# SSL 证书

# 产品公告

腾讯云

【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

# 产品公告
# 关于 DigiCert 及旗下品牌 SSL 证书价格调整的通知

最近更新时间：2025-06-06 16:35:22

**尊敬的腾讯云 SSL 证书用户**

**根据 DigiCert 官方全球统一调价策略（2024年6月10日起生效），腾讯云 SSL 证书将对代理的 Rapid、GeoTrust、SecureSite、DigiCert 品牌 SSL 证书执行价格调整，新价格将于北京时间2025年7月1日零点生效。本次调价涉及的证书规格如下：**

> **说明：**
> 多域名证书为特殊规格，未包含在下图中，具体调整价格请以 购买页 为准。

| 证书品牌 | 证书类别 | 域名类型 | 证书年限（年） | 调整前公开价格（元） | 调整后公开价格（元） |
|---|---|---|---|---|---|
| Rapid | 域名型（DV） | 单域名 | 1 | 378 | 405 |
| | 域名型（DV） | 通配符 | 1 | 1,788 | 1,918 |
| GeoTrust | 企业型（OV） | 单域名 | 1 | 2,778 | 2,970 |
| | 企业型（OV） | 通配符 | 1 | 7,278 | 7,840 |
| | 增强型（EV） | 单域名 | 1 | 6,000 | 6,420 |
| SecureSite | 企业型（OV） | 单域名 | 1 | 5,600 | 5,990 |
| | 企业型（OV） | 通配符 | 1 | 40,000 | 42,800 |
| | 增强型（EV） | 单域名 | 1 | 8,992 | 9,620 |
| | 企业型专业版（OV Pro） | 单域名 | 1 | 8,992 | 9,620 |
| | 增强型专业版（EV Pro） | 单域名 | 1 | 16,800 | 17,900 |
| Digicert | 代码签名证书 | / | 1 | 6,000 | 6,420 |
| | 代码签名证书（EV版） | / | 1 | 9,000 | 9,630 |

感谢您对腾讯云 SSL 证书的支持与关注，并敬请您谅解这一必要的调整。如果您有任何疑问，欢迎随时与我们沟通。

# 关于 DNSPod 品牌根证书的调整公告

最近更新时间：2025-05-12 10:30:02

**⚠ 注意：**

- 原定于2025年5月12日14时调整 DNSPod 品牌（国际算法 RSA/ECC）根证书将顺延至2025年5月27日14时调整。
- 原定于2025年5月12日14时调整 DNSPod 品牌（国密算法 SM2）根证书将顺延至2025年6月30日14时调整。

**尊敬的腾讯云 SSL 证书用户**

**为响应全球证书信任体系规范（Mozilla 根证书策略），提升证书服务安全性及国产化合规能力。腾讯云 SSL 证书计划于北京时间2025年5月27日14时对 DNSPod 品牌的根证书信任链进行调整。本次调整涉及根证书的替换与更新，不影响已签发的证书。现将相关事项公告如下：**

## 一、调整内容（DNSPod 品牌专属）

- **国际算法（RSA/ECC）证书**

| 调整项 | 旧根证书（截至2025年5月27日） | 新根证书（2025年5月27日启用） |
| --- | --- | --- |
| 签名算法 | RSA/ECC | RSA/ECC |
| 根证书 | USERTrust RSA Certification Authority | UCA Global G2 Root（国产根）<br>满足政务、金融等场景数据不出境需求 |
| | | • DigiCert Global Root G2<br>• DigiCert Global Root G3（ECC 算法） |

- **国密算法（SM2）证书**

| 调整项 | 旧根证书（截至2025年6月30日） | 新根证书（2025年6月30日启用） |
| --- | --- | --- |
| 签名算法 | SM2 | SM2 |
| 根证书 | TrustAsia Global SM2 Root CA G2 | UCA Root SM2 |

**说明：**

- 北京时间2025年5月27日前申请的 DNSPod 品牌 SSL 证书续费时可自主选择继续延用旧根证书 USERTrust RSA Certification Authority，已开启自动续费的证书默认沿用旧根证书 USERTrust RSA Certification Authority 续费证书。
- 北京时间2025年5月27日以后，若您还需要使用 USERTrust RSA Certification Authority 根证书，可在腾讯云选购 Wotrus 品牌的 SSL 证书。
- **如您的 DNSPod 证书用于 App 业务、IoT 终端等非 PC 浏览器，请您务必检查是否在终端预置过根证书。如您曾预置过根证书，需要您修改成系统自带的信任库做验证或下载最新的根证书和中间证书进行替换。**

