阿里云
SSL证书

快速入门

文档版本：20190215

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	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:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
##	表示参数、变量。	`bae log list --instanceid` *`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。	`swich` *`{stand | slave}`*

目录

1 限制说明

在使用云盾证书服务选购证书时，有如下限制：

- 暂时只支持四种服务器证书（免费、普通、专业、高级），每种服务器证书所对应的CA中心可能有不同产品（或者不提供相应证书），您可按照您的需求进行选择。
- 根据CA中心的要求，需要您提供您企业的真实合法的验证材料，阿里云会将这些材料提交至CA中心进行审核。审核过程中，CA中心会直接通过邮件或者电话的方式联系您。
- 对证书申请时的密钥加密位数限制为至少RSA 2048，哈希签名算法至少SHA 256，请您依据限制生成CSR文件。
- 云盾证书服务提供的证书格式为PEM格式。

2 概述

快速入门介绍了如何快速购买数字证书、填写审核资料、推送证书至阿里云产品等，旨在引导您一站式地完成数字证书购买、审核和快速应用流程。

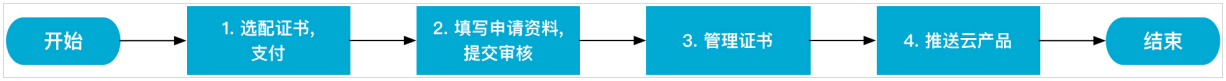
读者对象

本文档作为快速入门参考，适用于有以下需求的读者对象：

- 想要了解如何购买数字证书、区分数字证书的类型。
- 想要购买数字证书、提交审核资料。
- 想要在云产品中应用数字证书。

快速入门流程

购买和管理数字证书的流程：



一般情况下，可按以下步骤使用云盾证书服务：

1. 选配证书。
2. 填写申请资料并提交审核。
3. 管理证书。
4. 推送至其他阿里云产品。

3 步骤一：选配证书

本文档介绍了如何选择和购买阿里云SSL证书，以及不同类型证书的功能差异和特点。

1. 您可通过登录云盾证书服务购买页面购买数字证书。

2. 选配您需要的数字证书后，完成支付即可进入证书配置流程。

选择证书品牌（CA供应商）

目前，支持阿里云颁发数字证书的安全CA中心包括：

- Symantec：赛门铁克（Symantec）是全球第一大数字证书颁发机构、全球最值得信赖的SSL证书品牌，所有证书都采用业界领先的加密技术，为不同的网站和服务器提供安全解决方案。
- CFCA： 中国金融认证中心（CFCA）通过国际WebTrust认证，遵循全球统一鉴证标准，是国际CA浏览器联盟组织成员。CFCA全球信任SSL证书，由中国权威数字证书认证机构自主研发，纯国产证书。CFCA提供 7x24 小时金融级的安全保障服务，且有完善的风险承保计划。提供中文版全球信任体系电子认证业务规则（CPS），便于用户理解双方权利和义务。

> 说明:
> CFCA服务器证书目前不支持苹果 iOS 10.1 及 10.1 以前的版本，不支持安卓 6.0 及以前的版本。

- GeoTrust： GeoTrust 是全球第二大数字证书颁发机构， 也是身份认证和信任认证领域的领导者，采用各种先进的技术使任何大小的机构和公司都能安全、低成本地部署SSL数字证书和实现各种身份认证。
- GlobalSign： GMO GlobalSign是全球最早的数字证书认证机构之一，一直致力于网络安全认证及数字证书服务，是一个备受信赖的CA和SSL数字证书提供商。

