ALIBABA CLOUD

# 阿里云

## SSL证书服务

## 证书管理

文档版本：20200915

阿里云

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式 | 说明 | 样例 |
| --- | --- | --- |
| 危险 | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 危险<br>重置操作将丢失用户配置数据。 |
| 警告 | 该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 警告<br>重启操作将导致业务中断，恢复业务时间约十分钟。 |
| 注意 | 用于警示信息、补充说明等，是用户必须了解的内容。 | 注意<br>权重设置为0，该服务器不会再接受新请求。 |
| 说明 | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 | 说明<br>您也可以通过按Ctrl+A选中全部文件。 |
| > | 多级菜单递进。 | 单击**设置**> **网络**> **设置网络类型**。 |
| **粗体** | 表示按键、菜单、页面名称等UI元素。 | 在**结果确认**页面，单击**确定**。 |
| `Courier字体` | 命令或代码。 | 执行 `cd /d C:/window` 命令，进入Windows系统文件夹。 |
| *斜体* | 表示参数、变量。 | `bae log list --instanceid`<br>*Instance_ID* |
| [] 或者 [a\|b] | 表示可选项，至多选择一个。 | `ipconfig [-all\|-t]` |
| {} 或者 {a\|b} | 表示必选项，至多选择一个。 | `switch {active\|stand}` |

# 目录

# 1.概述

阿里云SSL证书服务提供多种类型和品牌的证书。

## 证书购买

有关如何购买证书和选择证书类型、品牌等详细内容，请参见证书选型和购买。

## 证书到期续费

证书有效期为1~2年，到期前需续费购买。续费的具体操作，请参见到期续费。

> 说明 如果您的现有证书即将过期，您未通过到期续费功能更新证书，而是通过重新购买的方式签发新证书，那么您新购买证书的有效期将无法叠加您的旧证书过期前未使用的有效期。

## SSL证书类型对比

证书根据不同的验证级别，分为以下三类：

- 域名型SSL（DV SSL）
- 企业型SSL（OV SSL）
- 增强型SSL（EV SSL）

> 说明
>
> - 目前仅DigiCert提供免费型数字证书，该证书仅支持绑定一个域名。
> - 除专业版OV SSL证书外，DigiCert还提供增强型OV SSL证书。增强型OV SSL证书采用ECC椭圆曲线算法。

根据保护域名的数量需求，SSL证书分为以下三类：

- 单域名版：只保护一个域名，例如www.abc.com或者login.abc.com之类的单个域名。
- 多域名版：一张证书可以保护多个域名，例如同时保护www.abc.com、www.bcd.com、pay.efg.com等多个域名。
- 通配符版：一张证书保护该通配符域名同一级的所有子域名，域名个数不限，例如*.abc.com，即保护abc.com主域名下的所有子域名。

# 2.吊销证书

当您无需再使用SSL证书，或者出于安全因素考虑，可以在阿里云证书控制台随时申请吊销证书。

## 背景信息

**证书吊销**是指已经签发的证书从签发机构处注销。证书吊销后将失去加密效果，浏览器不再信任该证书。阿里云SSL证书服务支持对阿里云签发的证书进行吊销处理，上传的第三方证书不支持吊销。

> **注意** 证书提交吊销申请后，您将无法在SSL证书控制台查看或下载该证书，请谨慎操作。

阿里云SSL证书吊销后可从SSL证书控制台删除，已签发的证书如果未被吊销不支持删除。关于吊销和删除的区别，请参见吊销证书和删除证书有什么区别？

> **说明**
>
> - 已签发证书如果需要申请退款，必须在证书签发后的30个自然日内先完成吊销流程，否则无法退款。证书**签发超过30个自然日或签发30天个自然日内无法完成吊销流程**，不支持退款。
> - 由于CA中心处理证书吊销申请最长需要5个工作日，如果您需要吊销证书并申请退款，请务必在证书签发后30个自然日内**提前至少5个工作日**在阿里云SSL证书控制台申请吊销。如果没有预留足够的吊销处理时间，可能导致您的证书签发超过30个自然日，最终无法退款，给您造成损失。

## 操作步骤

1. 登录阿里云SSL证书控制台。
2. 在左侧导航栏单击**概览**。
3. 在**SSL证书**页面，定位到需要吊销的证书实例，单击**吊销**。


4. 在**证书吊销**页面中，选择吊销原因并单击**确定**。
5. 在吊销确认提示框中单击**继续吊销**。
6. 完成邮件确认。提交证书吊销申请后，CA中心会向您的邮箱（即申请证书时填写的**申请人邮箱**）发送一封确认邮件，您需要及时登录该邮箱并确认吊销证书。