## 二、涉及调整的 DNSPod 根证书列表

**说明：**
购买国际标准算法(RSA/ECC)的 DNSPod 证书后，可在控制台提交资料时自主选择根证书。

| 证书类型 | 算法类型 | 原根证书 | 原中间根证书 | 新根证书 | 新中间根证书 |
| --- | --- | --- | --- | --- | --- |
| 域名型(DV) | RSA | USERTrust RSA Certification Authority | DNSPod RSA DV | UCA Global G2 Root（国产根） | DNSPod DV TLS RSA CA G1 |
| | | | | DigiCert Global Root G2 | DNSPod DV TLS RSA CA 2025 |
| | ECC | USERTrust RSA Certification Authority | DNSPod ECC DV | UCA Global G2 Root（国产根） | DNSPod DV TLS ECC CA G1 |
| | | | | DigiCert Global Root G3 | DNSPod DV TLS ECC CA 2025 |
| | SM2 | TrustAsia Global SM2 Root CA G2 | DNSPod TLS SM2 CA G2 | UCA Root SM2 | DNSPod DV TLS SM2 CA G1 |

| | | | | | |
|---|---|---|---|---|---|
| 企业型(OV) | RSA | USERTrust RSA Certification Authority | DNSPod RSA OV | UCA Global G2 Root（国产根） | DNSPod OV TLS RSA CA G1 |
| | | | | DigiCert Global Root G2 | DNSPod TLS RSA CA 2025 |
| | ECC | USERTrust RSA Certification Authority | DNSPod ECC OV | UCA Global G2 Root（国产根） | DNSPod OV TLS ECC CA G1 |
| | | | | DigiCert Global Root G3 | DNSPod TLS ECC CA 2025 |
| | SM2 | TrustAsia Global SM2 Root CA G2 | DNSPod TLS SM2 CA G2 | UCA Root SM2 | DNSPod OV TLS SM2 CA G1 |
| 增强型(EV) | RSA | USERTrust RSA Certification Authority | DNSPod RSA EV | DigiCert Global Root G2 | DNSPod TLS RSA CA 2025 |
| | ECC | USERTrust RSA Certification Authority | DNSPod ECC EV | DigiCert Global Root G3 | DNSPod TLS ECC CA 2025 |

**感谢您对腾讯云 SSL 证书的支持与关注，并敬请您谅解这一必要的调整。如果您有任何疑问，欢迎随时与我们沟通。**

# 关于谨防假冒腾讯云 SSL 证书供应商的说明

最近更新时间：2025-03-07 15:52:22

**尊敬的腾讯云用户：**

**近期，我们接到用户反馈，有不法企业或个人假冒腾讯云 SSL 证书供应商，通过电话、微信等方式，以“低价续费、套件服务升级、测试证书不安全”等话术，试图诱导用户前往非腾讯云官方平台购买或续费 SSL 证书，请务必提高警惕，避免因轻信虚假信息导致经济损失或信息泄露风险。腾讯云不会将用户数据泄露或出售给第三方公司，腾讯云合作伙伴也不会让客户去非腾讯云平台购买产品。**

**为避免给您造成困扰，腾讯云 SSL 团队特此声明：**

1. 当您在腾讯云平台购买的 SSL 证书即将到期时，腾讯云会在证书到期前7天、前15天、前29天通过官方渠道（邮件、站内信、短信）的方式通知您及时续费，不会通过微信或其他个人形式直接联系您办理续费业务。如遇类似情况，请提高警惕并及时核实信息真实性。
2. 腾讯云合作的 CA 厂商只有在证书审核环节和证书使用过程出现特殊情况（例如：私钥泄漏、申请强制吊销等）时才会主动联系您，否则不会以腾讯云合作厂商的身份主动联系您。

   **腾讯云合作的 CA 厂商信息如下，如收到非官方来源的联系，请务必谨慎核实。**

| 合作 CA 厂商 | 外呼电话号码（仅用于接听，请勿回拨） | 对外邮箱后缀 |
| --- | --- | --- |
| 亚数信息科技（上海）有限公司 | 021-54970081、021-54971631 | @trustasia.com |
| 上海市数字证书认证中心有限公司 | 021-36392785 | @ptc.sheca.com |
| 中金金融认证中心有限公司 | 010-87549888、010-87549666 | @cfca.com.cn |
| 沃通电子认证服务有限公司 | 0755-26027839 | @wotrus.com |

如果您无法判断收到信息的真实性，请您记录对方联系方式和信息详细内容，及时通过 提交工单 反馈给腾讯云。

对于冒充腾讯云欺骗客户的个人或组织，腾讯云保留追究法律责任的权利。

感谢您对腾讯云的信任与支持！

# 关于 TrustAsia 品牌根证书的调整公告

最近更新时间：2025-01-08 11:36:22

**尊敬的腾讯云 SSL 证书用户**

**腾讯云收到证书厂商对 TrustAsia 品牌调整根证书的通知，将于北京时间2025年1月14日对 TrustAsia 品牌的证书进行升级，涉及根证书的变更，详情如下：**

- **2025年1月14日之前，签发的 TrustAsia 证书均使用原来的根证书。**
- **2025年1月14日后，签发的 TrustAsia 证书会使用新根证书。**

