

腾讯云SSL证书

常见问题

产品文档



腾讯云

【版权声明】

©2013-2017 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模式的承诺或保证。

文档目录

文档声明.....	2
常见问题.....	4
证书是否支持吊销？	4
安全审核失败的原因？	5
访问站点提示连接不安全？	6
什么是OpenSSL？	7
什么是SSL证书？	10
什么是私钥？	11
什么是CSR？	12
域名型证书是否永久免费？	13
Chrome浏览器提示“您的连接不是私密链接”问题	14
忘记私钥密码怎么办？	16

常见问题

证书是否支持吊销？

证书目前仅支持线下吊销，请工单联系腾讯云工程师协助您进行吊销。

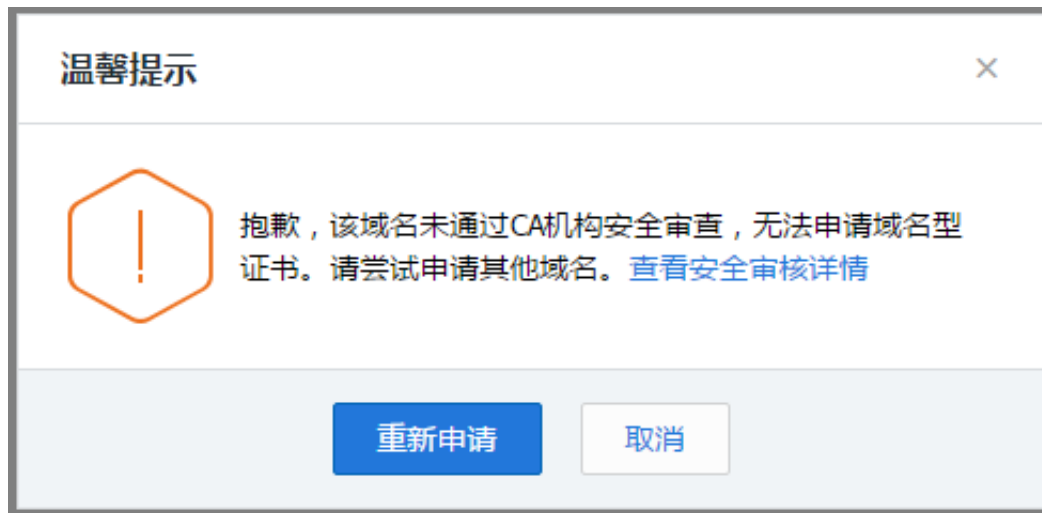
域名型证书吊销流程详情见 [操作指引](#)

安全审核失败的原因？

申请域名型（DV）SSL证书时

，出现如下提示，说明申请域名的安全审核失败，

赛门铁克CA机构的快速审核流程不支持对该域名颁发域名型SSL证书，请购买付费证书。



安全审核失败的具体原因：

由于CA机构的反钓鱼机制，一般是域名信息中包含敏感词，例如bank、pay等，会引起安全审核失败，具体敏感词由CA机构定义，同时部分不常用的根域名也可能会审核失败，例如 www.qq.pw www.qcloud.pw 等以.pw 根域名后缀的无法通过审核。

因为域名型SSL证书通过自动认证快速签发，不会人工介入审核，会用较为严格的敏感词来加强审核标准。

访问站点提示连接不安全？

SSL证书部署以后，访问站点提示“连接不安全”，是否是证书部署失败？

答：证书已成功部署，会出现这个问题，是因为采用https协议的站点如果网页中包含未经加密的http内容时，会被浏览器认为是不安全的；需要对代码进行改造。

前端改造上，可以有参考以下几点：

1. 使用相对路径引用资源；
2. 引用绝对路径的时候，采用

//

引用资源，例如：

//img.qcloud.com/example.png

，表示遵从当前页面的协议，浏览器会自动补齐。

什么是OpenSSL ?