   > **说明** 当您提交证书吊销申请后，只有OV、EV证书才会收到CA中心发送的确认邮件，申请吊销DV证书无需邮件确认。

   当您完成邮件确认后，证书吊销成功。

## 相关文档

SSL证书退款说明

到期续费

# 3.上传已有证书

您可使用阿里云SSL证书服务上传您所拥有的其他证书，在SSL证书控制台对您的全部证书进行统一管理。

## 证书说明

SSL证书服务只支持上传PEM编码格式的证书文件，其他编码格式的证书需要转化成PEM编码文件后才能上传。证书转化详细操作，请参见转化。

PEM编码文件包括以下两种类型的扩展名：

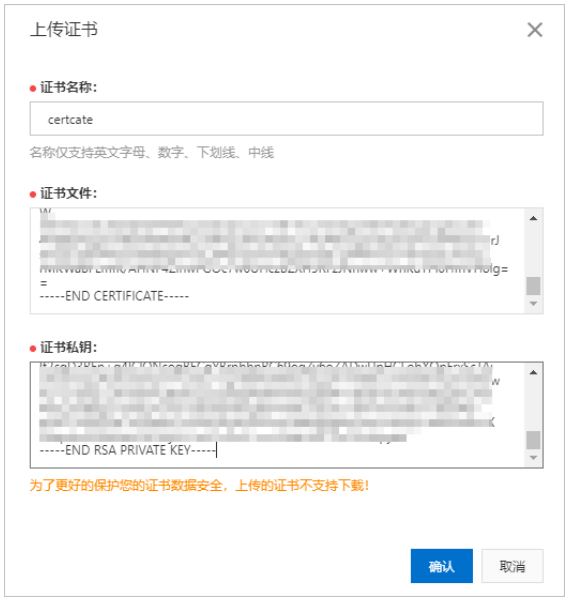
- .pem
- .crt

> 说明 SSL证书控制台不支持下载上传的证书。

## 操作步骤

1. 登录阿里云SSL证书控制台。
2. 在SSL证书页面，单击证书列表上方的上传证书。


3. 在上传证书对话框中，按要求输入证书名称，并将您的证书文件（文件格式或后缀为.pem或.crt）内容拷贝至证书文件对话框中，将证书私钥文件（文件格式或后缀为.key）内容拷贝至证书私钥对话框中。




> **说明** 建议您使用文本工具（notepad或notepad ++）打开您的证书文件和私钥文件。

4. 单击**确认**完成证书上传。
   您可以在上传证书中找到您刚上传的证书。上传的证书也可以部署到云产品。

## 后续步骤

您可以将已签发的证书部署到云产品。具体操作指导请参见已签发证书部署到阿里云产品。

# 4.常见问题

## 4.1. 吊销证书和删除证书有什么区别？

阿里云SSL证书服务支持对证书进行吊销，支持对已过期或已吊销的证书进行删除。

**证书吊销**是指已经签发的证书从签发机构处注销。证书吊销后将失去加密效果，浏览器不再信任该证书。

**证书删除**是指将已吊销的证书资源从阿里云系统中删除。

### 证书吊销与退款限制条件

您可能会在以下场景下需要吊销证书：

- 证书申请信息填写错误、但证书已签发，需要重新提交证书申请信息
- 证书已签发，但是需要更换证书绑定的域名
- 已无需使用该证书
- 出于安全因素考虑，不再使用该证书

证书吊销无限制条件，您可在任何时候申请吊销证书。

收费证书在签发后的30天内完成吊销（提交了吊销申请并完成吊销审核）可全额退款，超过30天完成吊销不退款。

> **说明** 证书吊销后将失去加密效果，请谨慎吊销。

### 证书删除限制条件

- 未过期的证书只有吊销后才可删除。
- 已过期的证书可以随时删除。
- 手动上传的证书可随时删除。

## 4.2. SSL证书服务控制台是否支持删除证书？

SSL证书服务控制台支持对已过期和已吊销的证书进行删除；未签发的证书不支持删除。

### 证书支持删除的状态

- 已过期
- 已吊销

### 证书不支持删除的状态

未签发的证书和已签发但还处于有效期、也未执行吊销的证书不支持删除。

- 已付款
- 审核中
- 审核失败

### 相关文档

吊销证书和删除证书有什么区别？

# 4.3. 如何设置证书的TLS协议版本？

TLS协议版本包括TLSv1.0、TLSv1.1和TLSv1.2，您可以根据需要在阿里云产品和Web服务器上设置证书的TLS协议版本。

如果您的证书部署到以下阿里云产品，请参见以下链接进行设置：

- SLB：TLS安全策略说明
- CDN：配置TLS
- DCDN：配置TLS

如果您的证书安装在Web服务器上，请在Web服务器的证书配置文件中找到 `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` ，根据实际需要进行修改。例如：您的证书需要支持TLSv1.1和TLSv1.2版本，在 `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` 中去掉 `TLSv1` 即可。