

# SSL 证书

## 词汇表

## 产品文档



腾讯云

---

**【版权声明】**

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

# 词汇表

最近更新时间：2024-03-06 17:57:49

## 安全套接层数字证书

安全套接层（Secure Sockets Layer, SSL）是一种安全协议，目的是为互联网通信，提供安全及数据完整性保障。SSL 证书遵循 SSL 协议，可安装在服务器上，实现数据传输加密。

数字证书认证（Certificate Authority, CA）机构，是承担公钥合法性检验的第三方权威机构，负责指定政策、步骤来验证用户的身份，并对 SSL 证书进行签名，确保证书持有者的身份和公钥的所有权。CA 机构为每个使用公开密钥的用户发放一个 SSL 证书，SSL 证书的作用是证明证书中列出的个人/企业合法拥有证书中列出的公开密钥。CA 机构的数字签名使得攻击者不能伪造和篡改证书。

安全套接层数字证书（SSL Certificate, SSL 证书）实际上就是 CA 机构对用户公钥的认证，内容包括电子签证机关的信息、公钥用户信息、公钥、权威机构的签字和有效期等。

## CA

参见 [数字证书认证机构](#)

## 超文本传输安全协议

超文本传输安全协议（Hypertext Transfer Protocol Secure, HTTPS）也被称为 HTTP over TLS、HTTP over SSL 或 HTTP Secure，是一种网络安全传输协议。在计算机网络上，HTTPS 经由超文本传输协议进行通信，但利用 SSL/TLS 来对数据包进行加密。

## CSR

参见 [证书签名申请](#)

## HTTPS

参见 [超文本传输安全协议](#)

## 数字证书认证机构

数字证书认证机构（Certificate Authority, CA）是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

## 私钥

SSL 证书是基于公钥加密（public-key cryptography）开发，公钥加密使用数字密钥对信息进行加密编码，从而使信息只能被目标收件人读取，然后收件人对信息进行解密读取。

一个密钥对包含一个公钥和私钥，用户对公钥进行公开分发，私钥由用户保管，公钥加密的内容只有对应私钥可以解密，私钥加密的内容只有对应公钥可以解密。

---

SSL 证书实际上就是 CA 机构对用户公钥的认证，内容包括电子签证机关的信息、公钥用户信息、公钥、权威机构的签字和有效期等。

### 证书签名申请

CSR 即证书签名申请（Certificate Signing Request）。获取 SSL 证书，需要先生成 CSR 文件并提交给证书颁发机构（CA）。CSR 包含了公钥和标识名称（Distinguished Name），通常从 Web 服务器生成 CSR，同时创建加解密的公钥私钥对。