# SSL 证书

# 产品简介

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

# 文档目录



版权所有：腾讯云计算（北京）有限责任公司

# 产品简介

# 产品概述

最近更新时间：2023-03-30 17:19:02

## 概述

SSL 证书（SSL Certificates）又称数字证书，是由腾讯云与业界知名的数字证书授权机构合作（CA，Certificate Authority），并在腾讯云平台为您提供免费与付费 SSL 证书的申请、管理、云部署等一站式管理服务。SSL 证书将为您的网站、移动 App、Web API 等应用提供身份验证和数据加密传输等整套 HTTPS 解决方案。

## HTTPS 原理介绍

以下视频将为您进一步介绍 SSL 协议的原理：
观看视频

## SSL 证书与 HTTPS 关系

基于 SSL 证书，可将站点由 HTTP（Hypertext Transfer Protocol）切换到 HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer），即基于安全套接字层（SSL）进行安全数据传输的加密版 HTTP 协议。
如通过腾讯云购买 SSL 证书后，您可以在腾讯云证书管理控制台向数字证书授权机构（CA）提交证书申请，等待 SSL 证书成功颁发；SSL 证书颁发后您可以将 SSL 证书进行下载并安装部署到您服务器的 Web 服务或一键部署至腾讯云的云资源中，则您的 Web 服务或云资源可以通过 HTTPS 加密协议来传输数据。

## HTTPS 优势

| 优势 | 说明 |
| --- | --- |
| 防劫持、防篡改、防监听 | 使用 SSL 证书实现网站、移动 App、Web API 等应用的 HTTPS 协议化后，HTTPS 将对用户与服务端间的数据交互进行加密，从而实现传输数据的防劫持、防篡改、防监听。 |
| 提升网站搜索排名（SEO） | 使用 SSL 证书实现网站的 HTTPS 协议化后，更利于搜索引擎对其信任，使网站在收录速度上更快，搜索结果中的排名更高，提升网站可信度。 |
| 提升网站的访问流量（PV） | 使用 SSL 证书实现网站的 HTTPS 协议化后，可以强化网站在用户侧的身份可信程度，使网站用户能更安心地访问网站，提升网站的访问流量。 |
| 杜绝钓鱼网站 | 可以帮助用户识别出钓鱼网站，保障用户和企业的利益不受损害，增强用户信任。 |

# 腾讯云SSL证书介绍

最近更新时间：2023-12-22 15:22:21

本文介绍腾讯云 SSL 证书支持的类型、域名类型、品牌介绍、行业选型案例以及加密算法。

## SSL 证书类型

腾讯云 SSL 证书支持购买 DV 证书、OV 证书和 EV 证书三种类型的 SSL 证书。不同类型证书的安全性、支持的证书品牌和适用的网站类型不同，具体如下表所示。

| 证书类型 | 适用网站类型 | 公信等级 | 认证强度 | 安全性 | 支持品牌 |
| --- | --- | --- | --- | --- | --- |
| DV（域名型） | 个人网站 | 一般 | CA 机构只验证网站的真实性，不验证企业信息，域名验证通过就可以颁发证书 | 一般 | • DNSPod（腾讯云自主品牌）<br>• TrustAsia<br>• Wotrus |
| OV（企业型） | 政府组织、企业、教育机构等 | 强 | CA 机构会验证网站的真实性，同时也需要验证企业信息真实性 | 高 | • SecureSite（同 DigiCert）<br>• GeoTrust<br>• GlobalSign<br>• DNSPod（腾讯云自主品牌）<br>• TrustAsia<br>• Wotrus |
| EV（企业增强型） | 大型企业、金融机构等 | 最高 | 最严格的认证标准，CA 机构会验证网站的真实性，同时也需要验证企业信息真实性 | 最高 | • SecureSite(同 DigiCert)<br>• GeoTrust<br>• GlobalSign<br>• DNSPod（腾讯云自主品牌）<br>• TrustAsia<br>• Wotrus |

