

SSL 证书 证书申请



腾讯云

【 版权声明 】

©2013–2025 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 】

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

证书申请

证书提交资料流程

- DV (域名型) SSL 证书提交流程

- GeoTrust 等通用品牌证书提交流程

- Wotrus 品牌证书提交流程

- DNSPod 品牌国密标准 (SM2) OV 与 EV 型 SSL 证书材料提交流程

免费 SSL 证书使用指南

- 免费 SSL 证书概述

- 免费 SSL 证书申请流程

通过 API 接口申请证书

证书申请

证书提交资料流程

DV (域名型) SSL 证书提交流程

最近更新时间：2024-12-06 14:39:22

操作场景

域名型 (DV) SSL 证书在购买成功后, 需要进行相关材料提交。证书购买流程请参见 [SSL 证书购买流程](#)。
CA 机构认证审核通过后, 将会正式颁发证书, 您可下载证书进行安装。

前提条件

1. 登录 [SSL 证书控制台](#), 选择并进入待提交管理页面。
2. 选择已购买的证书行, 单击提交资料。

操作步骤

⚠ 注意:

- 不同域名类型的证书, 需填写信息和填写界面略有不同。
- 本操作以 Wotrus 品牌域名型 (DV) 多域名证书为例。其他品牌证书以控制台实际填写界面为准。

步骤1: 填写域名

根据实际需求, 选择 CSR 生成方式 (择一)。

- 选择 “在线生成 CSR” 方式, 执行 [在线生成 CSR 的操作](#) (推荐使用在线生成 CSR, 由平台生成和管理您的私钥和公钥证书文件, 避免私钥文件丢失)。
- 选择 “粘贴 CSR” 方式, 执行 [粘贴 CSR 的操作](#) (自行上传, 不可生成私钥)。

在线生成 CSR

1. 填写域名信息。如下图所示：

1 提交资料 > 2 选择验证方式 > 3 验证域名 > 4 签发证书

CSR生成 在线生成 粘贴CSR
推荐使用在线生成CSR，由平台生成和管理您的私钥和公钥证书文件，避免私钥文件丢失

算法选择 RSA算法 ECC算法

密钥长度 2048 4096

证书绑定域名
即绑定证书的域名，请填写单个域名。例如tencent.com、ssl.tencent.com。

其他域名 ⓘ
请输入证书绑定的其他域名，注意不要与通用名称重复，提交CA机构后将无法修改

私钥密码(选填)
为了保障私钥安全，目前不支持密码找回功能，请您牢记私钥密码。
如需部署腾讯云负载均衡、CDN等云服务，请勿填写私钥密码。

公司信息

选择方式 已有公司 新增公司信息

公司名称

城市

地址

电话

管理人信息

姓名

部门

职位

电话

邮箱

联系人信息

选择方式 与管理人相同 自定义联系人信息

[下一步](#)

主要参数信息如下：

- **算法选择：**根据您的实际情况选择证书加密算法。
- **密钥长度：**根据您的实际情况选择证书密钥长度。
- **证书绑定域名：**填写绑定证书的单个域名。例如 `tencent.com`、`ssl.tencent.com`。
- **其他域名：**填写证书绑定的其他域名，不能与通用名称重复，提交 CA 机构后将无法修改。

① 说明：
单个域名证书无此参数。

- **私钥密码：**可选填，填写后不可更改也不支持密码找回，请牢记私钥密码。

① 说明：
如需部署腾讯云负载均衡、CDN 等云服务、请勿填写私钥密码。

2. 填写公司信息。

- **已有公司：**选择**已有公司**，可直接使用公司信息。
- **新增公司信息：**请如实填写公司名称（全称），公司部门，公司所在城市与地址以及公司座机号码。

3. 填写管理人信息。

- **已有管理人：**选择**已有管理人**，可直接使用管理人信息。
- **新增管理人信息：**请如实填写管理人姓名，职位，电话以及邮箱。

4. 填写联系人信息，可勾选和管理人相同。

5. 单击**下一步**，进入 [步骤2](#)。

粘贴 CSR

1. 将已准备好的 CSR 信息粘贴至文本框中，输入“域名信息”，并填写公司信息（可选择“已有公司”）、管理人信息（可选择“已有管理人”）以及联系人信息（可勾选和管理人相同）。如下图所示：

1. 在“验证域名”页面，请根据页面提供的信息进行域名验证操作。例如，您选择的是 DNS 验证方式，将会展示以下信息。如下图所示：



- 申请域名型（DV）1年期的证书：
 - **DNS 验证**：域名验证操作请参考 [DNS 验证](#)。
 - **文件验证**：域名验证操作请参考 [文件验证](#)。
- 申请 TrustAsia 品牌域名型（DV）（泛域名2年期或3年期）的证书：
 - **自动 DNS 验证**：域名验证操作请参考 [自动 DNS 验证](#)。
 - **自动文件验证**：域名验证操作请参考 [自动文件验证](#)。

2. 域名验证操作完成后，可单击[查看域名验证状态](#)，查看域名验证操作是否成功。

说明：

- DNSPod 品牌国密标准（SM2）DV 型证书，首次域名验证通过后，该域名验证将保留13个月。
- 13个月内该域名以相同公司名称申请 DNSPod 品牌国密标准（SM2）DV 型证书，将无需执行域名验证。

步骤4：签发证书

CA 机构认证审核通过后，将会正式签发证书，您可下载证书进行安装。

GeoTrust 等通用品牌证书提交流程

最近更新時間：2025-04-29 16:53:22

操作場景

GeoTrust、SecureSite、GlobalSign、TrustAsia、CFCA 品牌的企业型（OV）、增强型（EV）证书、企业型专业版（OV Pro）、增强型专业版（EV Pro）证书需要审核企业信息。

前提条件

1. 已购买 SSL 证书。
2. 登录 [SSL 证书控制台](#)，在我的证书页面。
3. 选择状态为待提交的证书，单击提交资料。



操作步骤

⚠ 注意：

不同域名类型的证书，需填写信息略有不同。本操作以单域名证书为例。

步骤1：设置基本参数

根据实际需求，选择 CSR 生成方式（择一）。

- 选择“在线生成 CSR”方式，由平台生成和管理您的私钥和公钥证书文件，避免私钥文件丢失。（推荐使用）
- 选择“粘贴 CSR”方式，由您自行上传 CSR，平台不生成私钥。

复用配置	<input type="checkbox"/> 开启自动续费时自动沿用旧证书的配置（新签发的证书沿用旧证书的CSR文件、私钥及私钥密码） 新证书签发后依旧需要重新替换旧证书，推荐您使用证书托管功能实现自动替换。 了解更多
CSR生成	<input checked="" type="radio"/> 在线生成 <input type="radio"/> 粘贴CSR 推荐使用在线生成CSR，由平台生成和管理您的私钥和公钥证书文件，避免私钥文件丢失。 了解更多
算法选择	<input checked="" type="radio"/> RSA算法 <input type="radio"/> ECC算法 RSA对浏览器和客户端的兼容性更好，但对网站服务器的性能开销更大；ECC加密效率更高，服务器性能开销小但兼容性略弱。 了解更多
密钥长度	<input checked="" type="radio"/> 2048 <input type="radio"/> 4096
签名算法	<input checked="" type="radio"/> RSA 256 <input type="radio"/> SHA 384