> **说明：**
>
> 1. **如您的TrustAsia 证书用于 App 业务、IoT 终端等非 PC 浏览器，请您务必检查是否在终端预置过根证书。如您曾预置过根证书，需要您修改成系统自带的信任库做验证或下载最新的根证书和中间证书进行替换。**
> 2. **如您还需要使用 USERTrust RSA Certification Authority 根证书，可在腾讯云选购 Wotrus 品牌的 SSL 证书。**

| 原根证书 | 涉及的证书规格 | 新根证书 |
| --- | --- | --- |
| USERTrust RSA Certification Authority | TrustAsia 全系列证书（RSA 算法）<br>腾讯云免费证书 | DigiCert Global Root G2 |
| USERTrust ECC Certification Authority | TrustAsia 全系列证书（ECC 算法） | DigiCert Global Root G3 |
| AAA Certificate Services（交叉老根证书） | / | DigiCert Global Root CA(交叉老根证书) |

# 关于 DigiCert、TrustAsia 品牌根证书的调整公告

最近更新时间：2024-08-13 14:06:41

> **注意：**
> 为了给用户预留更多时间处理，调整计划由2024年9月1日顺延至2024年12月1日。

尊敬的腾讯云 SSL 证书用户
由于 Mozilla 信任库更新了其根证书信任策略，对全球所有 CA 的可信根证书生成后最少15年更换一次，超过时间的可信根将会逐步被 Mozilla 停止信任。因此 DigiCert 证书厂商将逐步停用旧根体系（G1）颁发 TLS/SSL 证书，并开始使用新根体系（G2）颁发 TLS/SSL 证书，以确保 TLS/SSL 证书在 Firefox 浏览器中继续受到信任。

> **说明：**
> - Digicert Global Root G2 使用 SHA256 签名算法，安全性将会得到提升。
> - GeoTrust、SecureSite 为 DigiCert 的子品牌，此次根证书调整涉及三款证书，分别为 GeoTrust 系列、SecureSite 系列、TrustAsia 免费证书，具体请参考下方根证书列表。

调整计划如下：

- 2024年12月1日之前，您签发的证书均可正常使用。
- 自2024年12月1日起，您申请的 SecureSite 系列、GeoTrust 系列、TrustAsia 免费证书将陆续使用新的根证书和新的中间证书进行签发。

如您的 SSL 证书用于 PC 端业务，此次调整对您的业务不会有影响。Digicert Global Root G2 新根证书已在主流操作系统、移动端、JDK 环境预埋，不会导致客户端版本不兼容情况。**如您的 SSL 证书用于 APP 业务、IoT 终端等非 PC 浏览器，请您务必检查是否在终端预置过根证书。如您曾预置过根证书，需要您修改成系统自带的信任库做验证或下载最新的根证书和中间证书进行替换。**

> **其他建议：**
> 如果您的客户端还需使用 DigiCert Global Root CA 根证书，可**通过** 提交工单 **申请签发交叉证书链。**交叉证书链可同时拥有 DigiCert Global Root CA 和 Digicert Global Root G2 的兼容性，需要在下单前 联系我们 。

## 涉及的根证书列表

| 原根证书 | Mozilla 不再信 | 涉及的证书规格 | 新根证书 |
| --- | --- | --- | --- |

| | 任时间 | | |
|---|---|---|---|
| DigiCert Global Root CA | 2026年04月15日 | • GeoTrust 的OV、EV 类型证书<br>• SecureSite 的 OV 类型证书 | DigiCert Global Root G2 |
| DigiCert High Assurance EV Root CA | 2026年04月15日 | SecureSite 的 EV、EV Pro 类型证书 | DigiCert Global Root G2 |
| AAA Certificate Services | 2025年04月15日 | TrustAsia 的 DV 类型证书 | USERTrust RSA Certification Authority |

## OV、EV 类型证书链变更信息

| 证书品牌 | 证书类型 | 原中级证书 | 原根证书 | 新中级证书 | 新根证书 |
|---|---|---|---|---|---|
| GeoTrust | 企业型（OV） | GeoTrust ECC CN CA G2 | DigiCert Global Root CA | GeoTrust G3 TLS CN ECC P-384 SHA384 2022 CA1 | DigiCert Global Root G3 |
| | 企业型（OV） | GeoTrust RSA CN CA G2 | DigiCert Global Root CA | GeoTrust G2 TLS CN RSA4096 SHA256 2022 CA1 | DigiCert Global Root G2 |
| | 增强型（EV） | GeoTrust EV RSA CA G2 | DigiCert Global Root G2 | GeoTrust EV G2 TLS CN RSA4096 SHA256 2022 CA1 | DigiCert Global Root G2 |
| | 增强型（EV） | DigiCert TLS Hybrid ECC SHA384 2020 CA1 | DigiCert Global Root CA | GeoTrust EV G3 TLS CN ECC P-384 SHA384 2022 CA1 | DigiCert Global Root G3 |
| SecureSite | 企业型（OV） | DigiCert Secure Site CN CA G3 | DigiCert Global Root CA | DigiCert Secure Site OV G2 TLS CN | DigiCert Global Root G2 |