### 不同证书类型在浏览器的展现形式

由于浏览器机制，目前 DV/OV/EV 证书**不会有明显的绿色地址栏**区分（不会有绿锁标识），只能从证书详情中来区分证书类型。

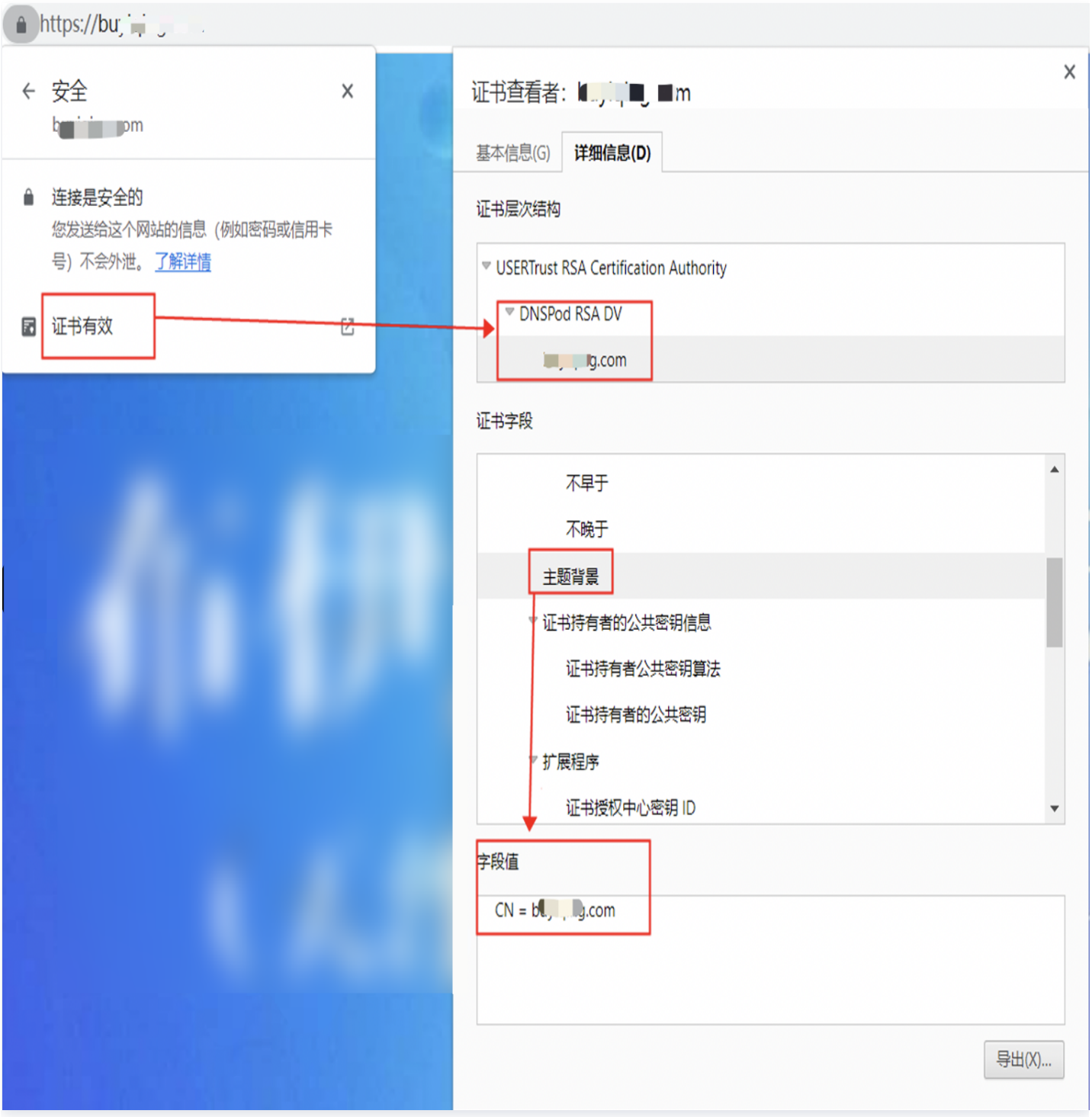
以下以 Chrome 浏览器作为示例（不同浏览器展示可能不同）。

> **说明：**
> 查看网站证书信息步骤：单击浏览器地址栏“锁”的标识 > **证书有效**。

**DV（域名型）证书**

只需验证域名所有权，无需人工验证申请单位真实身份，等几分钟即可颁发 SSL 证书。

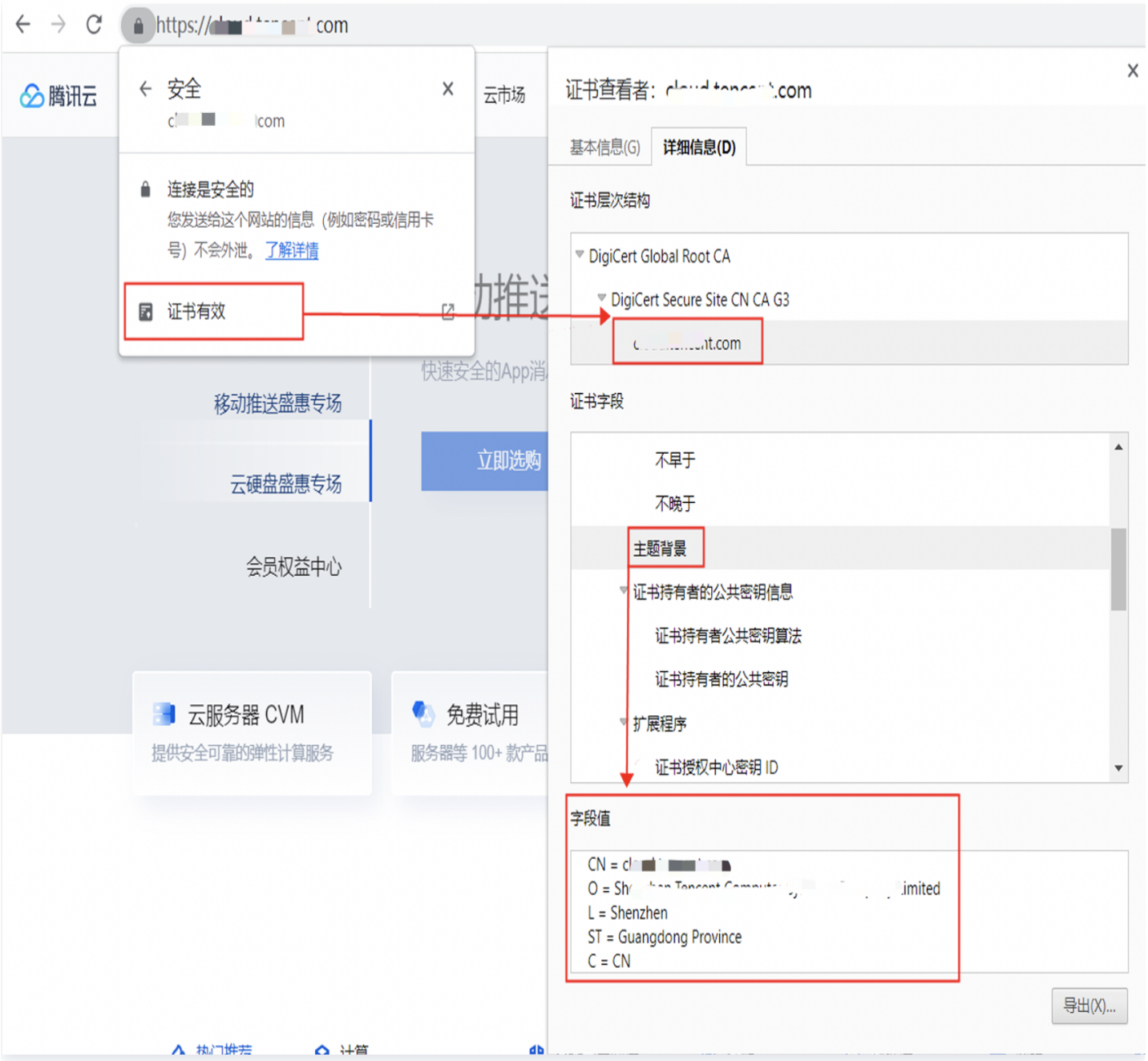
**浏览器仅显示域名信息**




**OV（企业型）证书**

**需要验证域名所有权以及企业身份信息，证明申请单位是一个合法存在的真实实体。**

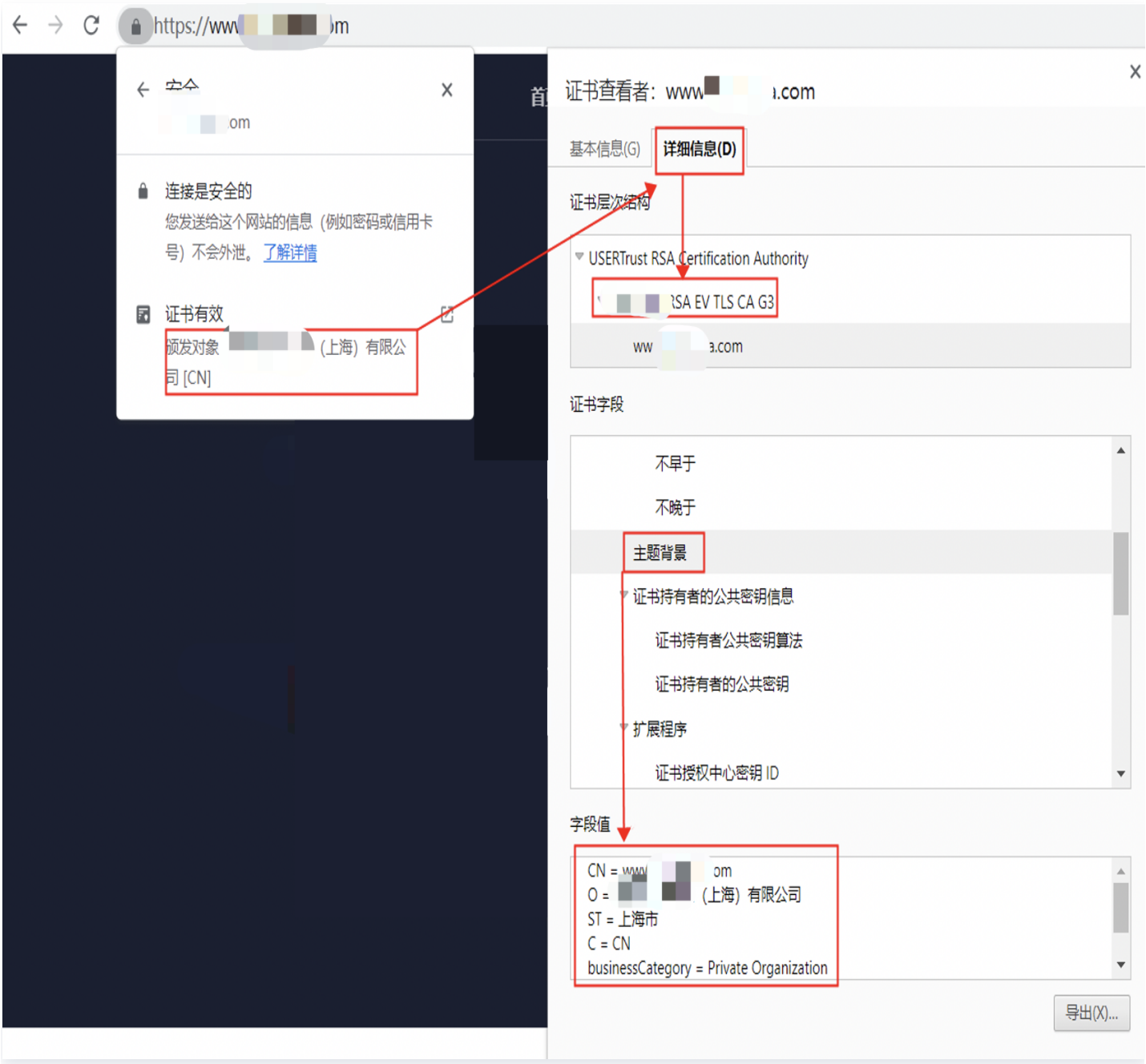
**浏览器显示域名信息和证书组织信息**




**EV（企业增强型）证书**

**除了需要验证域名所有权外，还会进行更严格的企业身份信息验证，需要提交扩展型验证文件，例如：邓白氏等，通常 CA 机构还会进行电话回访。**

**浏览器显示域名信息和更为详细的证书组织信息**




## SSL 证书有效期

SSL证书默认有效期为1年，如购买证书后未实际签发不计入有效期。SSL证书成功签发后视为生效，开始计算有效期（无法指定日期生效）。

## SSL 证书域名类型

下表为您说明 SSL 证书支持绑定的不同域名类型之间的区别

| 域名类型 | 说明 |
| --- | --- |

| | |
|---|---|
| 单域名 | 单域名是指一个证书只能保护一个主域名或一个子域名或一个公网IP |
| 多域名 | 多域名是指一个证书绑定多个单域名（需要同时绑定，证书签发后无法追加域名） |
| 通配符（泛域名） | 通配符域名是指对应一个主域名及其次级域名的所有子域名。例如 `*.tencent.com`；<br>如果您购买了一个 `*.tencent.com`，默认赠送 `tencent.com`，通配符 `*.tencent.com` 还可以匹配下一级子域名（ `www.tencent.com`、`example.tencent.com` ...），但不支持**跨级子域名**，例如 `www.example.tencent.com` |