选择证书类型

阿里云联合有资质的CA中心推荐以下几种数字证书配置组合方案：

> 说明:
> 不同品牌（CA供应商）提供的证书类型可能不同，例如GlobalSign目前仅提供专业版OV型证书。

- 免费型DV SSL： 免费型DV SSL证书是基础级SSL产品。

  > 说明:
  > 目前仅Symantec提供免费型数字证书，该证书仅支持绑定一个域名。

  - 只验证域名所有权，数小时内即可颁发。
  - 只提供通信链路加密功能。
  - 根证书一般使用CA中心认证的根证书。
  - 支持绑定一个明细子域名，且不支持通配符域名。
- 通配符DV SSL：通配符DV SSL证书属于DV型SSL证书（Domain Validation SSL）。
  - 只验证域名所有权，数小时内即可颁发。
  - 提供高强度通信链路加密功能。
  - 支持绑定一个带有通配符的域名。
- 专业版OV SSL： 专业版OV SSL证书属于OV型SSL证书（Organization Validation SSL）。
  - 验证域名所有权和申请单位的真实身份，解决在线信任问题。
  - 证书中显示申请者的企业单位名称，让访问用户安心使用。
  - 提供高强度通信链路加密功能。
  - 支持最多绑定100个域名，支持绑定通配符域名。

> 说明:
> 除专业版OV SSL证书外，Symantec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。

- 高级版EV SSL：高级版EV SSL证书属于EV型SSL证书（Extended Validation SSL）。
  - 严格验证域名所有权和申请单位的真实身份。
  - 证书在大部分浏览器中能显示绿色地址栏（部分证书在Safari浏览器中不显示），有效解决在线信任和网站被假冒问题。
  - 证书中详细显示申请者的企业单位信息，让访问用户安心使用。
  - 提供高强度通信链路加密功能。
  - 支持最多绑定100个域名。

> 说明:
> 除高级版EV SSL证书外，Symantec还提供增强型EV SSL证书。增强型EV SSL证书采用ECC椭圆曲线算法。

选择保护域名类型和个数

您在购买数字证书前，需要先规划好您需要保护什么样类型的域名和需要保护的域名个数，您可以选择保护一个、多个、或通配符域名。

- 1 个域名：您的数字证书只可以保护一个域名，且不支持通配符。例如，buy.example.com。
- 多个域名： 您的数字证书可以保护多个域名，根据证书种类不同有数量限制。一般数量上限为100个，您可根据域名个数进行选择，不支持通配符。例如，buy1.example.com；buy2.example.com。
- 通配符域名：您的数字证书可以保护一个带通配符的泛域名（暂不支持购买多个通配符子域名型证书）。例如，申请*.example.com，可以保护a1.example.com ，a2.example.com等域名，但不能保护 a1.sport.example.com，a2.thanks.example.com之类的域名。

> 说明:
> 在后续填写域名资料时，阿里云会对您选择的域名数量和类型的进行校验。如果您选择保护多个域名，您需要一次性提交全部域名。

选择证书有效期

您所选择数字证书的有效期年限。数字证书的有效期是在审核通过后开始计算，支持选择一年或两年。

说明:

免费版DV SSL证书限定最高申请年限为一年。

4 步骤二：填写资料

SSL证书完成购买和支付后，您需要填写证书申请人的详细信息并提交审核。审核通过后您才可使用SSL证书。

操作步骤

1. 登录SSL证书控制台。
2. 在证书控制台页面，单击待完成申请证书模块右下角的申请打开证书申请页面填写申请人的详细信息。

说明:

证书绑定域名：您可单击对话框后的问号图标查看域名添加提示，根据提示的限制来填写域名信息。

说明:

公司电话和申请人手机号码请填写正确，签证中心人员会拨打该电话号码确认证书认证相关的信息。

说明：
CSR生成方式建议选择系统生成，否则将无法推送到云产品。

3. 信息填写后完成后，单击下一步，进入证书验证信息页面。
4. 完成以下验证操作。
   a. 下载并打印校验文件模版。
   b. 完整填写校验文件并签署姓名。
   c. 签署姓名并加盖企业公章。
   d. 将校验文件拍照，并将照片上传（照片格式必须为PNG或JPEG格式的图片，且图片大小不能超过500 KB）。
5. 单击上传文件。