| | | | | |
|---|---|---|---|---|
| | | | RSA4096 SHA256 2022 CA1 | |
| 企业型（OV） | DigiCert Secure Site ECC CN CA G3 | DigiCert Global Root CA | DigiCert Secure Site OV G3 TLS CN ECC P-384 SHA384 2022 CA1 | DigiCert Global Root G3 |
| 增强型（EV） | DigiCert Secure Site EV CN CA G3 | DigiCert High Assurance EV Root CA | DigiCert Secure Site EV G2 TLS CN RSA4096 SHA256 2022 CA1 | DigiCert Global Root G2 |
| 增强型（EV） | DigiCert Secure Site EV ECC CN CA G3 | DigiCert High Assurance EV Root CA | DigiCert Secure Site EV G3 TLS CN ECC P-384 SHA384 2022 CA1 | DigiCert Global Root G3 |
| 增强型专业版（EV Pro） | DigiCert Secure Site Pro EV CN CA G3 | DigiCert High Assurance EV Root CA | DigiCert Secure Site Pro EV G2 TLS CN RSA4096 SHA256 2022 CA1 | DigiCert Global Root G2 |
| 增强型专业版（EV Pro） | DigiCert Secure Site Pro EV ECC CN CA G3 | DigiCert High Assurance EV Root CA | DigiCert Secure Site Pro EV G3 TLS CN ECC P-384 SHA384 2022 CA1 | DigiCert Global Root G3 |
| 企业型专业版（OV Pro） | DigiCert Secure Site Pro CN CA G3 | DigiCert Global Root CA | DigiCert Secure Site Pro G2 TLS CN RSA4096 SHA256 2022 CA1 | DigiCert Global Root G2 |

| | | | | | |
|---|---|---|---|---|---|
| | 企业型专业版（OV Pro） | DigiCert Secure Site Pro ECC CN CA G3 | DigiCert Global Root CA | DigiCert Secure Site Pro G3 TLS CN ECC P-384 SHA384 2022 CA1 | DigiCert Global Root G3 |
| TrustAsia | 免费证书 | TrustAsia RSA DV TLS CA G2 | AAA Certificate Services | TrustAsia RSA DV TLS CA G3 | USERTrust RSA Certification Authority |
| | 免费证书 | TrustAsia ECC DV TLS CA G2 | AAA Certificate Services | TrustAsia ECC DV TLS CA G3 | USERTrust ECC Certification Authority |

**感谢您对腾讯云 SSL 证书的支持与关注，并敬请您谅解这一必要的调整。如果您有任何疑问，欢迎随时与我们沟通。**

# 关于腾讯云 SSL 接口新增鉴权的通知

最近更新时间：2024-06-06 14:42:31

尊敬的腾讯云 SSL 证书用户

为了给子账号提供更完善的 SSL 证书服务，腾讯云 SSL 证书计划**在北京时间2024年6月17日（周一）10:30对接口（接口名称：GetUserProject）进行服务升级，开启接口鉴权**。鉴权开启后，有权限的子账号才可在 SSL 证书控制台获取到项目信息。若子账号需要使用 GetUserProject 接口，需要主账号进行授权。若您的子账号不需要访问对应接口可忽略此公告。

> **说明：**
> 此次升级仅影响需要使用 GetUserProject 接口的子账号用户，主账号不受影响。

如果您存在子账号访问过对应的接口，后续子账号仍需访问对应接口，请参见 通过策略生成器创建自定义策略 为您的子账号授权，**否则接口新增鉴权后，您的子账号则无法访问该接口。**

感谢您对腾讯云的信赖与支持！

# 关于免费 SSL 证书策略调整通知

最近更新时间：2024-03-21 17:52:41

尊敬的腾讯云用户

为了给您带来更好的服务，腾讯云 SSL 证书计划**在北京时间2024年4月25日（周四）零点对免费 SSL 证书策略进行调整。**

## 一、免费 SSL 证书有效期由12个月缩短至3个月。

接收到厂商 关于免费证书有效期调整 的通知，**免费 SSL 证书有效期由12个月调整至3个月。**2024年4月25日零点以后，在腾讯云申请的免费 SSL 证书有效期由12个月调整至3个月（2024年4月25日以前签发的证书有效期不变）。

> **说明：**
> - 2024年4月25日零点之前申请的证书还处于审核中，审核通过后证书有效期仍为12个月，如果证书审核失败，重新提交申请后，证书有效期将变更为3个月。
> - 证书有效期自证书签发之日起计算。

## 二、免费 SSL 证书账号额度统一上调至50张。

为了方便企业用户更好地管理证书，满足更多用量的需求，2024年4月25日零点以后，**企业账号的免费 SSL 证书额度从10张上调至50张，个人账号免费 SSL 证书额度维持50张不变。**

## 三、免费证书取消腾讯云域名额度和全网域名额度限制

2024年4月25日零点以后，**腾讯云免费证书可以绑定任意域名，不再区分腾讯云域名额度和全网域名额度**，为您使用腾讯云 SSL 证书带来更大的灵活性和便利性。

## 四、免费证书取消域名额度限制。

2024年4月25日之前，同一个主域名最多为20个子域名申请免费证书，超出限制后无法申请。2024年4月25日零点以后，**申请的免费SSL证书无域名额度限制。**

感谢您对腾讯云的支持与关注！

# 关于“证书关联资源”功能升级通知

最近更新时间：2024-01-11 19:19:21

为了给您提供更完善的服务，腾讯云 SSL 证书将在北京时间**2024年1月25日10:30:00对“证书关联资源”功能进行升级**。升级后您可以在 SSL 证书 控制台很直观地查看 SSL 证书关联了哪些腾讯云服务和资源，方便您更便捷地更新SSL证书。