## 腾讯云 SSL 证书品牌介绍

| 证书品牌 | 品牌介绍 |
|---|---|
| SecureSite | SecureSite 是 DigiCert（原 Symantec）旗下的品牌，全球最大的信息安全厂商和服务商，最权威的数字证书颁发机构，为企业、个人用户和服务供应商提供广泛的内容和网络安全解决方案，全球500强中有93%选择了 VeriSign SSL 数字证书。<br>SecureSite 证书具有安全、稳定、兼容性好等优势。 |
| GeoTrust | GeoTrust 是全球第二大数字证书颁发机构（CA），也是身份认证和信任认证领域的领导者，从2001年成立到2006年占领全球市场25%的市场份额，VeriSign 于2006年5月 - 2006年9月以1.25亿美元收购 GeoTrust，目前也同为 SecureSite 旗下 SSL 证书的性价比高的品牌。 |
| GlobalSign | GlobalSign 成立于1996年，是一家声誉卓著，备受信赖的 CA 中心和 SSL 数字证书提供商，在全球总计颁发超过2000万张数字证书。<br>GlobalSign 的专业实力获得中国网络市场众多服务器、域名注册商、系统服务供应商的青睐，成为其数字证书服务的合作伙伴。 |
| DNSPod | DNSPod 为腾讯云自有品牌，由国内知名 CA 机构提供基础设置支撑，DNSPod 证书针对中国市场特点设计，国内定制 OCSP，访问速度快。 |
| TrustAsia（亚洲诚信） | 亚数信息科技（上海）有限公司应用于信息安全领域的品牌，专业为企业提供包含数字证书在内的所有网络安全服务。TrustAsia 品牌 SSL 证书由 Sectigo 根证书签发。 |
| WoTrus（沃通） | 沃通电子认证服务有限公司（WoTrus CA Limited）是同时获得国内电子认证服务许可证（由工信部颁发）和通过国际认证的证书颁发机构（CA）。专业为企业提供权威第三方数字身份认证服务，颁发全球信任的各种数字证书产品。 |

| | |
|---|---|
| CFCA（国产） | 中国金融认证中心（CFCA）通过了国际 WebTrust 认证，是国际 CA 浏览器联盟的成员之一，提供全球信任证书，由中国权威数字证书认证机构自主研发，**纯国产证书。**<br>注意：CFCA 证书目前不支持苹果 iOS 10.1及10.1以前的版本，不支持 Android 6.0及以前的版本。 |

## 不同品牌差异

**不同品牌的证书最重要的差异点在于根证书：**

- SecureSite 是由 SecureSite 根证书签发，顶级根证书都是 DigiCert 旗下的。
- GeoTrust 是由 GeoTrust 根证书签发。
- GlobalSign 是由 GlobalSign 根证书签发。
- DNSPod 是由 Sectigo 根证书签发。
- TrustAsia 通配符是由 Sectigo 根证书签发。
- Wotrus 是由 Sectigo 根证书签发。

**从技术角度，SecureSite（原 Verisign）和 GeoTrust 的区别如下：**

- SecureSite 的兼容性优于 GeoTrust，SecureSite 可兼容市面上所有的浏览器，对移动端的支持也是极好的。
- SecureSite 在 OCSP 响应速度上优于 GeoTrust。
- SecureSite 在 CA 安全性方面优于 GeoTrust，SecureSite 是国际知名安全厂商，CA 的安全级别也是国际第一的安全系数。
- SecureSite 证书除实现加密传输以外，还有恶意软件扫描和漏洞评估的附加功能。
- SecureSite 与 GeoTrust 对证书均有商业保险赔付保障，SecureSite 赔付金额最高为175万美金，GeoTrust 赔付金额最高为150万美金。

## 支持绑定 IP 的 SSL 证书

| 证书品牌 | 企业型（OV） | 企业型专业版（OV Pro） | 域名型（DV） | 增强型（EV） | 增强型专业版（EV Pro） |
|---|---|---|---|---|---|
| SecureSite | **单域名/多域名支持**<br>其余域名类型不支持 | **单域名/多域名支持**<br>其余域名类型不支持 | 不支持 | 不支持 | 不支持 |
| GeoTrust | **单域名/多域名支持**<br>其余域名类型不支持 | – | – | 不支持 | – |

| | | | | | |
|---|---|---|---|---|---|
| TrustAsia | **单域名/多域名支持**<br>其余域名类型不支持 | – | 不支持 | 不支持 | – |
| GlobalSign | **单域名/多域名支持**<br>其余域名类型不支持 | – | – | 不支持 | – |
| Wotrus | 不支持 | – | 不支持 | 不支持 | – |
| DNSPod（国密） | **单域名/多域名支持**<br>其余域名类型不支持 | – | – | **单域名/多域名支持**<br>其余域名类型不支持 | – |
| DNSPod（国际） | **单域名/多域名支持**<br>其余域名类型不支持 | – | 支持 | 不支持 | – |
| CFCA | **单域名/多域名支持**<br>其余域名类型不支持 | – | – | 不支持 | – |

## SSL 证书行业案例

**下表为您介绍部分行业证书选型的案例，为您选择证书提供参考：**

| 行业分类 | 推荐的证书类型 | 案例类型 | 行业特征 |
|---|---|---|---|
| 金融、银行 | EV 型证书 | 中国银行 | • 希望企业身份信息展示在网站地址栏<br>• 对数据传输保密性有很高要求 |
| 教育、政府、互联网 | OV 通配符证书 | • 外交部<br>• 京东<br>• 腾讯新闻<br>• 上海黄金交易所<br>• 国家电网<br>• 用友软件 | • 网站后期有多个新增站点的需求<br>• 无需政府/公司名称展示在网站地址栏 |

| | | | |
|---|---|---|---|
| | | • 浪潮<br>• 腾讯云 | |
| 个人业务 | DV 型证书 | 个人博客等 | • 无数据传输业务<br>• 纯信息或内容展示的网站 |

## SSL 证书支持的加密算法

| 证书标准 | 证书类型 | 证书品牌 | 支持加密算法 | | | | | 支持签名算法 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | RSA | | ECC | | SM2 | RSA | | ECDSA | |
| | | | 2048 | 4096 | prime256v1 | secp384r1 | sm2 with SM4 | SHA256 | SHA384 | SHA256 | SHA384 |
| 国际标准 | 免费证书（域名型DV） | TrustAsia | 支持 | 不支持 | 支持 | 不支持 | 不支持 | 不支持 | 支持 | 支持 | 支持 |
| | 企业型（OV） | SecureSite | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| | | Geotrust | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| | | TrustAsia | 支持 | 支持 | 支持 | 不支持 | 不支持 | 不支持 | 支持 | 支持 | 支持 |
| | | GlobalSign | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| | | Wotrus | 支持 | 支持 | 支持 | 支持 | 不支持 | 支持 | 不支持 | 不支持 | 不支持 |
| | | CFC | 支 | 不 | 不 | 不 | 不支持 | 支 | 不支 | 不支 | 不 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | A | 持 | 支持 | 支持 | 支持 | | 持 | 持 | 持 | 支持 |
| | 企业型专业版（OV Pro） | Secure Site | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| | 域名型（DV） | TrustAsia | 支持 | 不支持 | 支持 | 不支持 | 不支持 | 不支持 | 支持 | 支持 | 支持 |
| | | Wotrus | 支持 | 支持 | 支持 | 支持 | 不支持 | 支持 | 不支持 | 不支持 | 不支持 |
| | 增强型（EV） | Secure Site | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| | | Geotrust | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| | | TrustAsia | 支持 | 支持 | 支持 | 不支持 | 不支持 | 不支持 | 支持 | 支持 | 支持 |
| | | GlobalSign | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| | 增强型专业版（EV Pro） | Secure Site | 支持 | 支持 | 支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 |
| 国密标准 | 企业型（OV） | DNSPod | 不支持 | 不支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 | 支持 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 域名型（DV） | | 不支持 | 不支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 | 支持 |
| | 增强型（EV） | | 不支持 | 不支持 | 不支持 | 不支持 | 支持 | 不支持 | 支持 | 支持 | 支持 |

