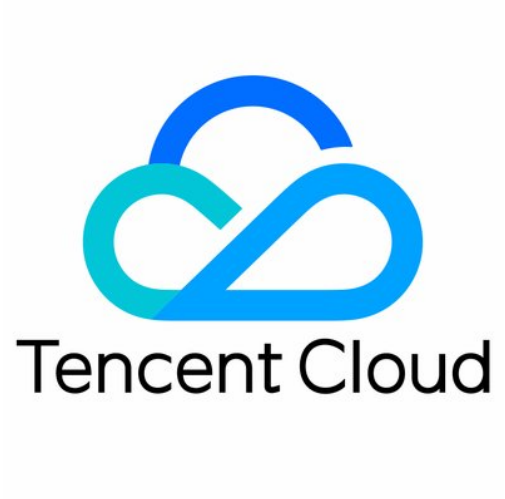
SSL Certificate Service

Glossary

Product Documentation



Glossary

Last updated：2020-09-25 11:19:49

SSL certificate

Secure Sockets Layer (SSL) is a security protocol designed to ensure the security and data integrity of internet communication. Based on the SSL protocol, an SSL certificate can be installed on a server to achieve encrypted data transmission.
A certificate authority (CA) is a third-party authority that verifies the validity of public keys. It is responsible for specifying policies and procedures to verify users' identities, signing SSL certificates, as well as validating the identities of certificate holders and the ownership of public keys. The CA issues an SSL certificate to each user using the public key. An SSL certificate is used to certify that the individuals/businesses listed in the certificate lawfully own the public key listed in the certificate. Digital signatures from a CA can prevent certificates from being forged and tampered with.
An SSL certificate actually represents CA’s verification of the public key, and contains digital signing authority information, the public key user information, the public key, the authority signature, and an expiration date.

CA

See certificate authority.

Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol Secure (HTTPS), also known as HTTP over TLS, HTTP over SSL, or HTTP Secure, is a secure network transfer protocol. On a computer network, HTTPS implements communication through the HTTP protocol but uses SSL/TLS to encrypt packets.

CSR

See certificate signing request.

HTTPS

See Hypertext Transfer Protocol Secure in Glossary.

Certificate authority

A certificate authority (CA) issues and manages digital certificates, and is responsible for verifying the validity of public keys in the public key system as a trusted third party in e-commerce transactions.

Private key

SSL certificates are developed based on public-key cryptography, which encrypts information with digital keys so that the information can only be read by the intended recipients after decryption.

A key pair consists of a public key and a private key. The public key may be publicly distributed by a user, while the private key is kept by the user. Information encrypted with the public key can be decrypted only with the corresponding private key, and vice versa.
An SSL certificate actually represents CA's verification of the public key, and contains digital signing authority information, the public key user information, the public key, authority signature, and an expiration date.

Certificate signing request

To obtain an SSL certificate, you need to generate a certificate signing request (CSR) file and submit it to a CA. A CSR includes a public key and a distinguished name. A CSR is usually generated by a web server, and a public and private key pair for encryption and decryption is created simultaneously.