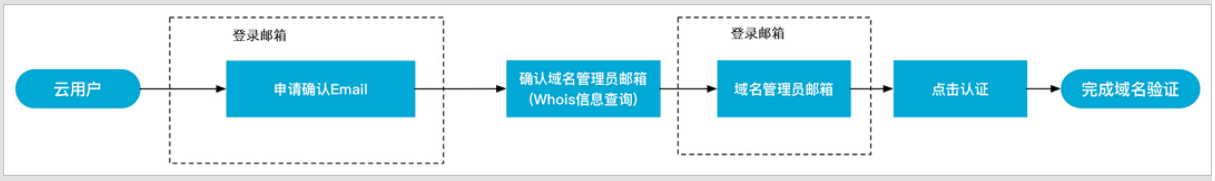
提交审核

当您填写完全部信息和上传后，需要提交审核来完成证书申请工作。

阿里云将在收到您的提交审核信息后开始证书资质的验证。验证时间根据不同CA中心的要求而不同，请您关注您的邮箱和电话，及时回馈将能有效缩短您的数字证书的验证时间。

如验证不通过，将会在您的订单中提示失败原因，您需要相应修改申请信息（尤其是企业资质审核信息）重新申请审核。

说明：
提交审核后，CA中心将向您的邮箱发送一封验证邮件，您需要按照如下流程进行域名验证。如不完成域名验证，您将无法通过证书审核，且您的证书申请将会一直显示审核中的状态。



5 步骤三：管理SSL证书

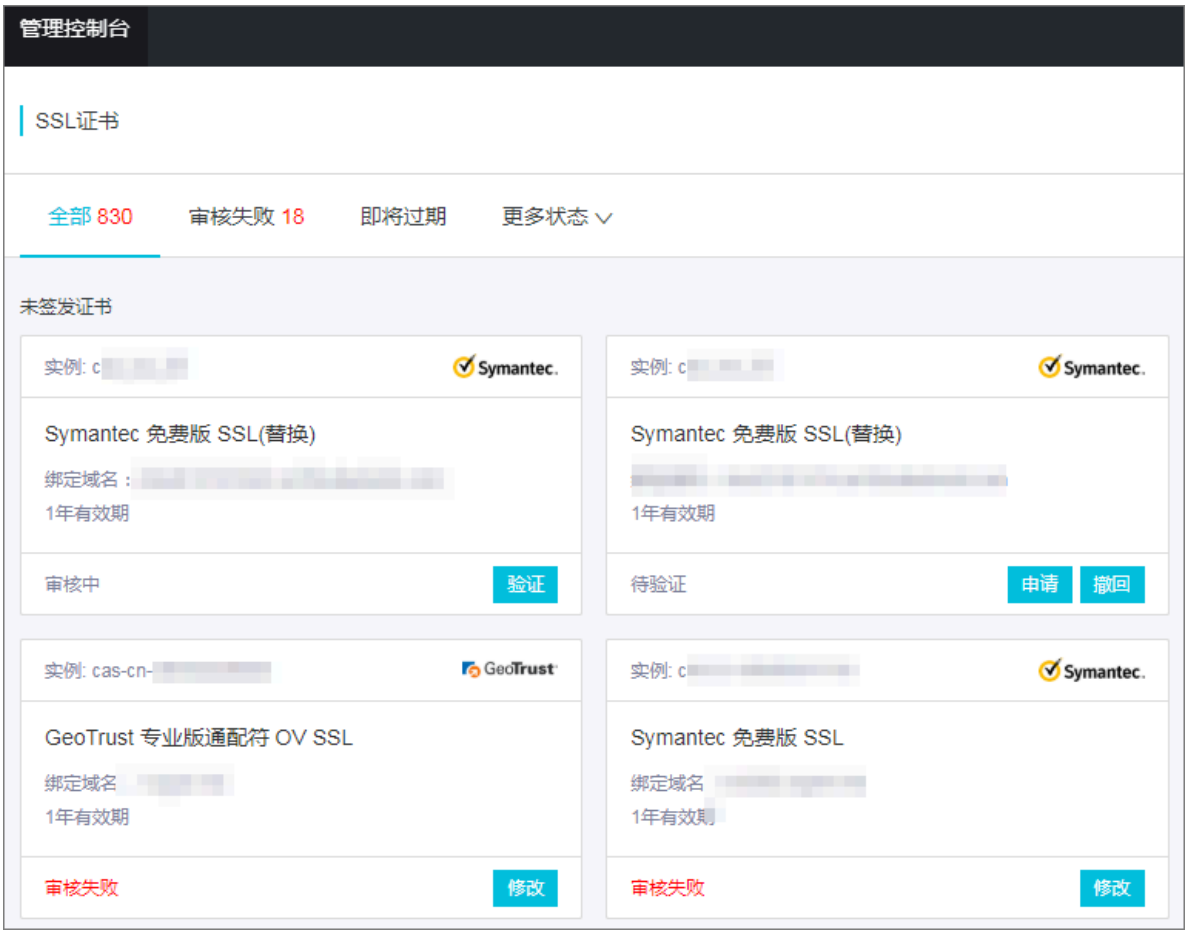
SSL证书审核通过后，您可以通过SSL证书服务控制台对您拥有的所有证书进行统一和集中的生命周期管理，包括查看证书的状态和有效期、上传您所拥有的其他证书到SSL控制台、到期新购证书等。