# 腾讯云SSL证书产品优势

最近更新时间：2023-03-30 17:19:02

## 支持各大知名品牌的国际证书

腾讯云SSL 证书由国际顶级 CA 机构授权颁发，安全有保障。数字证书授权机构（CA，Certificate Authority）是管理与签发安全凭证和加密信息安全密钥的网络机构，承担公钥体系中公钥的合法性检验的责任，需要对用户、企业的身份真实性进行验证，其权威性、公正性十分重要，腾讯云只选择和顶级权威的 CA 机构合作，提供安全有保障的 SSL 证书，目前可在腾讯云选购 DigiCert、GeoTrust、GlobalSign、TrustAsia、Wotrus 等证书。

## 支持国密（SM2）证书

腾讯云自有 DNSPod 品牌 SSL 证书支持 SM2 国密算法，满足政府机构、事业单位、大型国企、金融银行等行业客户的国产化改造和国密算法合规需求。

## 支持多年期 SSL 证书

简化 SSL 证书产品申请和续费时的繁琐流程，为您自动化管理 SSL 证书申请、验证、审核、签发、续费的整个生命周期。

## 完善的 SSL 证书自动化管理功能

腾讯云 SSL 证书提供的自动化管理功能，如下表所示：

| 服务名称 | 服务描述 |
| --- | --- |
| 一键部署至云服务 | 支持将 SSL 证书快捷部署至腾讯云的云服务，例如负载均衡、CDN、云直播、COS、DDOS 等12种云服务，支持批量部署 |
| 证书自动续费服务 | 帮助您解决每年手动续费 SSL 证书的困扰 |
| 证书托管服务 | 开启证书托管服务后，旧证书续费后，您不需要重新将新证书手动部署到云资源上的服务。即自动将新 SSL 证书部署至原 SSL 证书已部署的腾讯云云资源，例如负载均衡、CDN、云直播、DDOS 等。**帮助您降低因证书有效期而导致重复部署产生的运维成本。** |
| 扩展服务 | 支持通过 API 调用的方式申请和管理证书，让您不再受限于仅能使用证书控制台进行申请和管理证书。 |

版权所有：腾讯云计算（北京）有限责任公司

# 腾讯云SSL证书浏览器兼容性测试报告

最近更新时间：2023-06-01 15:10:23

**说明：**

- CT（Certificate Transparency）为 Google 浏览器提供用于监测和审核 HTTPS 证书的策略，所以通常用 CT 错误来形容证书不兼容。
- 不同的证书品牌兼容性不同，测试报告如下（以下报告仅供参考）

| 浏览器版本 | 国际标准 | | | | | | 国密标准 | |
|---|---|---|---|---|---|---|---|---|
| | SecureSite | Geotrust | TrustAsia | GlobalSign | DNSPod | Wotrus | DNSPod 国密 | Wotrus 国密 |
| IE6 (有 SHA2 补丁) | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| IE（8+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| QQ（9.5.1/9.5.2） | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | 支持 | CT 错误 | CT 错误 |
| QQ（7+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 百度（6+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 遨游（4.4+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 360（8.1） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 360（6+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| UC（5+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 搜狗（6+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 猎豹（3+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 2345（7.1+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |

版权所有：腾讯云计算（北京）有限责任公司

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 枫叶（2+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 世界之窗（3.6+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| Opera（34+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| Safari（5+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| Edge | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| Firefox（25+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| Chrome（53/54） | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | 支持 | CT 错误 | CT 错误 |
| Chrome（46+） | 支持 | 支持 | 支持 | 支持 | 支持 | 支持 | CT 错误 | CT 错误 |
| 密信 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | 支持 | 支持 |
| 360国密 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | 支持 | 支持 |
| 红莲花 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | CT 错误 | 支持 | 支持 |

**注意：**

因 Chrome（53/54）版本内核 BUG，SecureSite 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，所以建议升级至55+版本来解决这个问题。同时 QQ 浏览器使用 Chromium（53/54）版本内核也受到影响。

# 多年期 SSL 证书介绍

最近更新时间：2023-11-07 17:39:12

## 什么是多年期证书

- 多年期证书是用户可一次性购买多年证书，每年证书临近到期时，腾讯云会自动将证书信息提交给CA机构审核，无需用户主动发起申请。
- 简化 SSL 证书产品申请和续费时的繁琐流程，为您自动化管理 SSL 证书申请、验证、审核、签发、续费的整个生命周期。
- 在腾讯云购买1年以上多年期证书并完成审核后，腾讯云将在前一个 SSL 证书有效期**到期前30个自然日内**为您自动申请第二张 SSL 证书，若您的组织及域名审核在有效期内，则会签发第二张证书，无需您进行重新申请操作。

> **说明**
> - 证书自动审核通过后相当于重新颁发证书，您需要将新证书替换现有证书。如果证书部署在腾讯云产品上，首选使用证书托管功能，请参见 证书托管；如果证书部署在其他平台，安装请参见 证书安装相关文档。

## 支持多年期的国际标准证书

| 证书品牌 | 是否支持多年期 |
| --- | --- |
| DNSPod | 支持 |
| TrustAsia | 支持 |
| Wotrus | 不支持 |
| GeoTrust | 支持 |
| SecureSite | 支持 |
| GlobalSign | 支持 |
| CFCA | 不支持 |

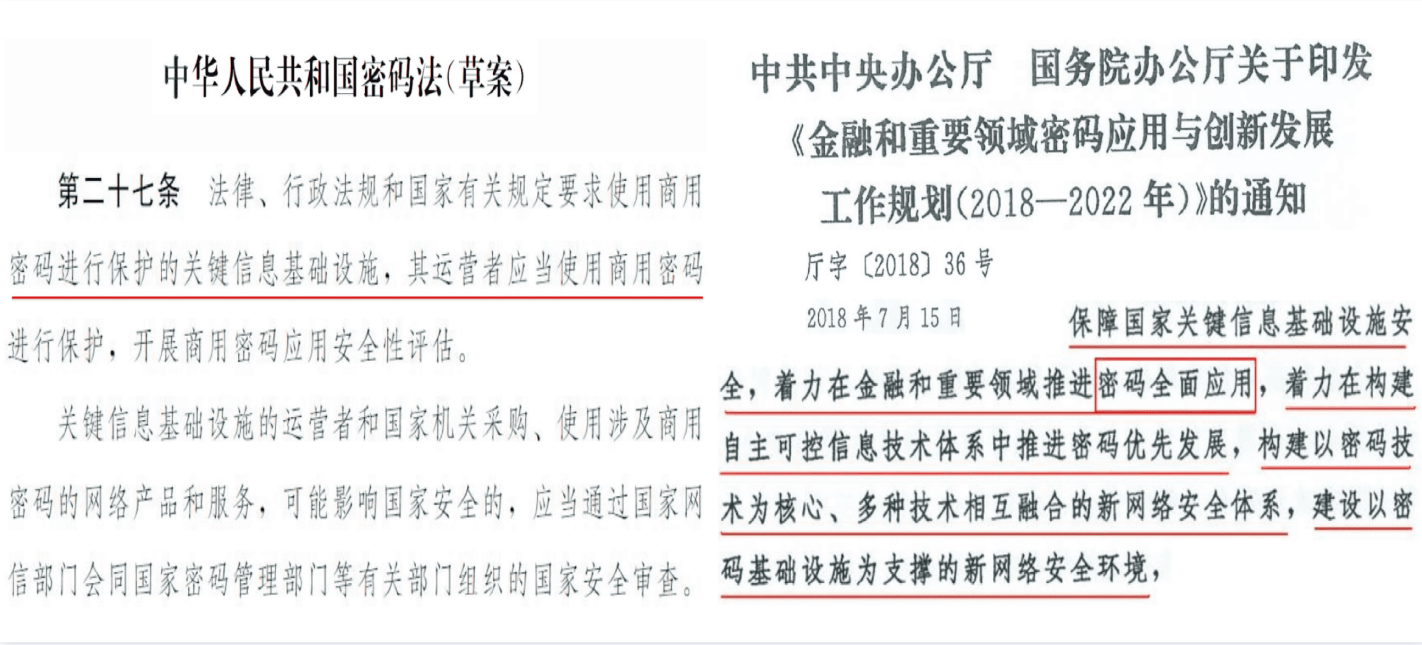
# 腾讯云国密方案介绍
# 政企国密解决方案介绍

最近更新时间：2023-03-30 17:19:03

腾讯云政企国密产品包在整套网络传输中，提供了国产密码化的服务。产品包中包含国际/国密双证书+国密自适应网关+国密浏览器+国密 DoH，同时包含完整建设和部署的整套方案，为您提供全流程的应用服务。
若您需要相关方案建设，请单击 **立即申请**，收到申请后腾讯云政企国密方案团队将会跟您联系。