OpenSSL是用于安全通信的著名开源密码学工具包，包括主要的密码算法、常见密码和证书封装功能。

1. OpenSSL官网

官方下载地址：<https://www.openssl.org/source/>

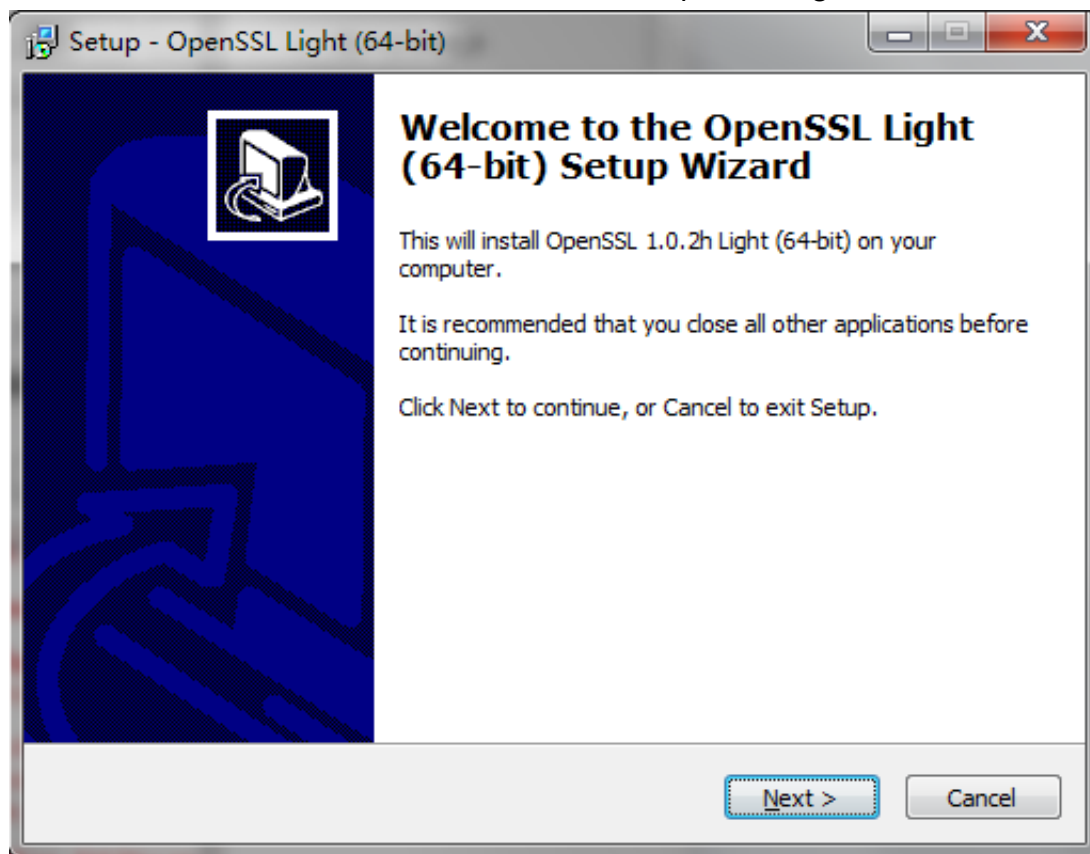
2. Windows安装方法

OpenSSL官网没有提供windows版本的安装包，可以选择其他开源平台提供的工具。例如

<http://slproweb.com/products/Win32OpenSSL.html>

以该工具为例，安装步骤和使用方法如下：

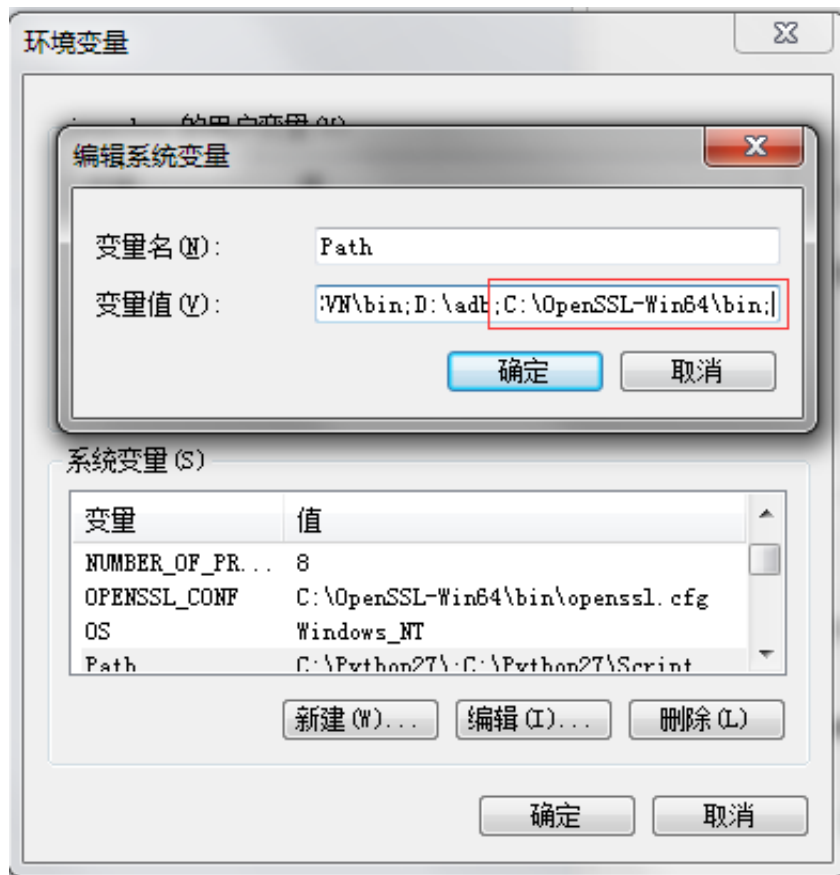
2.1 选择32位或者64位合适的版本下载，例如Win64OpenSSL_Light-1_0_2h.exe：