其他参数信息如下：

- **算法选择：**勾选所需证书加密算法，推荐 RSA 算法。
- **密钥长度：**勾选所需证书密钥长度，推荐2048。

步骤2：填写域名信息

⚠ 注意：

证书绑定域名后无法再次修改域名，请务必确认无误后再填写。

证书绑定域名	<input type="text" value="请输入证书要绑定域名"/>
即绑定证书的域名，请填写单个域名（一经绑定无法修改，如需更换域名需要重新购买证书）。例如tencent.com、ssl.tencent.com。 请注意：tencent.com只赠送www.tencent.com，不包含ssl.tencent.com，需单独申请。	
私钥密码(选填)	<input type="password"/>
为了保障私钥安全，目前不支持密码找回功能，请您牢记私钥密码。 如需部署腾讯云负载均衡、CDN等云服务，请勿填写私钥密码。 什么是私钥密码	

- **证书绑定域名**：填写绑定证书的单个域名。例如 `tencent.com`、`ssl.tencent.com`。
 - **单域名证书**：输入具体域名。
 - **通配符（泛域名）证书**：输入通配符格式域名（如`*.tencent.com`）。
- **其他域名**：填写证书绑定的其他域名，不能与通用名称重复，提交 CA 机构后将无法修改。
- **私钥密码**：可选填，填写后不可更改也不支持密码找回。如设置了私钥密码，下载证书后（仅限 pfx、jks 格式）需要使用私钥密码才可解压。

步骤3：完善企业信息

1. 填写公司信息。

- **已有公司**：选择已有公司，可直接使用公司信息。
- **新增公司信息**：请如实填写公司名称（全称），公司所在城市与地址以及公司座机号码。

2. 填写管理人信息。

- **已有管理人**：选择已有管理人，可直接使用管理人信息。
- **新增管理人信息**：请如实填写管理人姓名，部门，职位，电话以及邮箱。

3. 填写联系人信息，可勾选和管理人相同。

The screenshot shows a form with three main sections: 1. 公司信息 (Company Information) with radio buttons for '已有公司' (Selected) and '新增公司信息' (New company info), and input fields for '公司名称', '城市', '地址', and '电话'. 2. 管理人信息 (Manager Information) with radio buttons for '已有管理人' (Selected) and '新增管理人信息' (New manager info), and input fields for '姓名', '部门', '职位', '电话', and '邮箱'. 3. 联系人信息 (Contact Information) with radio buttons for '与管理人相同' (Selected) and '自定义联系人信息' (Custom contact info).

步骤4：选择域名验证方式

证书签发需要完成域名验证，即添加一条域名解析记录（证书未签发前，请勿删除解析记录），添加之前需要您先选择域名验证方式。

The screenshot shows a progress bar with four steps: 1. 提交资料 (Submitted), 2. 选择验证方式 (Selected), 3. 通过人工审核 (Passed), 4. 签发证书 (Issued). Below the progress bar, there is a blue banner with a tip: '如何申请 Wotrus 品牌 OV 与 EV 型证书? 查看申请流程'. The main content area has three radio button options: '自动添加DNS验证' (Selected, with a '强烈推荐!' label), 'DNS验证' (Recommended), and '文件验证'. Each option has a brief description and a '详细说明' link. At the bottom, there are '上一步' and '下一步' buttons, and a link for '体验吐槽 & 遇到问题? 加入SSL证书交流群'.

- **自动添加 DNS 验证**：腾讯云注册的域名或解析托管在 DNSPod 的域名，系统自动为域名添加一条对应的解析记录，无需人工操作。
- **DNS 验证**：非腾讯云注册或解析未托管在 DNSPod 的域名，需要手动前往域名解析平台添加一条解析记录，请参见 [DNS 验证](#)。

- **文件验证**：域名对应的网站根目录下创建指定的文件验证域名所属权，操作复杂，验证速度较慢，请参见 [文件验证](#)。

步骤5：选择企业信息审核方式

ⓘ 企业信息审核方式说明：

证书 CA 机构需要验证企业信息，各品牌企业信息审核方式如下：

- DNSPod、Wotrus 无需企业信息确认函，通过预留的电话和邮箱即可。
- GlobalSign、CFCA 品牌的证书每次都需要上传企业信息确认函。
- GeoTrust、SecureSite、TrustAsia 品牌的证书企业信息有效期最长1年，超出有效期需重新审核，审核方式可选择年报电话或登记电话、年报邮箱或登记邮箱。

方式一：企业年报电话审核（以 Geotrust 品牌的证书为例）

The screenshot shows the '企业信息验证' (Company Information Verification) step. The '企业年报电话审核' (Annual Report Telephone Verification) option is selected and marked as '推荐' (Recommended). The instructions state that the CA institution will verify the contact information through various channels. A list of channels is provided: 1. Annual report phone number (referencing the National Enterprise Credit Information Publicity System), 2. Official website registration phone number (for domain names used on official websites), 3. Baidu Map registration phone number, and 4. Other contact information from public platforms. A '常见问题' (FAQ) section on the right addresses questions about review time (3-5 working days), how to fill in the seat number, whether all content is mandatory, and whether every page of the confirmation letter needs a stamp. A '下一步' (Next Step) button is at the bottom left, and a link to '体验吐槽 & 遇到问题? 加入SSL证书交流群' is at the bottom right.

方式二：企业年报邮箱审核（以 Geotrust 品牌的证书为例）

The screenshot shows the '企业信息验证' (Company Information Verification) step. The '企业年报邮箱审核' (Annual Report Email Verification) option is selected and marked as '推荐' (Recommended). The instructions state that the CA institution will verify the contact information via email. A list of channels is provided: 1. Annual report email (referencing the National Enterprise Credit Information Publicity System), 2. Official website registration email (for domain names used on official websites), 3. Baidu Map registration email, and 4. Other contact information from public platforms. A '常见问题' (FAQ) section on the right addresses questions about review time (3-5 working days), how to fill in the seat number, whether all content is mandatory, and whether every page of the confirmation letter needs a stamp. A '下一步' (Next Step) button is at the bottom left, and a link to '体验吐槽 & 遇到问题? 加入SSL证书交流群' is at the bottom right.