**由于此功能需要访问您账号下其他云服务资源，因此在使用此功能前，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（如您不使用该功能可忽略此公告消息）。

如您对SSL证书角色策略有疑问，请参见 SSL 证书角色策略配置说明 。

# 【子账号用户必看】关于腾讯云SSL接口新增鉴权的通知

最近更新时间：2023-03-08 18:01:12

尊敬的腾讯云 SSL 证书用户

为了给子账号提供更完善的 SSL 证书服务，腾讯云 SSL 证书计划对整体接口服务进行升级。腾讯云 SSL 证书于**2023年3月20日（周一）9:00-18:00对SSL 证书所有接口新增鉴权**（合计116个接口），如您的**子账号正在使用 SSL 证书接口请务必对所有 SSL 证书接口新增授权，否则将直接影响接口访问**。如您的子账号不需要访问对应接口可忽略此公告，感谢您对腾讯云的信赖与支持！

> ⚠ **注意：**
> 此次升级仅针对子账号用户，主账号用户不受影响。

如果您存在子账号访问过对应的接口，后续子账号仍需访问对应接口，请参见 通过策略生成器创建自定义策略 为您的子账号授权，**否则接口新增鉴权后，您的子账号则无法访问该接口。**

## 新增鉴权的接口列表

API 文档

# 关于《免费证书扩容包》产品调整的通知

最近更新时间：2023-01-04 11:53:31

为了给您提供更好的服务，腾讯云SSL证书将对《免费证书扩容包》进行改造，将于2023年1月5日暂停新订单购买。后续恢复新购时间，请以腾讯云SSL证书官方公告为准。在2023年1月5日前购买的用户可正常使用免费证书扩容包。

给您带来不便，敬请谅解！
感谢您对腾讯云SSL证书的支持与关注！

# 关于DigiCert品牌下SSL证书售价调整通知

最近更新时间：2022-12-26 11:26:37

**尊敬的腾讯云用户**

**由于接到DigiCert关于调整旗下品牌SSL证书价格的通知，腾讯云SSL证书将在北京时间2023年1月9日起调整DigiCert品牌下的SSL证书的售价。实际调整情况，请以证书购买页为准。**

**DigiCert品牌下的SSL证书售价调整**

| 品牌 | 对应腾讯云售卖品牌 | 腾讯云证书种类 | 腾讯云域名类型 | 调整前公开价格（元） | 调整后公开价格（元） | 价格变化（元） |
|---|---|---|---|---|---|---|
| GeoTrust | GeoTrust | 企业型（OV） | 单域名 | 2,850 | 2,778 | -72 |
| | GeoTrust | 企业型（OV） | 多域名（内含5个） | 5,580 | 11,490 | 5,910 |
| | GeoTrust | 企业型（OV） | 泛域名 | 6,850 | 7,278 | 428 |
| | GeoTrust | 增强型（EV） | 单域名 | 4,850 | 6,000 | 1,150 |
| | GeoTrust | 增强型（EV） | 多域名（内含5个） | 9,650 | 18,000 | 8,350 |
| DigiCert SecureSite | SecureSite | 企业型（OV） | 单域名 | 5,000 | 5,600 | 600 |
| | SecureSite | 企业型（OV） | 多域名（内含2个） | 10,000 | 11,200 | 1,200 |
| | SecureSite | 企业型（OV） | 泛域名 | 40,000 | 4,0000 | 0 |
| | SecureSite | 企业型专业型（OV Pro） | 单域名 | 8,000 | 8,992 | 992 |
| | SecureSite | 企业型专业型 | 多域名（内含2个） | 16,000 | 17,984 | 1,984 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | （OV Pro） | | | | |
| | SecureSite | 增强型（EV） | 单域名 | 8,000 | 8,992 | 992 |
| | SecureSite | 增强型（EV） | 多域名（内含2个） | 16,000 | 17,984 | 1,984 |
| | SecureSite | 增强型专业版（EV Pro） | 单域名 | 12,800 | 16,800 | 4,000 |
| | SecureSite | 增强型专业版（EV Pro） | 多域名（内含2个） | 25,600 | 33,600 | 8,000 |
| DigiCert代码签名证书 | 代码签名证书 | 普通版 | - | 4,550 | 6,000 | 1,450 |
| | 代码签名证书 | 增强型（EV） | - | 7,950 | 9,000 | 1,050 |

**相关信息**

**关于DigiCert品牌调整价格的官方通知**

# 关于中国市场规范产品名称及建议零售价格的通知

2022 年 2 月起，DigiCert 品牌的部分产品实施全球价格变更。基于服务、产品成本和行业标准状况，公司决定在保持竞争力目标的情况下，更新价格以反映我们提供的价值。我们承诺会持续提供世界上最高安全性的 TLS/SSL 证书，同时希望我们的服务和产品以最高的价值达到业界最高的标准。