## 背景说明

微软在 CA/B Forum 发布的全球信任根认证计划，首次把 “贸易制裁（Trade Sanctions）” 列为微软全球信任根认证计划的评估条件之一。
早在1999年，国务院就颁布了《商用密码管理条例》，截止目前为止，国家陆续颁布了多个条例来规范标准，引导相关领域的数据安全国产化，其中最关键的一个信息传递就是：关键信息基础设施安全必须采用应用密码技术来保障。如下图所示：



中华人民共和国密码法(草案)

第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，开展商用密码应用安全性评估。

关键信息基础设施的运营者和国家机关采购、使用涉及商用密码的网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

中共中央办公厅 国务院办公厅关于印发
《金融和重要领域密码应用与创新发展
工作规划(2018—2022 年)》的通知

厅字〔2018〕36 号

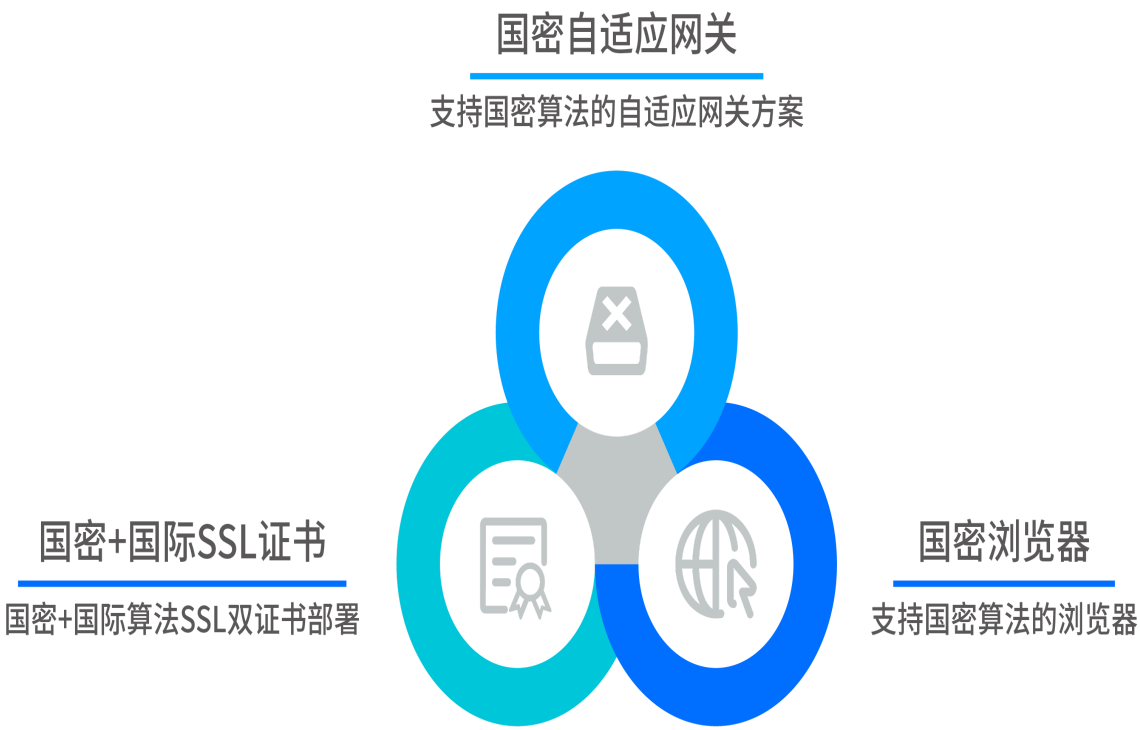
2018 年 7 月 15 日

保障国家关键信息基础设施安全，着力在金融和重要领域推进密码全面应用，着力在构建自主可控信息技术体系中推进密码优先发展，构建以密码技术为核心、多种技术相互融合的新网络安全体系，建设以密码基础设施为支撑的新网络安全环境，

网络安全等级保护2.0明确规定，要求对网络通信中的报文或会话过程全程加密（三级），其中密码技术标准之一就是 SM2 算法。
基于国家相关政策和要求，DNSPod 推出了腾讯云政企国密产品，使用国密（SM2）证书和相关生态建设，解决政企客户在网络传输过程中的等保合规需求。

## 方案说明

腾讯云政企国密产品包，一共包括三个主要模块：国际 + 国密双 SSL 证书、国密算法的浏览器、国密自适应网关。通过三者的相互结合，实现了完整网络传输中，国密链路的打通。如下图所示：




**用户通过不同的浏览器去请求访问站点，经过国密安全网关会进行判断：若系统自适应识别到浏览器支持国密算法，即可使用国密标准的 HTTPS 访问传输。若使用普通浏览器，则使用普通浏览器支持的国际算法证书来进行 HTTPS 访问传输。**

**即使国际标准证书不再被支持，也可以迅速的切换到国密标准，保证业务的连续性、稳定性。如下图所示：**

# 方案特点

## 目标客户

- 政府机关单位。
- 高校等教育单位。
- 电信网等提供公共信息网络服务单位。
- 广播电台、通讯社等新闻单位。
- 卫生医疗、金融、交通等公共服务单位。
- 其他需要进行国产密码化建设、满足等保合规需求的各大政府和企业。

## 国密 SM2 证书

**自主品牌**

腾讯云自主品牌、符合国家标准、完全自主知识产权、满足监控需求、无惧证书断供风险、服务及售后有保障。

**性能优越**

- 根据国外 ECC 加密算法性能研究报告：采用 ECC 算法，Web 服务器响应时间比 RSA 要快出10倍以上。
- 同时 SM2 的加密强度要远比 RSA 3072 高。

## 国密浏览器

**国密浏览器**

- 支持国密+国际双证书。
- 支持国密（SM2）、国际标准 SSL 证书访问。

**兼容性好**

- 支持 GB/T 38636-2020（GM/T 0024-2014）标准（TLCP）。
- 提供 Windows 系统版本和 Mac 系统版本。

**深度可定制**

- 腾讯云国密浏览器支持企业级的深度定制方案，可根据用户的不同需求进行浏览器各种配置的深度定制。

## 国密网关

版权所有：腾讯云计算（北京）有限责任公司

**负载均衡**
对 Web 应用深度优化，支持 IP 会话保持、会话应用保持、深度健康检查、支持 URL 重定向、双机热备。
**Web 加速**
支持动态压缩、对象存储、连接复用等加速技术，同时支持阈值上线限及告警。支持用户证书透传、页面智能预加载等。
**SSL 加速**
支持 RSA/ECC/SM2 加速、SSL v3.0、TLS v1.0-V1.3 协议、国密双证书、国密算法 SM1/2/3/4、国密浏览器。

国密 DoH

- 支持 DNSPod 国密 DoH 服务。
- DNS over HTTPS（缩写：DoH）是一个进行安全化的域名解析方案。其意义在于以加密的 HTTPS 协议进行 DNS 解析请求，避免原始 DNS 协议中用户的 DNS 解析请求被窃听或修改（例如中间人攻击），来达到保护用户隐私的目的。
- 国密网关及浏览器 DoH 模块均支持 SM2 加密算法，从而给用户提供了完整的域名解析国密链路。