方式三：企业信息确认函审核（以 GlobalSign 品牌的证书为例）

⚠ 注意：

2025年4月20日起，Digicert 旗下品牌（GeoTrust、SecureSite）以及 TrustAsia 品牌的 SSL 证书不支持通过企业信息确认函进行企业信息审核。

1. 单击下载**确认函模板**，进行确认函信息补充填写。如下图所示：

Wotrus 品牌证书提交流程

最近更新时间：2024-10-29 16:20:02

操作场景

Wotrus 品牌证书企业型（OV）与增强型（EV）SSL 证书在购买成功后，需要进行相关材料提交。证书购买流程请参考 [购买流程](#)。

说明：

Wotrus企业型（OV）、增强型（EV）证书无需上传企业信息，通过邮箱验证即可完成签发。

前提条件

- 已购买 SSL 证书。
- 登录 [SSL 证书控制台](#)，在**我的证书**页面。
- 选择状态为待提交的证书，单击**提交资料**。



操作步骤

注意：

不同域名类型的证书，需填写信息略有不同。本操作以企业型（OV）单域名证书为例。

步骤1：设置基本参数

根据实际需求，选择 CSR 生成方式（择一）。

- 选择“在线生成 CSR”方式，由平台生成和管理您的私钥和公钥证书文件，避免私钥文件丢失。（推荐使用）
- 选择“粘贴 CSR”方式，由您自行上传 CSR，平台不生成私钥。

复用配置	<input type="checkbox"/> 开启自动续费时自动沿用旧证书的配置（新签发的证书沿用旧证书的CSR文件、私钥及私钥密码） 新证书签发后依旧需要重新替换旧证书，推荐使用证书 证书托管 功能实现自动替换。 了解更多
CSR生成	<input checked="" type="radio"/> 在线生成 <input type="radio"/> 粘贴CSR 推荐使用在线生成CSR，由平台生成和管理您的私钥和公钥证书文件，避免私钥文件丢失。 了解更多
算法选择	<input checked="" type="radio"/> RSA算法 <input type="radio"/> ECC算法 RSA对浏览器和客户端的兼容性更好，但对网站服务器的性能开销更大；ECC加密效率更高，服务器性能开销小但兼容性略弱。 了解更多
密钥长度	<input checked="" type="radio"/> 2048 <input type="radio"/> 4096
签名算法	<input checked="" type="radio"/> RSA 256 <input type="radio"/> SHA 384

其他参数信息如下：

- 算法选择：**勾选所需证书加密算法，推荐 RSA 算法。
- 密钥长度：**勾选所需证书密钥长度，推荐2048。

步骤2：填写域名信息

注意：

证书绑定域名后无法再次修改域名，请务必确认无误后再填写。

证书绑定域名

即绑定证书的域名，请填写单个域名（一经绑定无法修改，如需更换域名需要重新购买证书）。例如tencent.com、ssl.tencent.com。
请注意：tencent.com只赠送www.tencent.com，不包含ssl.tencent.com，需单独申请。

私钥密码(选填)

为了保障私钥安全，目前 不支持密码找回 功能，请您牢记私钥密码。
如需部署腾讯云负载均衡、CDN等云服务，请勿填写私钥密码。[什么是私钥密码](#)

- **证书绑定域名：**填写绑定证书的单个域名。例如 `tencent.com`、`ssl.tencent.com`。
 - **单域名证书：**输入具体域名。
 - **通配符（泛域名）证书：**输入通配符格式域名（如`*.tencent.com`）。
- **其他域名：**填写证书绑定的其他域名，不能与通用名称重复，提交 CA 机构后将无法修改。
- **私钥密码：**可选填，填写后不可更改也不支持密码找回。如设置了私钥密码，下载证书后（仅限 pfx、jks 格式）需要使用私钥密码才可解压。

步骤3：完善企业信息

1. 填写公司信息。

- **已有公司：**选择已有公司，可直接使用公司信息。
- **新增公司信息：**请如实填写公司名称（全称），公司所在城市与地址以及公司座机号码。

2. 填写管理人信息。

- **已有管理人：**选择已有管理人，可直接使用管理人信息。
- **新增管理人信息：**请如实填写管理人姓名，部门，职位，电话以及邮箱。

3. 填写联系人信息，可勾选和管理人相同。

公司信息

选择方式 已有公司 新增公司信息

公司名称

如当前信息不符合要求，请新增公司信息或前往 [我的资料](#) 管理

城市

地址

电话

管理人信息

选择方式 已有管理人 新增管理人信息

姓名

部门

职位

电话

邮箱

联系人信息

选择方式 与管理人相同 自定义联系人信息

步骤4：选择域名验证方式

证书签发需要完成域名验证，即添加一条域名解析记录（证书未签发前，请勿删除解析记录），添加之前需要您先选择域名验证方式。



- **自动添加 DNS 验证：**腾讯云注册的域名或解析托管在 DNSPod 的域名可选择，系统自动为域名添加一条对应的解析记录，无需人工操作。
- **DNS 验证：**非腾讯云注册或解析未托管在 DNSPod 的域名，需要手动前往域名解析平台添加一条解析记录，请参见 [DNS 验证](#)。
- **文件验证：**域名对应的网站根目录下创建指定的文件验证域名所属权，操作复杂，验证速度较慢，请参见 [文件验证](#)。

步骤5：完成域名验证

1. 请根据“验证域名”页面的提示信息，进行域名所有权验证。例如，您选择的是手动 DNS 验证方式，将会展示以下信息，请您至对应的域名解析商平台添加解析。如下图所示：



2. 域名验证操作完成后，可单击查看域名验证状态，查看域名验证操作是否成功。



步骤6：企业信息审核

收到订单后，CA 机构会给您预留的邮箱发送两封邮件，需要您按邮件指引，完成企业信息验证。同时，CA 机构还有可能给您致电沟通证书审核相关事项，请保持联系方式畅通并耐心等待。

说明：验证邮件发件人通常为“WoTrus Customer Service”，点击邮件里面的链接，输入邮件里面的验证码即可完成验证。（请务必仔细阅读邮件内容，确认内容无误后再点击验证，以防诈骗或钓鱼邮件）

② 机构已发送一封电子邮件至您证书联系人的邮箱 (****@****.com)，请点击邮件中链接进行授权验证

- 如未收到邮件，请检查垃圾邮件文件夹是否拦截，或确认电子邮件地址是否正确
- 授权邮件不能重新发送，也不支持修改地址，如需更换新地址需[放弃订单或退款](#)，在[我的资料](#)中修改管理人信息，并重新提交

步骤7：证书签发完成

CA 机构认证审核通过后，将会正式签发证书，您可下载证书进行安装，您还需要将证书部署到云资源上，方可开启 HTTPS 服务。

DNSPod 品牌国密标准 (SM2) OV 与 EV 型 SSL 证书材料提交流程

最近更新时间: 2024-08-29 14:42:01

操作场景

DNSPod 品牌国密标准 (SM2) 的企业型 (OV) 与增强型 (EV) SSL 证书在购买成功后, 需要进行相关材料提交。证书购买流程请参考 [购买流程](#)。CA 机构认证审核通过后, 将会正式颁发证书, 您可下载该证书进行安装。