2.2 设置环境变量，例如工具安装在C:\OpenSSL-Win64，则将

C:\OpenSSL-Win64\bin；

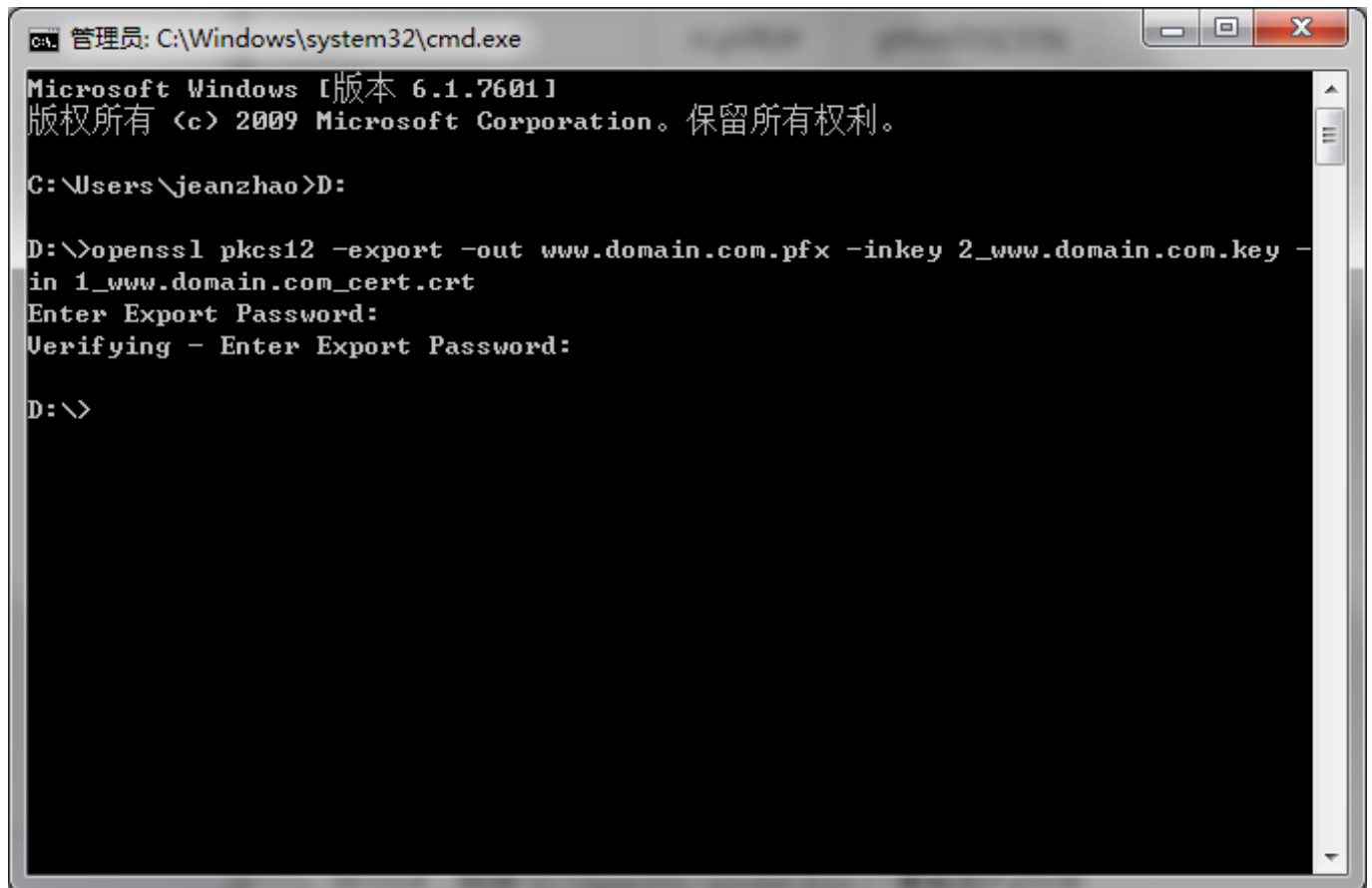
复制到Path中



2.3 打开命令程序cmd（以管理员身份运行），进入2_www.domain.com.key、1_www.domain.com_cert.crt所在目录，运行以下命令

```
openssl pkcs12 -export -out www.domain.com.pfx -inkey 2_www.domain.com.key -in
1_www.domain.com_cert.crt
```

例如key和crt文件保存在 D:\，运行情况如下：



Ps : Export Password不需要可以直接回车不进行输入。

2.4 则在 D:\ 已生成www.domain.com.pfx 文件，可以继续完成在IIS管理器中的证书安装。

什么是SSL证书？

首先说明SSL（安全套接层，Secure Sockets Layer）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。

CA（数字证书认证，Certificate Authority）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。

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。

什么是私钥？

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。

什么是CSR？

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。

在创建CSR过程中，需要提供相关组织机构信息，web服务器会根据提供的信息创建证书的标识名称，用来识别证书，内容如下：

国家/地区代码

您的组织机构依法注册所在国家/地区的国家/地区代码，以国际标准化组织 (ISO) 的两字母格式表示。

省/市/自治区

您的组织机构所在的省/市/自治区。

城市/地区

您的组织机构注册或所在的城市/地区。

组织机构

您的企业依法注册所用的名称。

组织机构单位

此字段用于区分组织机构中的各部门，例如“工程部”或“人力资源部”。

通用名称

在 CSR 的通用名称字段中输入的名称必须是您要为其使用证书的网站的完全限定域名 (FQDN)，例如“www.domainnamegoeshere”。

但是腾讯云采用了在线生成CSR的方式，无需您生成和提交CSR文件，域名型证书仅需要提交通用名称即可申请，帮助您简化申请流程。

域名型证书是否永久免费？

首先，SSL证书无论是免费的域名型或者是付费的企业型，CA机构都规定了有效期的，从安全性上考虑，不能保证一个合法网站永远不会成为一个钓鱼站点，CA机构需要定期审核，所以不会颁发永久有效的证书。