## 版本说明

| 类别 | | 企业版 | 高级版 | 尊享版 | 说明 |
|---|---|---|---|---|---|
| 价格 | | 400000 | 700000 | 1200000 | 所有方案均包含国密/国际标准证书+国密网关+国密浏览器整体交付。<br>方案均包含实施、部署及维护费用。<br>可根据用户增加的配置或服务进行单独计费。 |
| 证书 | 国际标准 SSL 证书（OV 通配符） | 5 | 10 | 15 | 采用 DigiCert 顶级根证书，安全可靠。 |
| | 国密标准 SSL 证书（OV 通配符） | 5 | 10 | 15 | 腾讯云自主品牌 DNSPod 中级根，服务售后有保障。 |
| 网关 | T100型 | ✓ | - | - | • 最大并发：30000<br>• SSL 吞吐：1 Gbps<br>• SSL 新建（RSA2048）：5500 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | • SSL 新建（国密）：3000<br>• 尺寸：2 U<br>• 电源：双电 |
| | T200型 | – | ✓ | – | • 最大并发：50000<br>• SSL 吞吐：1 Gbps<br>• SSL 新建（RSA2048）：15000<br>• SSL 新建（国密）：13000<br>• 尺寸：2 U<br>• 电源：双电 |
| | T500型 | – | – | ✓ | • 最大并发：100000<br>• SSL 吞吐：10 Gbps<br>• SSL 新建（RSA2048）：40000<br>• SSL 新建（国密）：30000<br>• 尺寸：2 U<br>• 电源：双电 |
| 国密专属浏览器 | 国密+国际双证书访问 | ✓ | ✓ | ✓ | 支持双证书访问 |
| | 浏览器图标定制 | – | ✓ | ✓ | 专属图标 |
| | 浏览器名称定制 | – | ✓ | ✓ | 专属名称 |
| | 浏览器颜色风格定制 | – | – | ✓ | 自定义颜色风格 |
| | 专属安装页面 | – | – | ✓ | 自定义安装 UI |
| | 定制开发服务 | 视情况而定 | 视情况而定 | 视情况而定 | 用户的定制化需求 |
| 政企国密支持服务 | 国密系统部署 | ✓ | ✓ | ✓ | 国密解决方案的一站式部署。 |
| | 国密产品培训 | ✓ | ✓ | ✓ | 国密解决方案的产品使用及维护培训。 |
| | 国密技术支持 | ✓ | ✓ | ✓ | 提供7*12的技术支持服务。 |
| | 国密产品 VIP 服务 | – | – | ✓ | 国密产品 VIP 服务将拥有更短的问题响应和解决时间，同时有专属的1V1技术人员支持。 |

版权所有：腾讯云计算（北京）有限责任公司

# DNSPod 品牌国密标准（SM2）SSL 证书基本概念

最近更新时间：2023-11-08 18:04:11

## DNSPod 品牌国密标准（SM2）证书概念

国产密码算法是保障我国网络安全自主可控的重要基础。网络信息安全应用领域 “HTTPS 加密”，逐步普及国密 SM2 算法。国密 SM2 算法通过自主可控的密码技术保护互联网中重要信息流转的数据安全，对提升我国网络信息安全与自主可控水平，具有重要战略意义。我国已经出台多项政策，要求大力推动国产密码算法在金融与重要领域的应用。
DNSPod 品牌国密标准（SM2）证书不仅满足政府机构、事业单位、大型国企、金融银行等行业客户的国产化改造和国密算法合规需求。同时通过 “SM2/RSA” 双证书服务帮助网站系统自适应兼容所有浏览器，兼顾国密合规和全球通用。

> **注意**
> - 国密证书目前暂不支持腾讯云产品**内容分发网络 CDN、T-Sec DDoS 防护、T-Sec Web 应用防火墙、云直播 CSS** 的部署，其他产品的支持情况请咨询客服4009100100或浏览相关产品文档进行确认。
> - 国密证书目前暂不支持 **Tomcat 服务器、GlassFlash 服务器、JBoss 服务器、Jetty 服务器、IIS 服务器、Weblogic 服务器**的部署。

## 国密算法的 SSL 认证和加密实现

国密 SSL 协议的握手过程如下：
1. 交换 Hello 消息来协商密码套件，交换随机数，决定是否会话重用。
2. 交换必要的参数，协商预主密钥。
3. 交换证书信息，用于验证对方。
4. 使用预主密钥和交换的随机数生成主密钥。
5. 向记录层提供安全参数。
6. 验证双方计算的安全参数的一致性、握手过程的真实性和完整性。

实现以上握手过程，需要客户端（浏览器）和服务端都支持国密算法。虽然目前 SM2/SM3/SM9 算法已相继纳入国际标准体系，但要实现客户端和服务端的广泛兼容，仍然需要漫长的推进过程。在此期间，通过技术解决方案让浏览器端、服务端都能够支持国密算法和国密 SSL 证书，才能推动国密算法普及应用。
因此，在服务端实现基于国密算法的 SSL 认证和 HTTPS 加密，需要网站运营者向工信部许可的权威电子认证机构（例如 DNSPod），申请符合国密标准的国密 SSL 证书，并将证书部署在支持国密标准证书的 web 服务器上。

版权所有：腾讯云计算（北京）有限责任公司

当使用国密浏览器访问已部署国密标准证书的站点时，浏览器和服务端将使用国密算法加密传输数据，实现国密算法 SSL 认证和加密。

版权所有：腾讯云计算（北京）有限责任公司

# DNSPod 品牌国密标准（SM2）SSL 证书浏览器问题

最近更新时间：2023-03-30 17:19:03

## 支持 DNSPod 品牌国密标准（SM2）证书的浏览器

360浏览器，密信浏览器，红莲花浏览器等可支持国密算法。

## DNSPod 品牌国密标准（SM2）证书浏览器兼容性问题解决

使用国密算法 SSL 证书的站点，在国密浏览器上可以正常访问，但由于国密算法还没有在所有主流浏览器中广泛兼容，因此一些仅支持国际算法的主流浏览器会对国密 SSL 证书报错。
您可以使用 “双证书部署” 和 “自适应浏览器兼容” 方案来解决这个问题，该方案可以同时兼容国密算法浏览器和仅支持国际算法的浏览器。通过此方案，您使用任意浏览器都能正常访问网站，满足部署国密 SSL 证书的合规需求，同时满足网站可用性、易用性和全球通用性要求，解决了国密 SSL 应用的技术障碍。

> **说明**
> 腾讯云提供 免费的 DV 型 SSL 证书 以供购买了 DNSPod 品牌国密标准（SM2）证书的用户顺利解决浏览器兼容问题，具体部署方式可以参考 国密标准证书安装 。

## DNSPod 品牌国密标准（SM2）不同证书类型浏览器区别

| 证书类型 | 企业型（OV） | 域名型（DV） | 增强型（EV） |
| --- | --- | --- | --- |
| 支持通配域名 | 支持 | 支持 | 不支持 |
| 支持多域名 | 支持（最多100个域名） | | |
| 密码算法 | 采用 SM2 国产密码算法体系，密钥强度高于国际标准 | | |
| 浏览器兼容性 | 兼容360浏览器、密信浏览器、红莲花浏览器等支持国密算法的浏览器 | | |

### DNSPod 品牌国密标准（SM2）证书地址栏区别

- 域名型（DV）：支持在国密浏览器中显示安全锁。
- 企业型（OV）：支持在国密浏览器中显示安全锁及单位名称。
- 增强型（EV）：支持在国密浏览器中直观显示绿色地址栏及单位名称。