前提条件

1. 登录 [SSL 证书控制台](#), 选择并进入待提交管理页面。
2. 选择已购买到的国密证书行, 单击提交资料。

操作步骤

⚠ 注意:

不同域名类型的证书, 需填写信息略有不同。本操作以企业型 (OV) 多域名证书为例。

步骤1: 填写域名

根据实际需求, 选择 CSR 生成方式 (择一)。

- 选择 “在线生成 CSR” 方式, 执行 [在线生成 CSR 的操作](#) (推荐使用在线生成 CSR, 由平台生成和管理您的私钥和公钥证书文件, 避免私钥文件丢失)。
- 选择 “粘贴 CSR” 方式, 执行 [粘贴 CSR 的操作](#) (自行上传, 不可生成私钥)。

在线生成 CSR

1. 填写域名信息。如下图所示:

📌 说明

如 “已有公司” 与 “已有管理人” 信息未符合您当前申请证书资料的要求, 您可请前往 [SSL 证书控制台](#) > [我的资料](#) 进行管理。

1 提交资料 > 2 选择验证方式 > 3 上传确认函 > 4 验证域名 > 5 通过人工审核 > 6 签发证书

CSR生成 在线生成 粘贴CSR
推荐使用在线生成CSR，由平台生成和管理您的私钥和公钥证书文件，避免私钥文件丢失

证书绑定域名 ✓
即绑定证书的域名或者IP，请填写单个域名或者IP，例如tencent.com、ssl.tencent.com、example.ssl.tencent.com、1.1.1.1。

其他域名 ① ✓
您还有0个域名输入。请输入证书绑定的其他域名或者IP，注意不要与通用名称重复，提交CA机构后将无法修改

私钥密码(选填) 密码不能小于6位且不能包含空格 ✓
为了确保私钥安全，目前不支持密码找回功能，请您牢记私钥密码。
如需部署腾讯云负载均衡、CDN等云服务，请勿填写私钥密码。

公司信息

选择方式 已有公司 新增公司信息

公司名称 请输入公司名称

城市 中国大陆 北京市 北京市

地址 不必重复省份信息

电话 区号 座机号/手机号码

管理人信息

姓名 名 姓

部门 请输入部门名称

职位 请输入职位

电话 请输入电话

邮箱 请输入邮箱

联系人信息

选择方式 与管理人相同 自定义联系人信息

[下一步](#)

主要参数信息如下：

- **证书绑定域名**：填写绑定证书的单个域名或外网 IP。例如 tencent.com、ssl.tencent.com、example.ssl.tencent.com、1.1.1.1。
- **其他域名**：填写证书绑定的其他域名或外网 IP，不能与通用名称重复，提交 CA 机构后将无法修改。
- **私钥密码**：可选填，填写后不可更改也不支持密码找回，请牢记私钥密码。

2. 填写公司信息。

- **已有公司**：选择已有公司，可直接使用公司信息。
- **新增公司信息**：请如实填写公司名称（全称），公司部门，公司所在城市与地址以及公司座机号码。

3. 填写管理人信息：

- **已有管理人**：选择已有管理人，可直接使用管理人信息。

1. 在“上传确认函”页面，单击**下载确认函模板**，进行申请书信息补充填写。如下图所示：



- 2. 完成申请书填写后，加盖公章后扫描或拍摄清晰照片上传。
- 3. 单击**上传**，上传确认函。

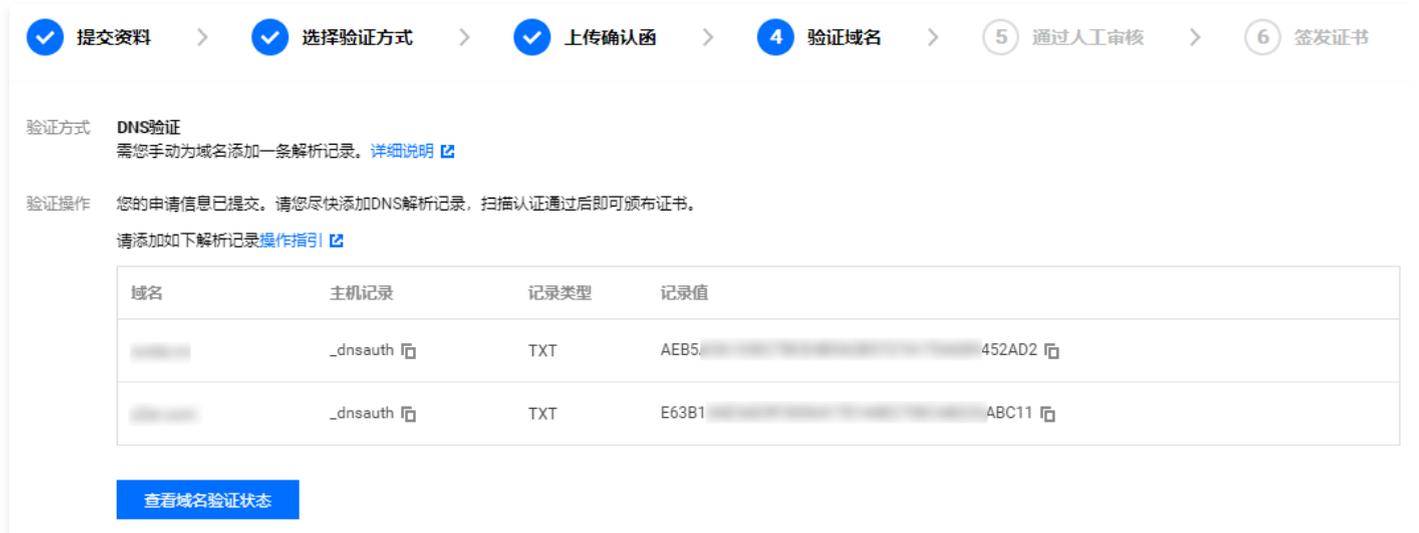
说明：

- 申请书支持 .jpg、.gif、.pdf 格式，大小在1.4M以内。
- 申请书上传后，不支持重新上传，请确保上传正确。

4. 单击**下一步**，进入“验证域名”页面。

步骤4：验证域名

1. 请根据“验证域名”页面的提示信息，进行域名所有权验证。例如，您选择的是手动 DNS 验证方式，将会展示以下信息。如下图所示：



- **DNS 验证：**域名验证操作请参考 [DNS 验证](#)。
 - **文件验证：**域名验证操作请参考 [文件验证](#)。
2. 完成域名验证操作后，可单击**查看域名验证状态**查看验证操作是否成功。