为了更好地体现在售的各款 TLS/SSL 证书的价值定位，规范产品名称的使用，配合 DigiCert 全球价格调整策略（见附件一），特通知贵司在公开场所使用统一的中文产品名称及建议人民币零售价（见附件二），包括但不限于网站，邮件，App，小程序，纸质或电子版销售材料等。

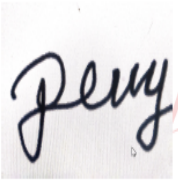
请于 12 月 1 日前完成相关改版工作，完成时间如有困难，请提前沟通协商。

注：促销价格可在此零售价格基础上进行打折，销售策略不受此影响。

DigiCert Website Security Technology(Beijing)Co.,Ltd

迪杰斯特网络安全技术（北京）有限公司

DigiCert China 2022



# TrustAsia 品牌根证书变更通知

最近更新时间：2022-10-11 14:29:32

## TrustAsia 品牌根证书变更通知

接 TrustAsia 品牌 CA 机构通知，自**2022年03月03日22:00:00**起，TrustAsia 根证书签发由 Digicert 根证书变更为 Sectigo 根证书。您可以理解为**2022年03月03日22:00:00**前申请的 TrustAsia 品牌 SSL 证书根证书由 Digicert 进行签发，**2022年03月03日22:00:00**后申请的 TrustAsia 品牌 SSL 证书根证书由 Sectigo 进行签发。
根证书变更后，基于 Sectigo 根证书支持中国区 OCSP（在线证书状态协议）节点特性，将在很大程度上解决中国区网站设置 HTTPS 后访问速度变慢问题。

**注意**

- 该变更对于已颁发使用的 SSL 证书没有任何影响。
- 变更后，原有的产品功能和服务保持不变。

# SSL 证书域名验证策略变更通知

最近更新时间：2022-10-11 14:29:32

根据 CA/Browser Forum 规定，自**2021年12月01日**起域名验证策略将会有以下重大变更：

**自2021年12月01日起，使用文件验证的域名，只能为当前被验证的域名签发 SSL 证书，不支持签发通配符 SSL 证书和其下级子域名 SSL 证书。**

目前，腾讯云 SSL 证书允许对主域名（例如 `dnspod.cn` ）进行域名验证即可，适用于通配符证书（例如 `*.dnspod.cn` 或 `*.sub.dnspod.cn` 等）和其下级所有子域名（例如 `sub.dnspod.cn` 或 `sub2.sub1.dnspod.cn` 等）。
但从2021年12月01日起，对于使用文件验证方式的域名，只能为当前被验证的域名签发证书。例如，使用文件验证方式验证域名 `dnspod.cn` ，则只能为 `dnspod.cn` 域名签发证书，不能为域名 `*.dnspod.cn` 或 `sub.dnspod.cn` 签发证书。

> **注意**
> 因以上规定，腾讯云将于**2021年11月21日**停止泛域名证书的文件验证方式，敬请知悉。

# SSL 证书与证书监控 SSLPod 联合说明

最近更新时间：2023-12-04 15:25:01

为了让您有更好的体验，现提供腾讯云证书管理控制台与证书监控 SSLPod 联合集成功能，可快速帮助您检查使用 SSL 证书时的证书健康问题。

> **说明**
> 当您遇到问题需要咨询时，您可以直接通过 在线客服 进行提问，腾讯云工程师7 × 24小时在线为您提供服务。

## SSL 证书与证书监控 SSLPod 联合集成

1. 登录 腾讯云证书管理控制台，单击左侧菜单栏的**我的证书**，即可进入 “证书列表” 管理页面。
2. 在 “证书列表” 管理页面中，单击 证书 ID，即可进入证书详情页。
3. 您可以通过证书详情页面查看证书监控状态：


## 证书状态说明

| 图标 | 状态说明 | 操作 |
| --- | --- | --- |

| | | |
|---|---|---|
|  | 目前该 SSL 证书状态异常 | 单击**查看监控报告**，即可跳转至健康报告页查看详情。 |
|  | 该域名目前还未开启证书监控 | 单击**免费开通**，即可快速对该证书进行监控。 |
|  | 目前该 SSL 证书状态良好 | 单击**查看监控报告**，即可跳转至健康报告页查看详情。 |
|  | 该域名正在使用其它证书 | 单击**查看监控报告**，即可跳转至健康报告页查看详情。 |

# 多年期 SSL 证书与自动审核更新说明

最近更新时间：2022-10-11 14:29:32

为了让您有更好的体验，腾讯云证书管理控制台 新增多年期证书购买和我的资料自动审核功能，可帮助您解决证书申请和续期需重新申请的问题。本文档将对多年期证书和我的资料自动审核功能进行简要说明。
如果在使用过程中有任何疑问、建议或意见，请 联系我们，感谢您的使用。

## 功能概述

> **说明**
> 具体操作以控制台显示为准。

| 模块 | 说明 |
| --- | --- |
| 我的资料 | 我的资料页可新增管理企业、管理人信息以及域名信息审核。包含以下功能：<br>• **企业信息管理**：可在我的资料页下管理企业信息，如新增、修改、删除等操作。<br>• **域名信息管理**：可在我的资料页对应的企业信息下管理域名，如新增、修改、删除、验证域名所有权等操作。 |
| 多年期证书 | 您可以登录 腾讯云 SSL 证书购买页，购买特定品牌的多年期证书，腾讯云将在前一个证书有效期到期前为您签发下一张证书，解决 CA 机构减少证书有效期的困扰。 |