版权所有：腾讯云计算（北京）有限责任公司

# 自动化管理方案

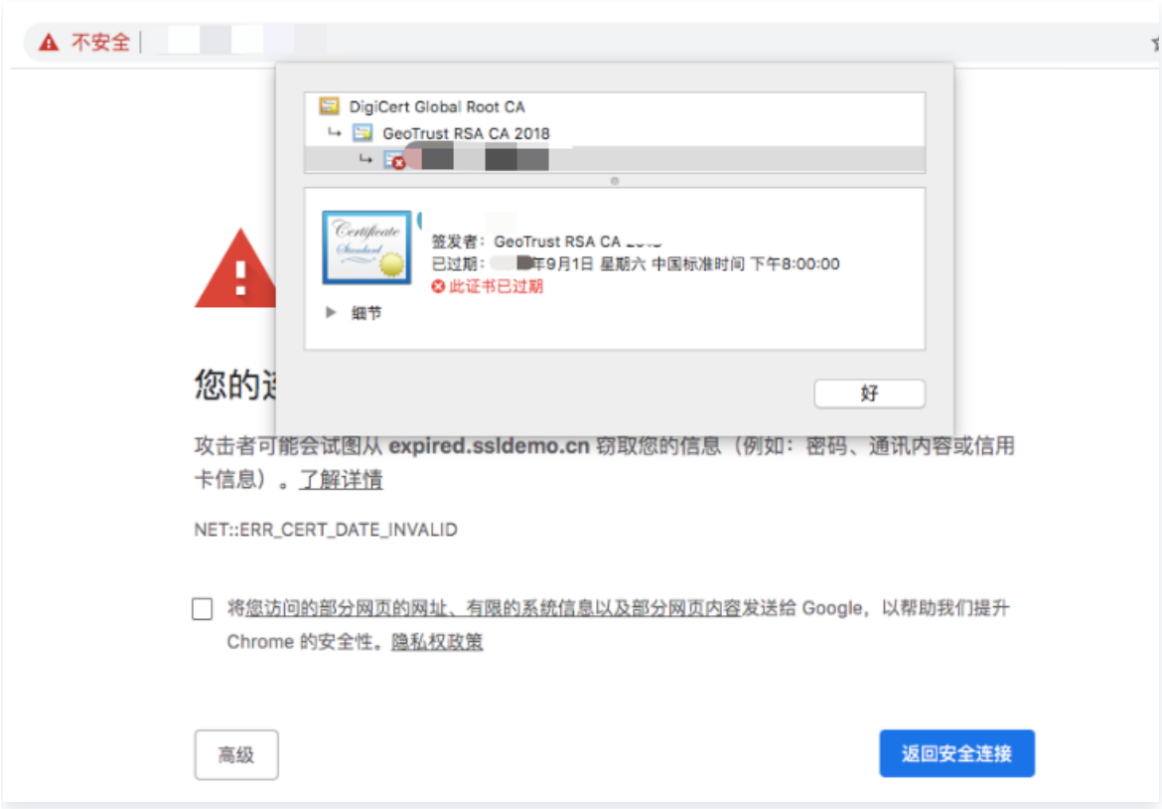
最近更新时间：2023-09-27 21:40:01

如果您是首次申请证书，您需要先对证书的品牌以及种类进行了解，再根据您的实际需求申请适合您的证书，具体请参见 腾讯云SSL证书介绍 。
本文主要介绍如何进行证书自动化管理。

> **说明：**
> 只需开启**自动添加 DNS 解析 + 证书自动续费 + 证书托管**三个服务，并且账号预留充足的余额即可实现证书自动化管理。

## SSL证书逾期未续费造成的影响

如果 SSL 证书过期没有续费，用户访问网站时会显示“网站的安全证书已过期”的警告信息，导致用户出于安全考虑停止访问网站；也有不法分子利用过期的SSL 证书，篡改或窃取浏览器与服务器之间传输的信息和数据，影响用户的数据安全。




## SSL 证书开启自动续费

请前往 SSL 证书控制台 > **我的证书**，在**我的证书**页面，开启自动续费，详情请参见 SSL 证书自动续费指引 。

> **说明：**

自动续费仅对正式证书开放，免费证书不支持自动续费。


## SSL证书续费后自动化替换旧资源

开启证书托管服务，您在 SSL 证书续费签发成功后，则不需要重新将证书部署至云资源上的服务，即该服务会自动将新 SSL 证书部署至原 SSL 证书已部署的腾讯云云资源，例如负载均衡、内容分发网络等。详情请参见 云资源托管指引 。

**说明：**
SSL 证书签发后即可开启云资源托管并绑定相关云资源，当该 SSL 证书进行续费操作生成新证书时，原证书上的关联云资源将自动绑定到新证书上。

1. 请前往 SSL 证书控制台 > **我的证书**，在**我的证书**页面，单击 ID。


2. 在打开的页面，按需开启证书托管服务。


省心用
证书托管服务
证书到期后，将续签的证书自动部署到当前证书部署的云产品上，不再因为证书更换而重新部署。
请选择需要托管的云产品类型：
内容分发网络（0）
负载均衡（0）
云直播（0）
Web应用防火墙（0）
DDoS防护（0）
当前证书托管只支持以上云产品，如果您的业务部署在其他类型的云产品上，请在证书到期续签后手动部署。
保存设置

# SSL 证书角色策略配置说明

最近更新时间：2024-01-17 15:00:32

**由于腾讯云 SSL 证书支持将证书部署到不同的腾讯云云服务，需要访问您账号下的云服务资源。**因此当您在腾讯云SSL证书控制台，使用**查询证书关联资源、证书部署、证书更新、证书托管**等功能时，需要您对 SSL 证书角色进行授权，通过策略控制 SSL 证书访问范围。

> **说明：**
> 服务（相关）角色是由腾讯云服务预定义，经用户授权后相应服务即可通过扮演服务相关角色对用户资源进行访问操作。

## 角色使用场景

能够申请担任角色的对象我们称它为角色载体。目前，腾讯云角色载体分为三类：腾讯云账号、已支持角色功能的产品服务、身份提供商。对应的场景如下：

- 您要向您账号中的用户授予临时的资源访问权限，或者是向另一个腾讯云主账号内的用户授予您账户中的资源访问权限。
- 您可能需要允许腾讯云产品服务对您的资源拥有访问权限，但不希望将长期密钥嵌入在产品服务中，因为这样存在难以轮换密钥以及被截取后泄露导致的安全问题。
- 您要向您账号中的资源（例如容器实例，云服务器实例等）绑定角色，使云资源对不同的云服务具有不同的访问权限。详情请参见 基于资源的服务角色 。

## SSL 证书在访问管理控制台的角色名称

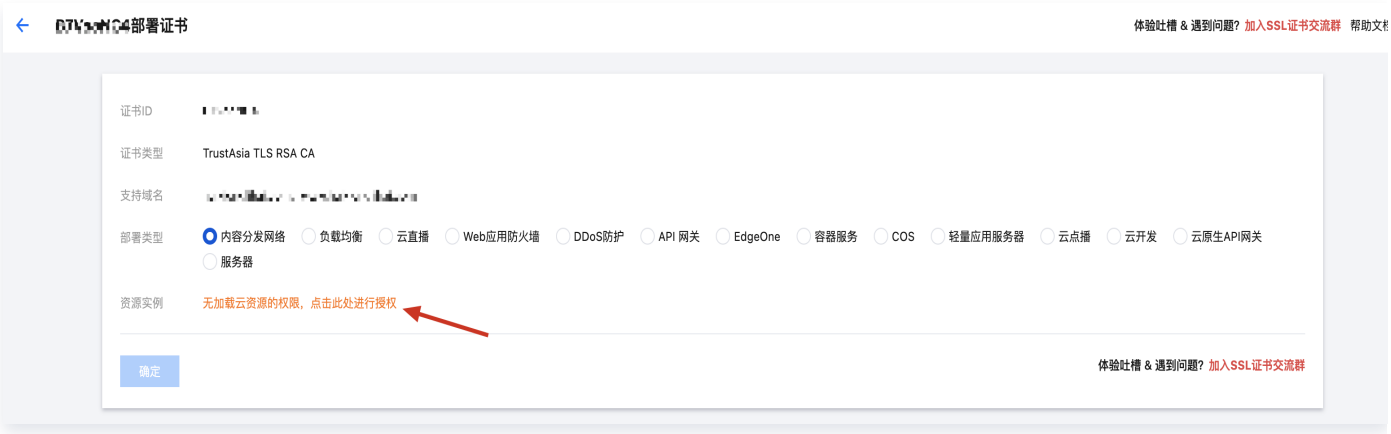
您可参考下列角色描述，根据自己的使用场景需要进行授权。例如，当您需要使用**查询证书关联资源、证书部署、证书更新、证书托管功能时，可以提前进行角色授权，**方便您后续使用。详细信息请参见 SSL 证书 。

| CAM 中产品名 | 角色名称 | 角色类型 | 备注 |
| --- | --- | --- | --- |
| SSL证书 | SSL_QCSLinkedRoleInCertificateWaf | 服务相关角色 | 使用**一键 HTTPS** 时授权。 |
| SSL证书 | SSL_QCSLinkedRoleInCertificateDependence | 服务相关角色 | 使用**自动添加 DNS** 时授权。 |
| SSL证书 | SSL_QCSLinkedRoleInReplaceLoadCertificate | 服务相关角色 | 使用**查询证书关联资源、证书部署、证书更新、证书托管**时授权。<br>点击此处前往访问管理控制台进行角色授权>> |