步骤5：通过人工审核

域名验证成功后，将进入人工审核阶段，人工审核通过后将正式签发证书。

说明：

- 首次域名验证通过后，该域名验证将保留13个月。13个月内该域名以相同公司名称申请 DNSPod 品牌国密标准（SM2）OV 与 EV 型 SSL 证书，将不执行域名验证的操作。
- 需人工审核及域名认证均通过后，才可颁布证书。
- OV 型证书人工审核时间为3 - 5个工作日，EV 型证书人工审核时间为5 - 7个工作日，请您耐心等待。
- 若已申请过该类型证书，且申请成功，再次以相同信息申请，则不需要人工审核。

步骤6：签发证书

正式签发证书后，您可下载证书进行安装。

免费 SSL 证书使用指南

免费 SSL 证书概述

最近更新时间：2024-11-27 17:28:52

免费 SSL 证书概述

腾讯云平台无偿提供的一款 SSL 证书，主要用于前期测试使用，供用户在网站建设前期业务需要 HTTPS 通信时使用。

免费 SSL 证书和正式 SSL 证书的区别

⚠ 注意：

正式证书的兼容性优于免费证书，为了您的业务稳定，正式项目请务必使用正式证书。单击前往 [选购正式证书](#)。

证书特性	免费证书	正式证书
域名额度	无限制	无限制
证书品牌	TrustAsia	<ul style="list-style-type: none">SecureSite (DigiCert)DNSPodGeoTrustGlobalSignTrustAsiaWoTrus
支持绑定泛域名（通配符）	不支持	支持
支持绑定IP	不支持	支持
支持多域名	不支持	支持
安装咨询服务	不支持	支持
售后服务	不支持	支持

免费证书额度规则

一个腾讯云账号最多只能申请50张免费证书。

免费 SSL 证书使用限制

- 免费证书仅支持绑定一个单域名，不支持绑定通配符域名或者 IP。不支持后缀为特殊词的域名申请免费证书。此类特殊词包括但不限于：`.edu`、`.gov`、`.org`、`.ru`、`.jp`、`.pay`、`.bank`、`.live`和`.nuclear`；
- 免费证书不支持人工技术支持或安装指导，请根据指导文档完成证书的安装部署。

免费 SSL 证书申请步骤

- 登录 [SSL 证书控制台](#)，进入 [我的证书](#) 页面，并单击 [申请免费证书](#)。
- 按需填写申请内容，单击 [提交申请](#)，进行 [域名验证](#)，验证完成后将在一个工作日内完成审核，审核结果将以短信、邮件及站内信的方式通知。如下图所示：

📌 说明：

详细的申请流程可参考 [免费 SSL 证书申请流程](#)。



如何升级成正式证书

免费 SSL 证书不支持续费，建议仅作为测试使用。为获得更高的安全等级并享有人工客服支持，可通过以下两种方式升级为付费版 SSL 证书。

方式一：前往证书控制台进行升级

1. 登录 [SSL 证书控制台](#)，进入“我的证书”管理页面，选择需要升级的证书，单击升级。如下图所示：



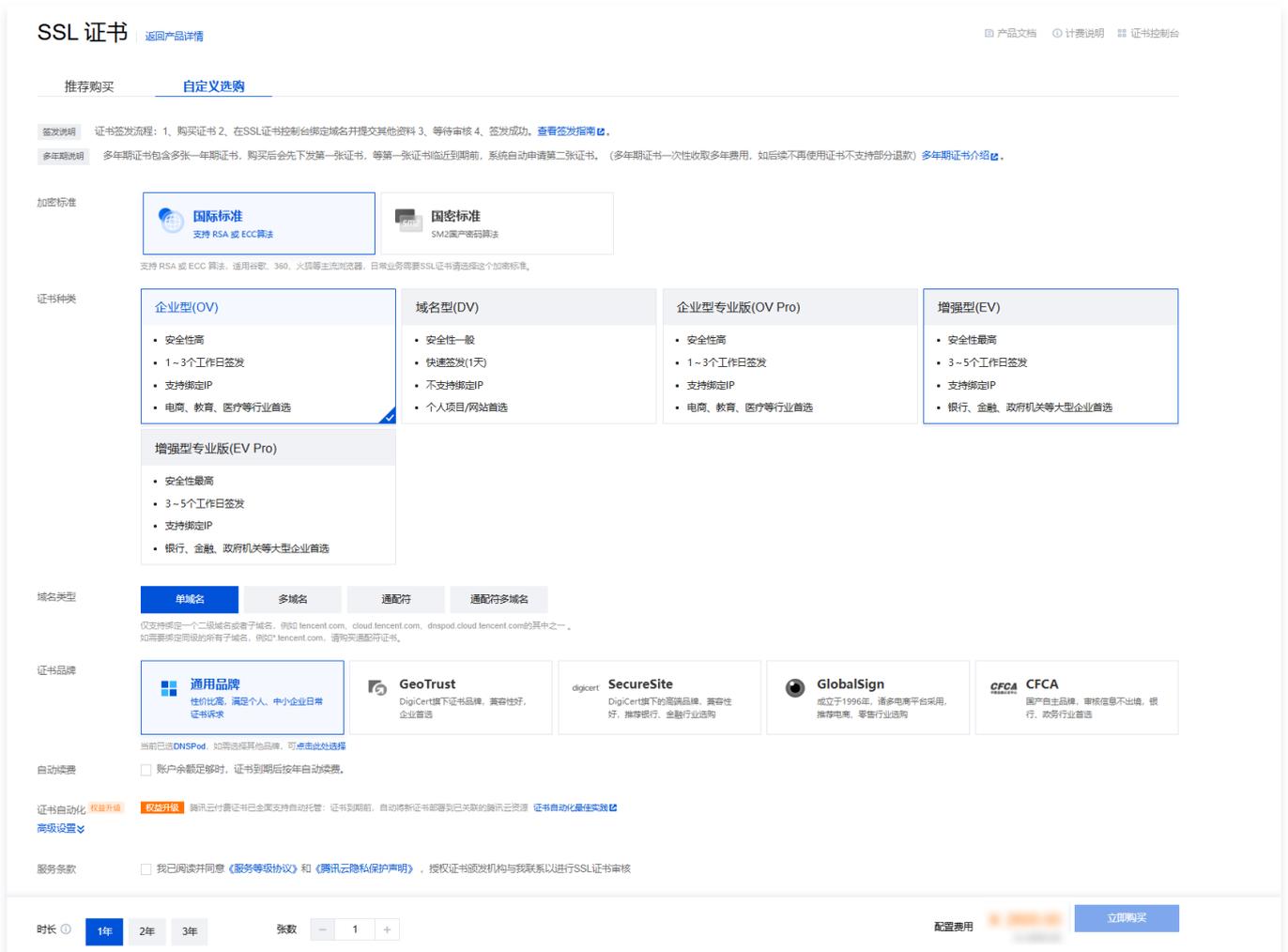
2. 在弹出的窗口，确认证书规格后，单击前往支付。如下图所示：



方式二：前往证书购买页付费证书

以购买自定义配置付费证书为例。

1. 在 [SSL证书购买页](#) 购买付费证书，详细信息请参见官网售卖提供的参数对比。如下图所示：



- 根据您的行业以及实际需求选择相应的证书种类及证书品牌。证书种类请参见 [各 SSL 证书类型案例](#)，证书品牌请参见 [SSL 证书品牌介绍](#)。
- 按需选择域名类型及支持的域名数目，域名类型说明如下图所示：