其次，当网站的私钥丢失时可以申请吊销，CA机构会将吊销的证书加入证书吊销列表（Certificate Revocation List，简称：CRL），每次Https站点被访问时，浏览器会向CA机构获取CRL，判断是否能信任该证书；然而永久有效的证书会导致CRL不断增加，不会减少，会增加浏览器的请求流量压力，所以指定证书的有效期是更科学的处理方式。

腾讯云目前提供免费的域名型证书，型号为TrustAsia DV SSL CA -

G5，证书有效期时长1年。证书过期前三个月

即可重新申请，域名型证书能在一个工作日内快速颁发，您有充足的时间为站点切换证书。

Chrome浏览器提示“您的连接不是私密链接”问题

2016年11月份起，部分chrome浏览器用

户反馈访问Https站点时的

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED错误情况，提示“您的连接不是私密链接”。

内容如下：



您的连接不是私密连接

攻击者可能会试图从pay.qq.com窃取您的信息（例如：密码、通讯内容或信用卡信息）。

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

隐藏详情

返回安全连接

该服务器提供了一个未通过证书透明度政策公开披露的证书。某些证书必须通过证书透明度政策进行公开披露，以确保它们值得信任且能保护用户免遭攻击。

[继续前往pay.qq.com（不安全）](#)

该CT错误经确认是chrome浏览器53、54版本的内核问题，该 BUG 导致与 Symantec CA机构颁发的SSL证书出现不兼容问题，Symantec CA机构所有2016年6月1日之后的证书都会被此问题影响出现CT错误的情况，Chrome方面在第一时间通过自动补丁方式处理了此问题，并在55版本修复此问题。

在能正常连接Chrome的服务器的客户都不会被此问题影响，但因中国大部分用户不能访问到Chrome的服务器，所以建议用户升级至55+版本来解决这个问题。

Q. When did this get patched?

A. Google patched in Chrome 55.

Q. What dates did this issue get resolved?

A. Chrome "stable" versions are the versions pushed out via their update mechanisms and are most commonly used. Dates for current releases can be found [here](#), and are copied below.

OS/Platform	User Action Required?
Chrome Mac	No
Chrome Windows	No
Chrome Linux	No
Chrome for Android	No
Chrome for iOS	No
Chromium	No action required by end users. May require Chromium distributors to rebuild.
Chromium based browsers (Opera, Opera Mini, Brave, Comodo Dragon)	No (n/a)
Chrome Custom Tabs	No.
This is the modern embedded browser for Android	No.
WebView This component is an embedded browser used in some Android apps. For example, an embedded browser might be used for an OAuth screen or an in-app web page display	YES App users will need to update/download WebView/Chrome 55 from the App Store/PlayStore for the fix. Downloading WebView/Chrome 54 today will provide a temporary solution. Build ID 54.0.2840.68 Expires 12/27/2016 Build ID 54.0.2840.85 Expires 1/7/2017
Android Open Source Platform (AOSP)	Developers need to apply the patch and users need to install an update

详情可查看赛门铁克官方公告：

<https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&id=ALERT2160>

Symantec官方声明：<https://www.symantec.com/connect/blogs/chrome-53-bug-affecting-symantec-sslts-certificates>

以及Chrome官方公告：

<https://bugs.chromium.org/p/chromium/issues/detail?id=664177>

另外，使用了 Chromium 53内核的QQ浏览器也会存在这个问题，已经在新版本中修复，使用了旧版本QQ浏览器的用户也建议更新到最新版本。

详情可查看QQ浏览器官方公告：<http://bbs.browser.qq.com/thread-222732-1-1.html>

忘记私钥密码怎么办？

腾讯云不会替您保存证书的私钥密码，请牢记私钥密码。

如果遗失私钥密码，请[提交工单](#)

，选择【其他问题】，提交给腾讯云工程师，协助您删除该证书后重新申请对应域名的证书。