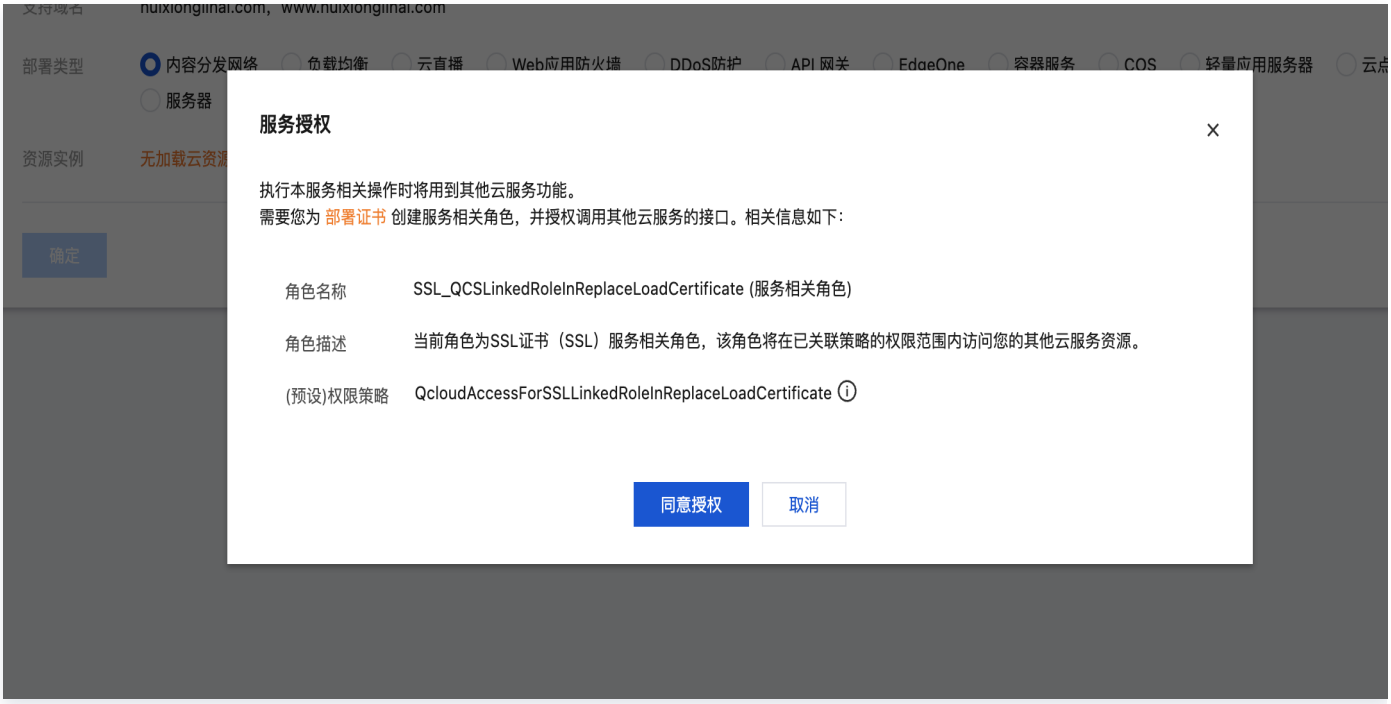
| | | | |
|---|---|---|---|
| SSL证书 | SSL_QCSLinkedRoleInCertificateCloudMonitor | 服务相关角色 | 使用**可视化监控**时授权。 |
| SSL证书 | SSL_QCSLinkedRoleInDescribeDeployedResources | 服务相关角色 | 使用**查询证书关联资源**时授权（旧接口）。 |

# 为 SSL 证书角色进行授权

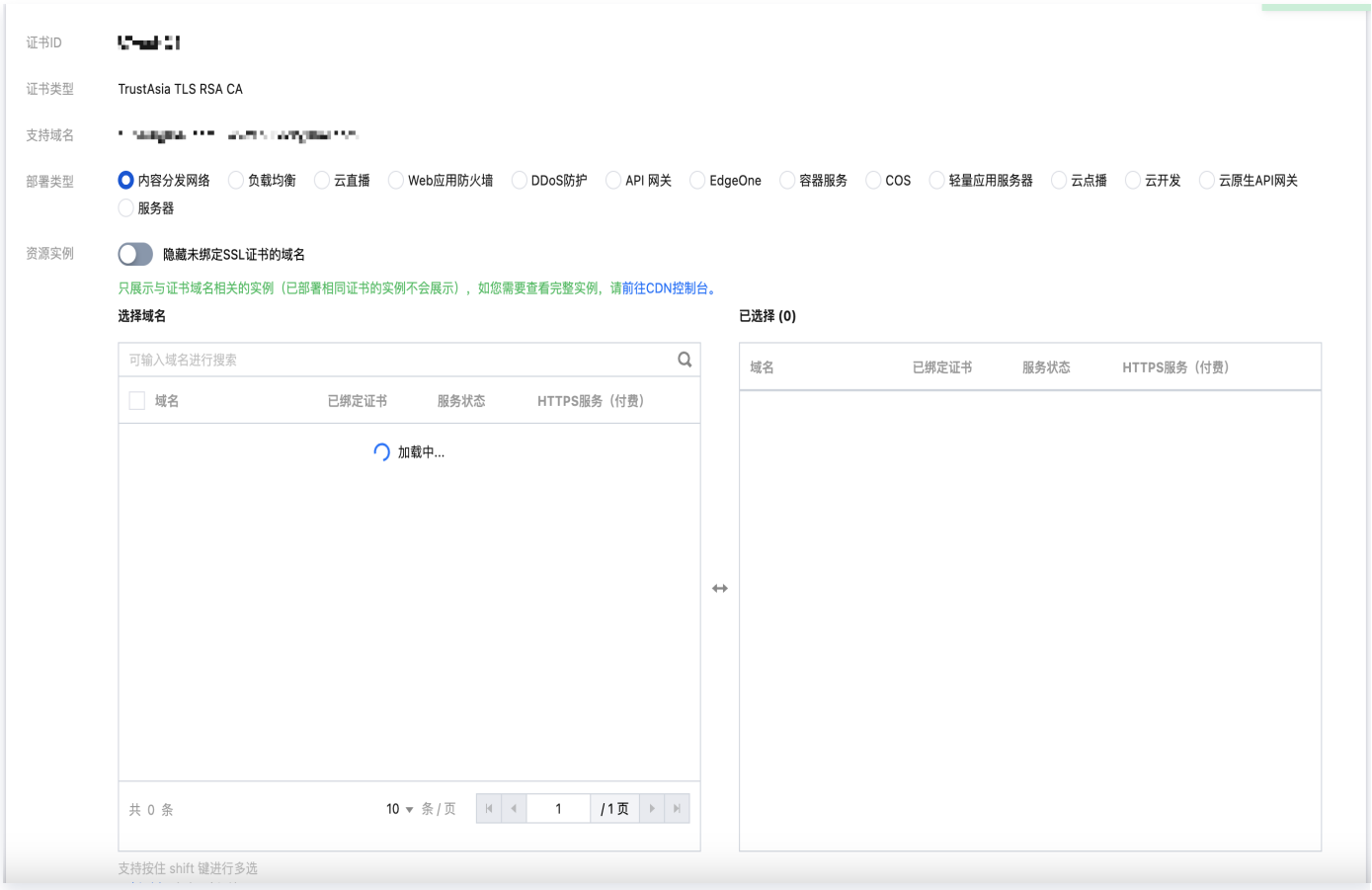
1. 当您使用证书部署时，若缺少角色授权，控制台页面会有相关提示，如下图所示：




2. 单击**点击此处授权**，在弹出的窗口中，单击**同意授权**进行授权。




3. 完成授权后，即可查询账号下云服务的资源。




# 如何为子账号赋予扮演角色策略?

详细信息，请参见 为子账号赋予扮演角色策略 。