traffic hijackings. This solution prevents small ads from being displayed in web pages and protects user privacy.

Improving website search ranking

HTTPS can help improve your website’s search ranking, credibility, and brand image.

Avoiding phishing websites

The green icon on the HTTPS address bar helps users identify phishing websites, protecting user and business interests and enhancing user trust.

Browser Compatibility Test Report

Last updated：2024-03-06 16:57:28

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

Browser	SecureSite EV	GeoTrust EV	WoTrus EV	SecureSite OV	GeoTrust OV	WoTrus OV	TrustA G5 DV
IE6 (with the SHA-2 patch)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
IE (8+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
QQ (9.5.1/9.5.2)	CT error	CT error	Supported	CT error	CT error	Supported	CT err
QQ (7+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
Baidu (6+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
Maxthon (4.4+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
360 (8.1)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
360 (6+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
UC (5+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
Sogou (6+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
Liebao (3+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
2345 (7.1+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
CoolNovo (2+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
TheWorld (3.6+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
Opera (34+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo
Safari (5+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppo

Edge	Supported	Supported	Supported	Supported	Supported	Supported	Suppor
Firefox (25+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppor
Chrome (53/54)	CT error	CT error	Supported	CT error	CT error	Supported	CT erro
Chrome (46+)	Supported	Supported	Supported	Supported	Supported	Supported	Suppor
MeSign	CT error	CT error	CT error	CT error	CT error	CT error	CT erro
360 Chinese SM	CT error	CT error	CT error	CT error	CT error	CT error	CT erro
Honglianhua (Haitai)	CT error	CT error	CT error	CT error	CT error	CT error	CT erro

Note:

Certificate Transparency (CT) is a policy for Google Chrome to monitor and review HTTPS certificates. Due to a kernel bug in Chrome 53/54, CT error occurs in all certificates of SecureSite CA issued after June 1, 2016. Chrome handled this problem with automatic patch immediately and fixed this issue in version 55. This issue doesn't affect users who can connect to Chrome's server. Since most users in the Chinese mainland cannot access Chrome's server, we recommend that you upgrade to version 55+ to solve this issue. In addition, QQ Browser using the kernel of Chromium 53/54 version is also affected.

Multi-Year SSL Certificate and Automatic Review Overview

Last updated：2024-03-06 16:57:28

Multi-year certificate

A multi-year certificate is a purchasable certificate valid for years. When such certificate is about to expire, Tencent Cloud will automatically submit the certificate information to the CA for review, so that you don't need to initiate an application.

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

After you purchase an SSL certificate valid for more than one year from Tencent Cloud and the certificate information is reviewed, Tencent Cloud will automatically apply for a second one for you **within 30 calendar days before its expiration**. If the approval for your organization and domain remains valid, the second certificate will be issued without reapplication.

Note:

A new certificate will be issued upon approval after automatic review, and you need to replace the existing one with the new one.

"-" indicates certificates not available for now.

Available multi-year international standard certificates

Certificate Brand	OV	OV Pro	DV	Free DV	EV	EV Pro
SecureSite	Supported	Supported	-	Not supported	Supported	Supported
GeoTrust	Supported	-	-	-	Supported	-
TrustAsia	Not supported	-	Not supported	-	Not supported	-
GlobalSign	Not supported	-	-	-	Not supported	-
WoTrus	Not supported	-	Not supported	-	Not supported	-

Automatic information submission for review

SSL Certificate Service provides the automatic information submission feature; that is, you can enter the application information such as organization information and domain and complete domain validation and organization information review in advance on the **My Profile** page in the SSL Certificate Service console, so that when you apply for an SSL certificate, Tencent Cloud will automatically complete the domain validation for the SSL certificate of a certain brand and submit the certificate for review, simplifying management.

During automatic review, the system will submit OV and EV SSL certificates as well as CS and EV_CS code signing certificates to the root CA. After approval, organization information review will be skipped when you apply for the corresponding certificate and type (otherwise, someone will get in touch via the contact information reserved 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:

For Chinese SM certificates or international standard certificates for which automatic information submission for review is not supported, domain validation and automatic information submission for review cannot be skipped, but you can quickly enter the existing organization information on the **My Profile** page.

Certificate Brand	OV	OV Pro	DV	Free DV	EV	EV Pro
SecureSite	Supported	Supported	-	Not supported	Supported	Supported
GeoTrust	Supported	-	-	-	Supported	-
TrustAsia	Supported	-	Not supported	-	Supported	-
GlobalSign	Not supported	-	-	-	Not supported	-
WoTrus	Not supported	-	Not supported	-	Not supported	-

SSL Certificate Security

SSL Certificate Data Security

Last updated：2024-03-06 16:57:28

Uploading certificates

When you upload SSL certificates in the SSL Certificates Service console, HTTPS is used for communication throughout the process, and the OV SSL certificates issued by SecureSite are used for encryption to ensure data communication security.

Hosting certificates

The certificates uploaded are stored in Tencent Cloud’s databases and are encrypted using the Advanced Encryption Standard and Cipher Block Chaining. The key is 128 bits long, which would take 210.4 billion years to break even using the most powerful computer we have currently.

To improve the availability and security of certificate data, Tencent Cloud has deployed three certificate databases across two regions, including a primary database, a hot backup database, and a cold backup database. They use private networks, have no externally exposed APIs, and are protected by Secure Tencent Gateway (STGW).

There are 6 backend servers for SSL certificates, which are accessed via a load balancer to ensure API stability.

Accessing and reading certificates

Accessing

SSL Certificate Service has integrated resource-level CAM. It’s backed by a well-established access management system that allows you to grant different access to different certificates on a per sub-account basis to prevent malicious revocation, deletion, etc.

Reading

Certificate reading by other Tencent Cloud services (e.g., Anti-DDoS):

SSL Certificate Service is interconnected with Tencent Cloud services including CLB, CDN, WAF, Anti-DDOS, CSS, etc., which can read SSL certificates via private APIs when necessary.

The certificate reading process is also protected by STGW. Other Tencent Cloud services are supposed to read the certificates only when necessary. Requests are validated and authenticated to prevent unauthorized and unnecessary access.