SSL Certificate Service

Product Introduction

Product Documentation

Contents

Product Introduction
Overview

Last updated : 2021-05-07 17:23:51

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.

Advantage	Description
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.

Supported Certificate Types and Brands

Tencent Cloud supports the following encryption standards of certificates:

Encryption Standard	Certificate Type	Certificate Brand
International standard	DV, OV, EV, OV Pro, EV Pro	SecureSite, GeoTrust, TrustAsia, GlobalSign, Wotrus
Chinese cryptographic standard	DV, OV, EV	DNSPod

Certificate Type Description

The following table describes the trust levels and use cases of the three certificate types:

SSL Certificate Type	Trust Level	Use Case
DV	Average	For general websites. The certificate can be issued if the website authenticity is verified.
OV	High	For organization websites. The certificate can only be issued if the organization is verified, making it more restrictive and secure.
EV	Highest	Usually for banks, securities companies, and other financial institutions. It requires rigorous auditing to ensure the highest security. The address bar turns green after the EV SSL certificate is deployed.

References

When purchasing a certificate, you can refer to the following documents:

- Certificate Type Selection Cases
- Certificate Brands

Strengths

Last updated : 2020-05-09 14:06:55

Top CAs

Issued by top international CAs, SSL certificates are safe and secure.
Certificate authorities (CAs) are network agencies that manage and issue secure credentials and encryption information keys. They are responsible for verifying the validity of public keys in the public key system and the identities of users and enterprises. Because the authority and fairness of CAs are crucial, Tencent Cloud only collaborates with top authoritative CAs to provide safe and 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 insertion by ISPs, and effectively resist man-in-the-middle attacks, greatly improving the security.

100% Compatible

DigiCert root certificate supports all browsers and mobile devices.
Compatibility determines whether web page security will properly prompts when users access sites via browsers. Supporting all current major browsers and mobile devices, DigiCert root certificates rank top in browser compatibility.

Improving Search Rankings

HTTPS can help improve search rankings and sites credibility.
Google adjusted the search engine algorithm in 2014. According to the platform, "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 optimization.

Advantages of HTTPS

Last updated : 2020-09-03 11:10:26

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.

Features

Last updated : 2020-05-11 10:30:23

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.

SSL Certificate Brands

Last updated : 2021-06-30 10:55:40

Certificate Brands and Models

Tencent Cloud provides the following brands of SSL certificates for sale:

Certificate Brand	Description
SecureSite	• SecureSite is the world's largest information security service provider and most reputable digital certificate issuer. It provides a wide spectrum of content and network security solutions to individuals, businesses, and service providers. • 93% of Fortune Global 500 companies choose VeriSign SSL digital certificates. SecureSite acquired VeriSign in August 2010, changed VeriSign's product name and brand logo in April 2012, and since then has been providing the VeriSign verification service.
GeoTrust	• GeoTrust, the world's second-largest digital certificate authority (CA) and a leader in identity verification 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 to implement a wide range of identity verifications. • GeoTrust was founded in 2001, and by 2006, it accounted for 25% of the global market. VeriSign acquired GeoTrust for 125 million USD in May-September 2006, and is now another cost-effective SSL certificate brand under SecureSite.
TrustAsia	• TrustAsia, a brand under Yashu Information Technology (Shanghai) Co., Ltd in the field of information security, is a SecureSite platinum partner. TrustAsia specializes in providing businesses with complete network security services including digital certificates. • TrustAsia SSL certificates are issued using Digicert root certificates.
GlobalSign	• Founded in 1996, GlobalSign is a reputable and trusted CA and provider of SSL certificates with more than 20 million SSL certificates issued worldwide. • A great number of server providers, domain name registrars, and system service providers in the Chinese market prefer GlobalSign and partner with it for digital certification services.
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.

DNSPod GM (SM2)	Tencent's DNSPod adopts the GM standard and is completely China-developed. Supported by well-reputed CAs in China, it is highly convenient and efficient, and meets the regulatory requirements of China.

Brand Differences

The certificates of different brands vary depending on the browser address bar, encryption level, and the level guaranteed compensation. The most important difference lies in their root certificates. For example, a GeoTrust wildcard certificate is issued using a GeoTrust root certificate, while a SecureSite wildcard certificate is issued using a SecureSite root certificate. Digicert root certificates are compatible with all browsers on the market and also best supports mobile devices. A TrustAsia wildcard certificate is also issued using a Digicert root certificate. A GlobalSign wildcard certificate is issued using a GlobalSign root certificate. A DNSPod certificate is issued using a Wotrus root certificate, and a Wotrus wildcard certificate is issued using a Sectigo root certificate.

From a technical point of view, the differences between SecureSite (formerly VeriSign) and GeoTrust are as follows:

- Compatibility: SecureSite outperforms GeoTrust. SecureSite is compatible with all browsers on the market as well as many mobile devices.
- OCSP response speed: SecureSite outperforms GeoTrust.
- CA security: SecureSite outperforms GeoTrust. As an internationally renowned security vendor, SecureSite provides the best CA security in the world.
- Data security: in addition to encrypted data transmission, SecureSite certificates provide malware scanning and vulnerability assessment features.
- Certificate commercial insurance compensation: SecureSite (up to 1.75 million USD) outperforms GeoTrust (up to 1.5 million USD).

Certificate Type Selection Cases

Last updated : 2020-09-01 09:58:06

This topic lists certificate type selection cases for certain industries to help you determine which certificate type for which to apply or purchase.

Industry	Recommended Certificate Type	Case	Industry Requirement
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 • JD.com • 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 blog	• No data transmission. • The website displays pure information or content.

SSL Certificate Data Security

Last updated : 2021-07-19 14:32:01

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.

Browser Compatibility Test Report

Last updated : 2020-12-16 12:21:46

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	SecureSite 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 (9.5.1/9.5.2)	CT error	CT error	CT error	CT error	CT error	CT error
QQ (7+)	Supported	Supported	Supported	Supported	Supported	Supported
Baidu (6+)	Supported	Supported	Supported	Supported	Supported	Supported
Maxthon (4.4+)	Supported	Supported	Supported	Supported	Supported	Supported
360 (8.1)	Supported	Supported	Supported	Supported	Supported	Supported
360 (6+)	Supported	Supported	Supported	Supported	Supported	Supported
UC (5+)	Supported	Supported	Supported	Supported	Supported	Supported
Sogou (6+)	Supported	Supported	Supported	Supported	Supported	Supported
CM (3+)	Supported	Supported	Supported	Supported	Supported	Supported
2345 (7.1+)	Supported	Supported	Supported	Supported	Supported	Supported
ChromePlus (2+)	Supported	Supported	Supported	Supported	Supported	Supported
TheWorld (3.6+)	Supported	Supported	Supported	Supported	Supported	Supported
Opera (34+)	Supported	Supported	Supported	Supported	Supported	Supported
Safari (5+)	Supported	Supported	Supported	Supported	Supported	Supported

Edge	Supported	Supported	Supported	Supported	Supported	Supported
Firefox (25+)	Supported	Supported	Supported	Supported	Supported	Supported
Chrome (53/54)	CT error	CT error	CT error	CT error	CT error	CT error
Chrome (46+)	Supported	Supported	Supported	Supported	Supported	Supported

Certificate Transparency (CT) is a policy for Google Chrome to monitor and verify 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 problem in version 55. This issue doesn’t affect users who can connect to Chrome's server. Since 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.