域名类型	描述	注意事项
单域名	只支持绑定1个域名,可以支持绑定二级域名 <code>tencent.com</code> 、或是三级域名 <code>example.tencent.com</code> 。	不支持绑定二级域名下的所有子域名。 域名级数最多可以支持100级。 绑定 <code>www.tencent.com</code> 域名（子域名是 <code>www</code> ）的 SSL 证书，会同时支持 <code>tencent.com</code> 二级域名。
多域名	单个证书可以绑定多个域名，最多可以支持数量以控制台展示为准。	SecureSite 多域名证书的价格即按域名数目进行叠加。 Geo Trust、TrustAsia、GlobalSign、Wotrus、DNSPod 多域名证书除默认支持域名数量外,附加域名再另叠加计价。
泛域名	支持绑定一个且只有一个泛域名,泛域名只允许添加一个通配符。	例如, <code>*.tencent.com</code> , <code>*.example.tencent.com</code> , 最多支持100级。 例如, <code>*.*.tencent.com</code> 多个通配符的泛域名是不支持的。 绑定 <code>*.tencent.com</code> 域名（必须是二级泛域名）的 SSL 证书，会同时支持 <code>tencent.com</code> 二级域名。
通配符多域名	支持绑定多个泛域名。	例如, <code>*.tencent.com</code> 、 <code>*.ssl.tencent.com</code> 、 <code>*.another.com</code> , 共计3个泛域名，包含同一级的全部子域名，最多可以支持数量以控制台展示为准。

- 按需选择证书年限。
- 单击**立即购买**，前往订单管理页面并单击**提交订单**完成付款即可。

免费 SSL 证书申请流程

最近更新时间：2024-11-27 17:28:52

注册账号

腾讯云平台申请证书首先需要注册腾讯云账号并且完成实名认证。

1. 新用户请单击 [腾讯云官网](#) 右上角的[免费注册](#)，进入注册页面。
2. 请您 [注册腾讯云账号](#)，即可登录腾讯云控制台。
3. 完成 [实名认证](#)，方可继续申请证书。

申请免费证书

④ 说明：

- 免费证书仅提供二级域名及其子域名证书申请，不支持 IP 与泛域名申请。例如 `dnspod.cn`、`docs.dnspod.cn`。
- 亚洲诚信范围内（不一定在腾讯云申请）的同一主域名最多只能申请20张免费证书，申请时请注意该域名是否在其他服务商平台存在亚洲诚信下的证书，避免申请达到上限无法申请。更多详情请参见 [免费证书名额相关问题](#)。
- 免费证书到期后如需继续使用证书，请重新申请并安装。

1. 登录 [SSL 证书控制台](#)，进入我的证书页面，并单击[申请免费证书](#)。
2. 填写证书申请表单，如下图所示：

④ 免费证书仅供测试使用，由于免费证书的兼容性不如正式证书，若将免费证书应用在正式项目中可能存在潜在风险从而影响业务，出于对业务稳定的考虑，建议您[购买正式证书](#)使用。由于免费证书是无偿提供，因此腾讯云SSL证书不提供免费证书的技术支持或安装指导，如您申请中遇到问题，请查阅[免费证书使用指南](#)。

1 提交证书申请 > 2 验证域名

证书额度 [已用 1 / 共60张](#)
证书吊销或正常过期24小时后，会释放占用免费证书的额度[免费证书额度说明](#)

证书绑定域名 *
tencent.com只赠送www.tencent.com，不包含ssl.tencent.com，需单独申请；如需绑定泛域名（例如 *.tencent.com）或者绑定IP，请购买付费证书，[前往购买](#)

域名验证方式 * 手动DNS验证 自动DNS验证 文件验证
手动前往域名解析平台添加一条解析记录（不影响域名使用），证书签发成功后即可删除记录

申请邮箱 *

证书有效期 90天
接到厂商通知，2024年4月25日起，腾讯云新签发的免费证书有效期调整为90天，策略生效前申请的证书有效期仍为12个月。[关于免费证书策略调整通知](#)

[更多](#)

[提交申请，进行域名验证](#) [返回列表](#)

[常见问题](#) [更多](#)

- 证书过期后要怎么办？
证书过期后请重新申请，签发后将新证书重新部署才可生效。
- 新证书已经部署了，为什么网站还是显示不安全？
建议尝试以下方案：1、先清除浏览器缓存 2、检查服务器443端口、80端口是否开启 [查看详情](#)
- 证书签发需要多久呢？
域名验证完成后，2个小时内可签发，如果长时间没签发，可以检查下域名验证是否添加有误。
- 已添加了域名解析值，但未检测到？
请先确认解析值是否添加正确，添加无误后还需等待1~5分钟让域名解析生效。 [查看更多](#)

[加入SSL证书交流群](#)
产品咨询 问题反馈



[有问题，产品体验您说了算](#)

- 证书绑定域名：请填写单个域名。例如 `tencent.com`、`ssl.tencent.com`。
- 域名验证方式：

④ 说明：

- 自动DNS验证：验证方法请参见 [自动添加 DNS](#)。
若申请的域名已成功托管在 [云解析 DNS 控制台](#)，可支持自动添加 DNS。
- 手动DNS验证：验证方法请参见 [DNS 验证](#)。
- 文件验证：验证方法请参见 [文件验证](#)。

- 申请邮箱：请输入您的邮箱地址。
- 算法选择：勾选所需证书的加密算法。加密算法具体内容请参见 [RSA 加密算法与 ECC 加密算法的区别？](#)
- 证书备注名：可选，请输入证书的备注名称，不可超过200字。
- 私钥密码：可选，为了保障私钥安全，目前不支持密码找回功能，请您牢记私钥密码。

⚠ 注意：

如需部署腾讯云负载均衡、CDN 等云服务，请勿填写私钥密码。

- 标签：请选择您的标签键和标签值，方便您管理腾讯云已有的资源分类。

说明：

如需添加标签，请参见 [管理标签](#)。

- **所属项目：**请选择您证书所属项目，方便您通过项目管理您的证书。

3. 根据**验证操作**提示，完成域名身份验证，并单击**完成**。如下图所示：



4. 域名验证通过后，CA 机构将在24小时内完成签发证书操作，请您耐心等待。

注意：

提交域名未通过 CA 机构安全审核，具体原因请参见 [安全审核失败原因](#)。

下载和部署

完成域名审核后，颁发的证书即可单击**下载**到本地进行安装部署或部署到腾讯云相关云服务上。相关操作请参见 [如何选择 SSL 证书安装部署类型](#)？

相关问题

- [免费 SSL 证书名额相关问题](#)
- [SSL 证书配置的 TXT 解析是否可以删除？](#)
- [忘记私钥密码怎么办？](#)
- [免费 SSL 证书一直在待验证怎么办？](#)
- 更多问题，请参见 [热点问题](#)。