# 腾讯云 SSL 证书控制台更新说明

最近更新时间：2022-10-11 14:29:32

为了让您有更好的体验，腾讯云证书管理控制台 已全面升级，在原 SSL 证书控制台的基础上进行了合并与优化。新版控制台新增证书概览、操作记录、快速上手等功能模块，并与证书监控 SSLPod 协同使用，提供更全面更便捷的配置和管理。本文档将对新版 SSL 证书控制台的使用进行简要说明。
如果在使用过程中有任何疑问、建议或意见，请 联系我们，感谢您的使用。

## 功能概述

| 模块 | 说明 |
| --- | --- |
| 证书概览 | SSL 证书概览页可用于 SSL 证书申请状态与监控状态的查看与进行相关操作。包含以下功能：<br>• 申请状态：可快速查看待提交、验证中、已签发、审核失败的 SSL 证书，并进行相关操作。<br>• 监控状态：可快速查看访问正常、访问异常、过期预警的 SSL 证书监控信息并查看对应的 SSLPod 监控报告。 |
| 我的证书 | 我的证书页面主要用于查看申请中、已签发、已过期的 SSL 证书查看与证书管理。包含但不限于以下功能：<br>• 查看申请中、已签发、已过期的证书信息。<br>• 购买证书。<br>• 申请免费证书。<br>• 上传已有证书。<br>• 对证书进行相关管理，如提交申请资料，重颁发证书、续费等。 |
| 操作记录 | 操作记录主要用于对现有 SSL 证书的相关操作记录查看。包含以下功能：<br>• 支持导出 CSV 与 JSON 格式的操作记录。<br>• 对操作记录进行相关条件筛选。 |
| 证书监控 | 主要用于 SSL 证书产品与监控 SSLPod 产品的协同使用，提供更便捷的管理与使用。 |

# 腾讯云即日起支持 DNSPod 品牌国密标准（SM2）SSL 证书购买通知

最近更新时间：2022-10-11 14:29:33

国密是国家商用密码的简称，是国家密码局认定的国产密码算法。而国产密码算法是保障我国网络安全自主可控的重要基础，腾讯云 DNSPod 品牌国密标准（SM2）证书支持 SM2 国产密码算法和国密安全协议，可以实现高强度 SSL 加密连接及服务器身份认证，适合对国密合规性有要求的网站。更多详情请查看：国密证书介绍 。

## 腾讯云 DNSPod 品牌国密标准（SM2）证书

- **域名型（DV）**：域名型加密 SSL 证书，支持在国密浏览器中显示安全锁。对域名所有权进行验证，满足绑定多域名和泛域名的需求，快速颁发，经济实惠，保护网站数据安全，适合个人，中小企业应用。
- **企业型（OV）**：企业级加密 SSL 证书，支持在国密浏览器中显示安全锁及单位名称。对申请公司单位做严格的身份审核验证，保护内外部网络上敏感数据传输，是中小型企业应用、电商等服务的最佳选择。
- **增强型（EV）**：增强型加密 SSL 证书，支持在国密浏览器中直观显示绿色地址栏及单位名称。对申请者做最严格的身份审核验证，信任等级最高，适合大型企业、金融等机构平台。

## 购买流程

请您登录腾讯云账号，并进入 SSL 证书购买页 进行购买。

# 关于 CA 机构于2020年9月1日起停止签发为期两年 SSL 证书的通知

最近更新时间：2023-05-22 16:54:54

由于苹果和谷歌根存储政策的更改，自2020年9月1日起，政策禁止使用有效期超过13个月（397天）新颁发的 SSL/TLS 证书。因此，自2020年9月1日起，全球 CA 认证机构不再签发2年期 SSL 证书，腾讯云将于2020年8月25日关闭2年期证书购买服务，如有2年期证书购买需求，请于服务下线前完成申请签发。
常见问题如下：

## 这次政策更改带来了什么变化?

由于苹果和谷歌根存储政策的变化，自2020年9月1号开始，所有新的 SSL/TLS 证书的最长有效期不得超过13个月。

## 此变更何时生效?

2020年9月1号。

## 我刚刚购买了有效期为2年的 SSL 证书，2020年9月1号之后会被信任吗?

在2020年9月1号之前颁发且有效期大于397天的 SSL 证书将继续受到信任，使用不受影响。

## 更改生效后，重颁发现有的2年期证书会怎么样?

如果您在9月1号之后重颁发现有的2年期证书，我们需要把重颁发出来的新证书有效期限制为397天。

**说明**

- 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
- 如您使用过程中遇到产品相关问题，您可咨询 在线咨询 寻求帮助。