操作步骤

1. 登录云盾证书服务管理控制台。

   说明:
   您也可以上传您已有的数字证书在我的证书页面进行统一管理。

2. 在SSL证书页面查看并管理您的数字证书。

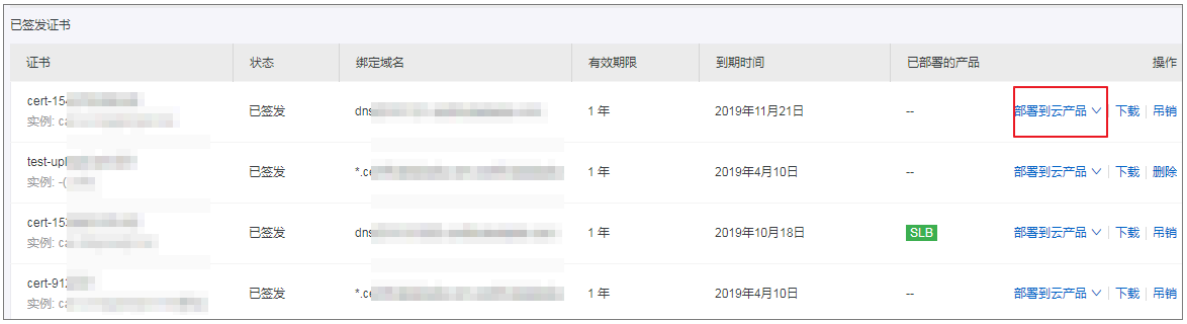


6 步骤四：推送云产品

SSL证书完成审核和签发后可以推送到其它阿里云产品，包括CDN、SCDN、DCDN和SLB服务，帮助您提升云产品访问数据的安全性。

操作步骤

1. 登录阿里云SSL证书控制台。
2. 在已签发证书区域单击目标证书的部署到云产品。



3. 在下拉列表中选择需要部署的云产品。
4. 在右侧打开的证书部署到CDN/SLB页面中勾选需要部署的区域。

> 说明：
> 部署到SLB时需选择您购买的SLB所部署的区域；绑定的CDN域名要和证书域名匹配。

5. 单击确定完成云产品区域部署。

如果您在申请数字证书时选择系统自动生成CSR方式，系统已经保存您的私钥，不需要再次上传；如果选择手动生成CRS方式，您需要上传您的私钥才能将证书推送到云产品。

> 说明：
> 私钥是和证书一一对应的，请确保上传正确的私钥文件。关于私钥的更多信息，参见什么是公钥和私钥。

说明:

您上传的私钥不允许再次下载，请您务必保存好您的原始私钥文件。