通过 API 接口申请证书

最近更新时间：2024-10-22 17:13:32

概述

腾讯云 SSL 证书提供 API 接口申请 SSL 付费证书，本文档将指导您如何使用 SSL 证书 API 接口申请付费证书的具体流程。

前提条件

已注册腾讯云账号。

证书 API 接口申请流程

由于证书品牌及类型原因，证书 API 接口申请流程具有一定差异，请根据您的实际需求申请证书的品牌和类型。

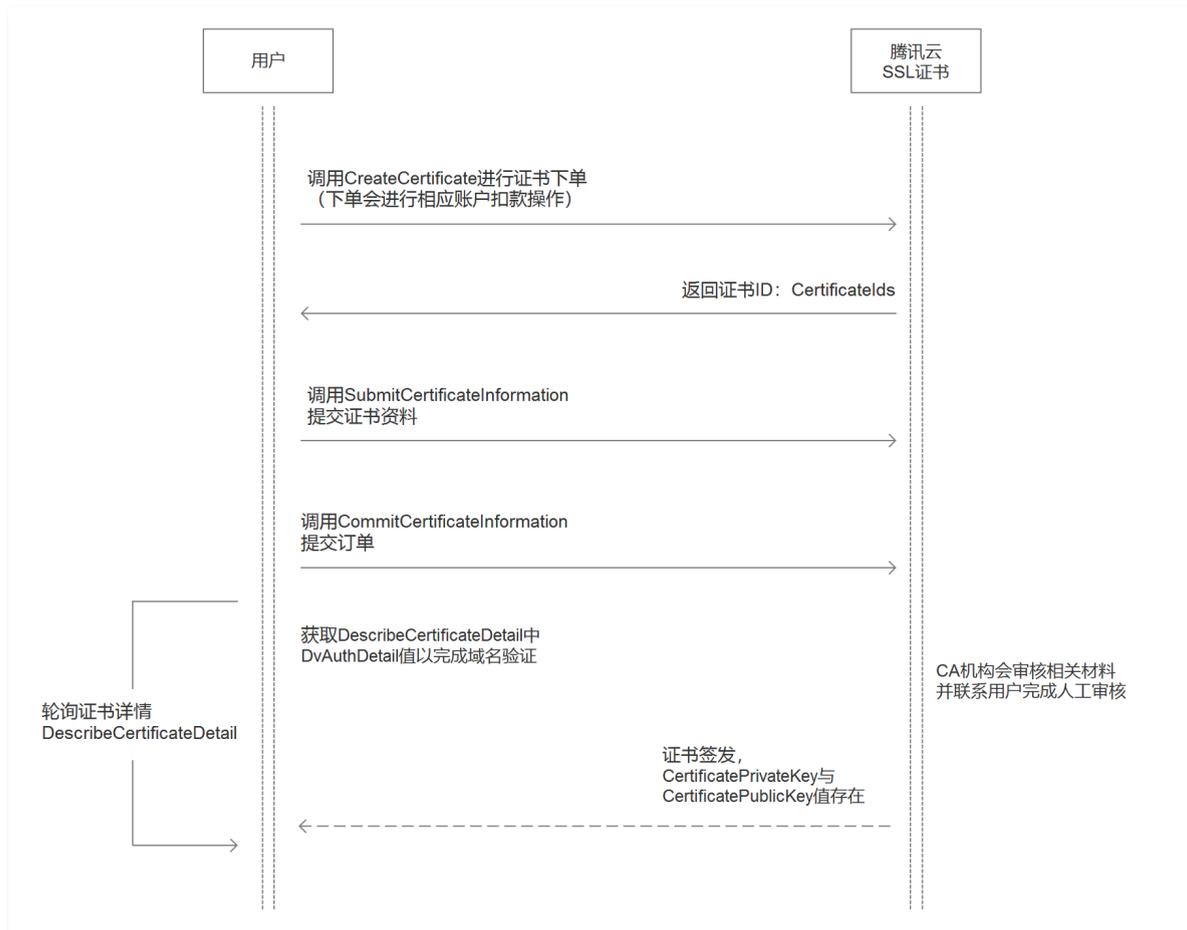
说明：

- API 调用方式请参见：[请求结构](#)。
- 相关密钥创建方式请参见：[签名方法 v3](#)。

付费 DV 型证书 API 接口申请流程

请您按照流程图调用相关 SSL 证书接口，CA 机构会审核相关材料并联系您完成人工审核。

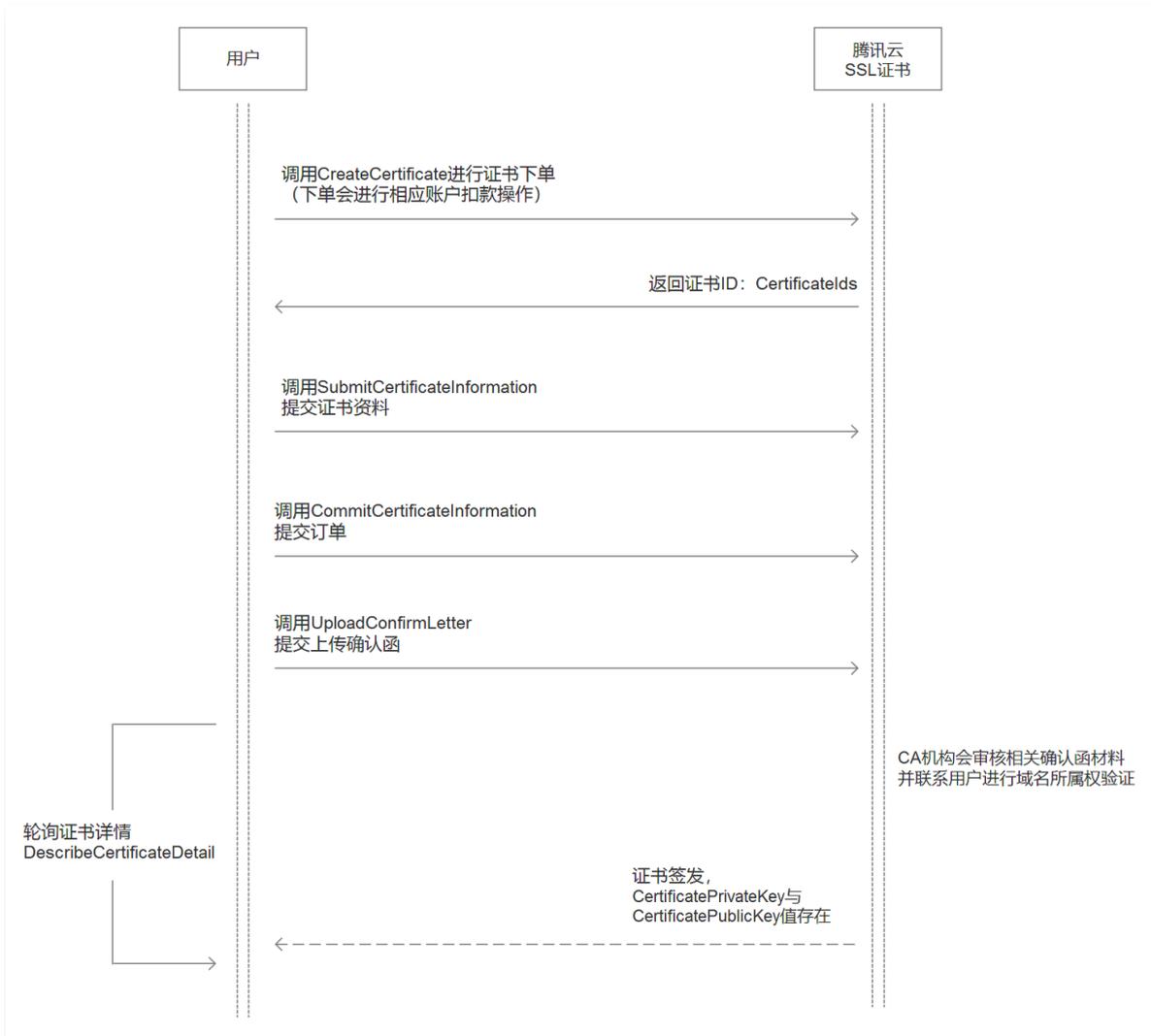
证书签发后可通过下载证书（DownloadCertificate）接口进行证书下载操作。如下图所示：