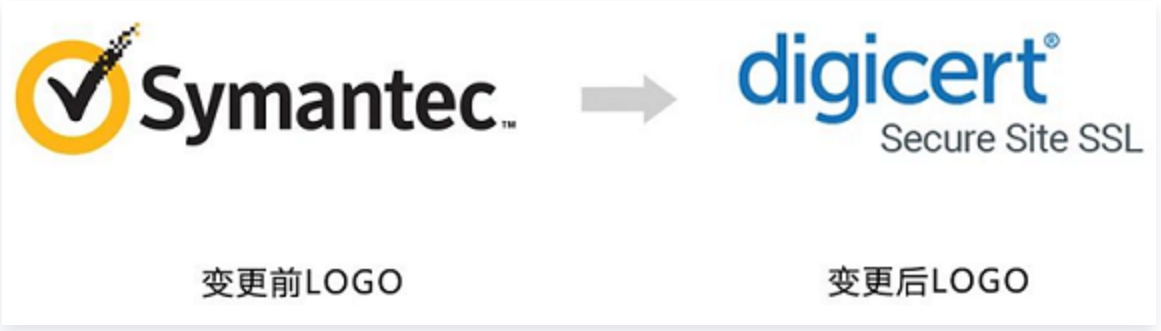
# 关于 Symantec SSL 证书品牌名于2020年4月30日停止使用的通知

最近更新时间：2022-10-11 14:29:33

接原厂通知，Symantec SSL 证书品牌名将于2020年4月30日停止使用，您可以理解为该日期是 Symantec 品牌用于 SSL 证书的最后一天。

## 本次更新点

1. Symantec 品牌 SSL 证书更名为 DigiCert Secure Site 品牌 SSL 证书。如下图所示：




2. 诺顿安全认证签章同步进行了更新。如下图所示：


**注意**

- 此次更名对于证书交付和使用流程没有任何影响。
- 更名后，原有的产品功能和服务保持不变的基础上，Secure Site 品牌新增 Pro 版本支持抗量子算法功能。

## 原厂公告

以下是原厂公告：

Greetings APAC partners,

As part of the migration the Symantec logo cannot be used after 30 April 2020. However, the phrase DigiCert (formerly Symantec) or similar can be used in marketing collaterals and to an extent on product descriptions. Please keep in mind not to over-use the wording and ensure that it is not heavily emphasised.

If there's any further questions on this please email me directly.

Please stay safe during this period.

Regards,

Albert Cheng
Channel Marketing Manager, APAC
O +61 0 8866 8043 | M +61 423 585 290

digicert®

**说明**

- 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
- 如您使用过程中遇到产品相关问题，您可咨询 在线咨询 寻求帮助。

# 关于私钥泄露导致被厂商吊销 SSL 证书的情况说明

最近更新时间：2022-10-11 14:29:33

证书签发机构（CA）会在 GitHub、SourceForge 等项目代码托管平台进行自动检测，检测到私钥泄露后机构会通知用户并在24小时后进行证书吊销操作。
为了保护您的网站及信息安全，请于申请完证书后妥善保管您的私钥。请勿将私钥上传至公网，以免出现证书被吊销或发生信息泄露等事件。

**说明**

- 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
- 如您使用过程中遇到产品相关问题，您可咨询 在线咨询 寻求帮助。

# 关于免费域名型（DV）SSL 证书的申请额度限制通知

最近更新时间：2024-09-09 17:51:11

**说明：**
该额度限制已于2024年4月25日解除，请参考最新的免费证书规则：关于免费 SSL 证书策略调整通知 。

由于 CA 机构和证书代理商策略调整，自2018年1月1日起，同一主域最多只能申请20张亚洲诚信品牌免费型 DV 版 SSL 证书（二级域名及其子域名均属于同一主域，例如，`tencent.com`、`ssl.tencent.com`、`ssl.ssl.tencent.com` 都属于同一主域）。之前已颁发的证书在有效期内使用不受影响。若您的业务因此次调整受限，建议您购买泛域名型 SSL 证书。

**注意：**

- 自2022年9月1日起，1个腾讯云UIN账号申请免费证书的额度由50张下调至20张。
- 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
- 如您使用过程中遇到产品相关问题，您可使用 在线咨询 寻求帮助。

# 关于 Let's Encrypt 根证书将于2021年9月30号过期说明

最近更新时间：2022-10-11 21:38:51

Let's Encrypt 品牌 SSL 证书根证书于**2021年9月30日**停用旧版根证书（Root CA）。若您的网站已部署 Let's Encrypt 品牌的 SSL 证书并在过期前未及时更新，将导致您的网站面临不受计算机、设备或 Web 浏览器信任，网站兼容性降低，甚至部分网站不能访问的现象，将会影响您的使用。如下图所示：


为避免您的业务受到影响，建议您尽快自查正在使用的 Let's Encrypt 品牌 SSL 证书是否存在该问题。您可通过证书监控 SSLPod 进行检查并查看报告详情。操作详情参见：证书监控 SSLPod 操作指南 。

**说明**

- 若存在以上问题，建议您尽快更新为其他品牌的 SSL 证书，从源头上避免 Let's Encrypt 根证书过期带来的一系列问题。
- 因腾讯云未售卖颁发 Let's Encrypt 品牌证书，若您使用腾讯云颁发的 SSL 证书，可忽略该说明。