证书服务

快速入门

快速入门

限制说明

目前，对云盾证书服务有如下限制：

证书选购

- 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。

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。

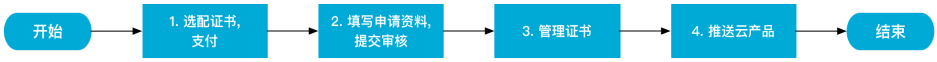
读者对象

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. 填写申请资料提交审核。
3. 管理证书。
4. 推送至其他阿里云产品。

步骤1：选配证书

您可通过登录云盾证书服务购买页面购买数字证书。

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：

免费型 SSL： 免费型 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。
- 仅支持绑定一个域名，且不支持通配符域名。

普通版 SSL： 普通版 SSL 证书属于 DV 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。
- 支持最多绑定 100 个域名。

专业版 SSL： 专业版 SSL 证书属于 OV 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。

高级版 SSL: 高级版 SSL 证书属于 EV 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。

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。
注意： 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。

注意： 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的多个域名。

选择证书有效期

您所选择的数字证书均有有效期年限限制：

- 免费版 SSL 证书限定最高申请年限为一年。
- 普通版 SSL 和专业版 SSL 证书限定最高申请年限为三年。
- 高级版 SSL 证书限定最高申请年限为两年。

步骤2：填写资料

当您购买数字证书并支付完成后，您需要填写证书的详细信息并且提交审核，完成证书申请流程。

1. 登录证书服务管理控制台。

在我的订单列表中，选择实例，单击**补全**，即可进入补全信息页面填写证书的详细信息。

补全证书信息后，单击**提交审核**，完成证书申请流程。

填写域名信息

您需要按照选购证书时选定的域名种类和域名个数来填写域名信息。例如，您选择了保护多个域名，并限定保护五个域名，则您需要在此步骤填写全部的五个域名，每行一个域名。

阿里云会对您填写的域名信息进行校验。

注意： CA 中心会对您所提交的域名做所有权验证，您会收到由 CA 中心发送的一封电子邮件要求您进行域名所有权验证。在您提交资料后，请及时检查您的邮箱（申请人 Email 邮箱）并进行验证。如果您的域名所有权验证不通过，您将无法通过证书审核。

填写申请信息

根据您选择的证书类型不同，您需要填写不同的信息。

如果您购买的是免费版 SSL 或者普通版 SSL证书，您需要填写申请人个人信息；如果您购买的是专业版 SSL 或者高级版 SSL 证书，您在填写申请人个人信息的同时还需要填写申请单位的详细信息。

填写个人信息

按要求填写申请人的联系信息，务必确认**申请确认Email**内容的准确性。

填写企业组织信息

按要求填写所需的企业组织信息，这些信息将会用来验证您企业的真实性。

上传相关信息

建议您使用“系统生成CSR”的方式来直接生成证书请求文件。

使用 **系统生成CSR** 方式，系统将自动帮您生成证书私钥，并且在证书申请成功后可直接在证书管理列表中下载您的证书和私钥。

您也可以自己生成 CSR（Certificate Signing Request）证书请求文件，并上传。关于如何生成 CSR 文件，请查看如何制作CSR文件。

注意：

- 您的 CSR 文件格式正确与否直接关系到您的证书申请流程是否能顺利完成。
- 您在制作 CSR 文件时请务必保存好您的私钥文件，私钥和数字证书一一对应，**一旦丢失了私钥您的数字证书也将不可使用**。阿里云不负责保管您的私钥，如果您的私钥丢失，您需要重新购买并替换您的数字证书。

如果您购买的是专业版 SSL 或者高级版 SSL 证书，您必须完成企业真实合法性校验。

企业真实合法性校验步骤

1. 下载并打印校验文件模版。
2. 完整填写校验文件。
3. 签署姓名并加盖企业公章。
4. 将校验文件拍照，并将照片上传。（照片格式必须为PNG、GIF、或JPEG格式的图片，且图片大小不能超过500 KB）

注意： 不同的 CA 中心对企业资质验证的需求不同，您需要按照 CA 中心的要求提供相应的审核资料。如审核资料不完整，将无法通过证书审核。申请过程中，您可以保存您所填写的信息以供下一次证书申请时使用。

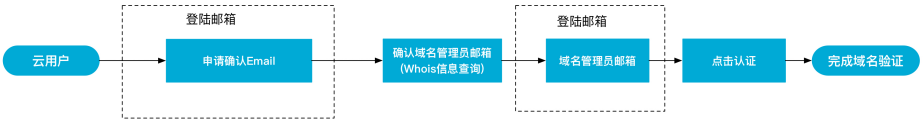
提交审核

当您填写完全部信息后，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。

重要： 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。

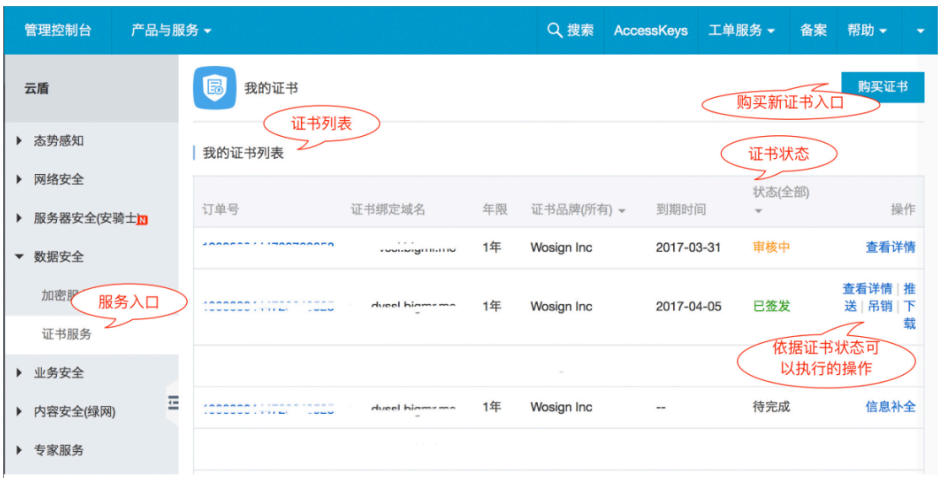


步骤3：管理证书

证书审核通过后，您可以在云盾证书服务管理控制台管理您的证书：

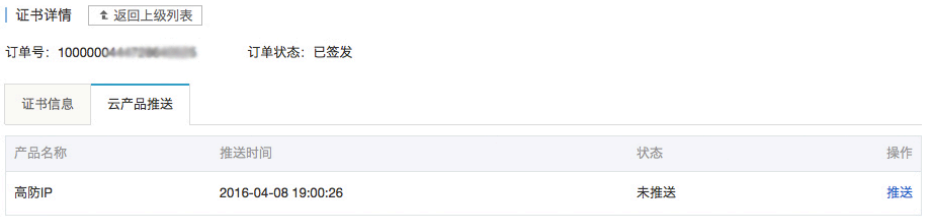
1. 登录云盾证书服务管理控制台，单击**我的证书**。
   注意： 您也可以上传您已有的数字证书在**我的证书**页面进行统一管理。

   在我的证书表中查看并管理您的数字证书。



步骤4：推送云产品

数字证书审核成功后，可以推送到其它阿里云产品，包括 CDN、DDoS 高防 IP、WAF、及 SLB 服务。



您需要上传您的私钥，才能使用推送数字证书到云产品功能。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。

注意： 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，请查看什么是公钥和私钥?。

重要： 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。