GeoTrust、SecureSite、TrustAsia、GlobalSign 品牌 OV/EV 型证书 API 接口申请流程

请您按照流程图调用相关 SSL 证书接口，CA 机构会审核相关确认函材料并联系您完成域名验证操作。具体验证操作请参见 [DNS 验证](#) 或 [文件验证](#)。

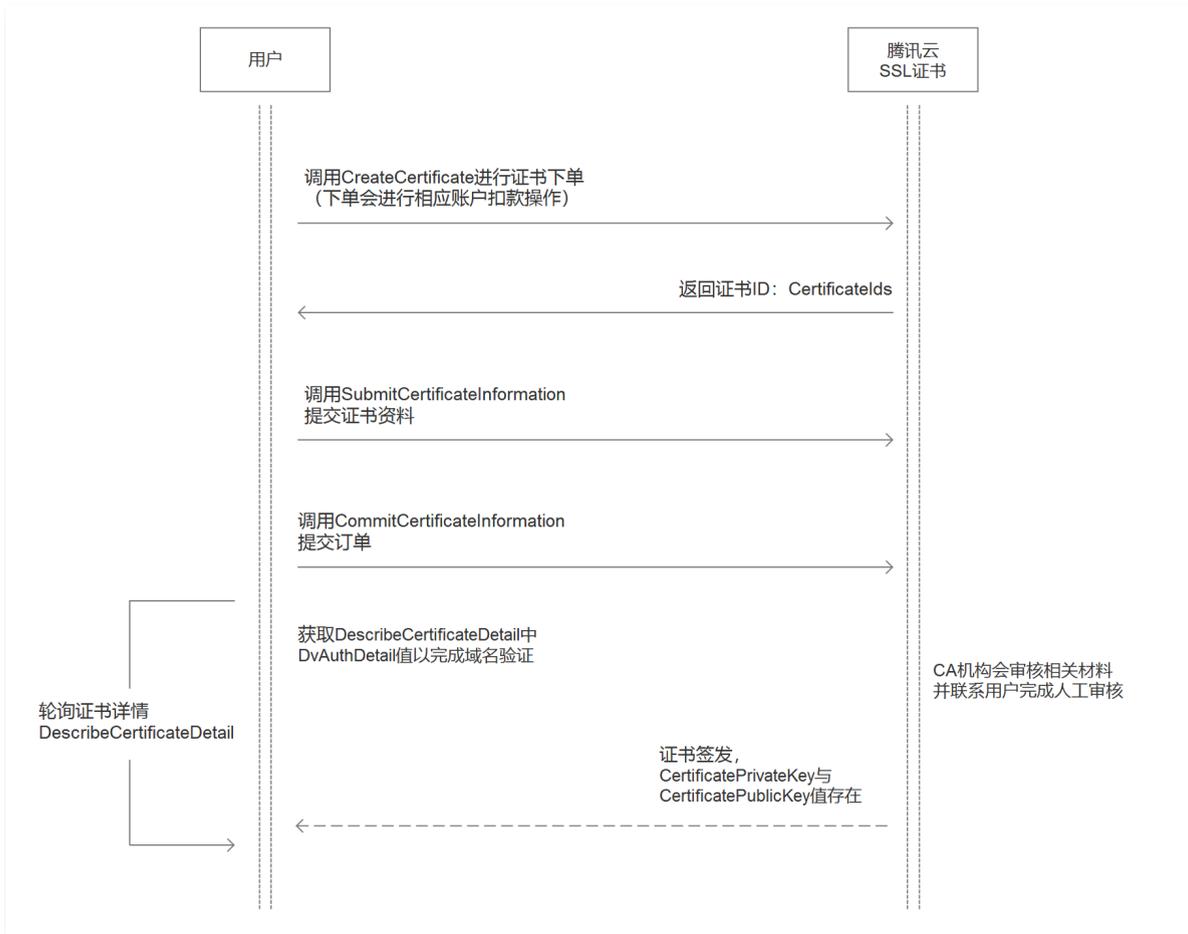
证书签发后可通过下载证书（DownloadCertificate）接口进行证书下载操作。如下图所示：



WoTrus 品牌付费 OV/EV 型证书 API 接口申请流程

请您按照流程图调用相关 SSL 证书接口，CA 机构会审核相关材料并联系您完成人工审核。

证书签发后可通过下载证书（DownloadCertificate）接口进行证书下载操作。如下图所示：



DNSPod (国密标准) 品牌付费 OV/EV 型证书 API 接口申请流程

请您按照流程图调用相关 SSL 证书接口，CA 机构会审核相关确认函材料并联系您完成域名验证操作。具体验证操作请参见 [DNS 验证](#) 或 [文件验证](#)。证书签发后可通过下载证书 (DownloadCertificate) 接口进行证书下载操作。如下图所示：

说明：
DNSPod (国密标准) 证书采用了国密 SM2 算法，现阶段仅支持特定 Web 服务器部署安装证书，特定浏览器访问相应域名。具体详情请参见 [DNSPod 品牌证书国密标准 \(SM2\) 介绍](#)。

