ALIBABA CLOUD

Alibaba Cloud

SSL证书服务

产品简介

文档版本：20220707

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 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 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 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 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` *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

1.什么是数字证书管理服务

数字证书管理服务（Certificate Management Service）是由阿里云联合全球多家数字证书颁发机构，在阿里云平台上直接提供数字证书申请、管理、部署等的服务。数字证书管理服务同时支持SSL证书和私有证书，帮您以较低的成本将数据传输协议从HTTP转换成HTTPS，实现网站或移动应用的身份验证和数据加密传输。

SSL证书和HTTPS的关系

您通过数字证书管理服务完成证书购买、申请，并将证书部署到您的Web服务器后，Web服务将会通过HTTPS加密协议来传输数据。HTTPS加密传输协议可激活客户端浏览器到网站服务器之间的SSL加密通道（SSL协议），从而实现高强度单向加密传输，防止传输数据被泄露或篡改。

HTTPS加密传输为手机APP、小程序应用、代码程序、控件等上线应用市场或应用生态必备特征。HTTPS加密传输可为网站带来以下优势：

- 安全合规：满足对应APP市场或应用生态的要求。
- 加密传输网络数据：加密网站用户与网站间的数据通信，实现传输数据的防劫持、防篡改、防监听，保障数据传输安全。
- 提升网站安全性：规避钓鱼事件发生。网站用户在访问网站时浏览器提示安全可信，可以提升网站的可信度、访问流量和搜索排名。

功能特性

功能模块	功能	说明	相关文档
SSL证书签发和应用	证书购买	购买DV、OV、EV型SSL证书。	购买SSL证书
	证书申请	使用已购买的证书实例提交证书申请并处理审核异常，直到CA中心成功为您签发证书。	提交证书申请
	证书合并申请	将多个品牌和类型都相同的证书实例合并为一个证书实例，并使用合并生成的证书实例提交证书申请。简化多证书的申请和管理流程。	提交证书申请
	证书安装	下载已签发的证书文件到本地，然后安装到您的Web服务器上。	SSL证书安装指南
		将已签发的证书一键部署到支持的阿里云产品上，节省在对应云产品中配置HTTPS时，单独上传证书的操作。	部署证书到阿里云产品
	证书吊销	按照标准的证书吊销流程，经过CA认证中心审核后，安全、快捷地吊销已签发的SSL证书。	吊销SSL证书
	证书退款	在符合退款条件的情况下，您可以在数字证书管理服务控制台申请退款。	SSL证书退款
证书续费	手动续费	在证书到期前30个自然日内，通过数字证书管理服务控制台手动续费及更新证书。	续费购买证书
PCA服务	私有证书	PCA服务使您可以通过简单的可视化操作，搭建企业自己的证书颁发机构，实现在企业内部签发和管理自签名私有证书，用于企业内部的应用身份认证和数据加解密。	概述

功能模块	功能	说明	相关文档
网站安全	域名监控	域名监控服务帮助您监测多个站点（使用不同域名）的HTTPS业务状态，及时发现站点上的SSL证书安全问题（例如，未配置SSL证书、证书已过期等），方便您统一维护多站点HTTPS，降低因人为疏忽导致HTTPS业务中断的风险。	域名监控
	网站安全检测	自动检测您的阿里云账号的网站资产及网站的SSL证书状态，帮助您全面了解网站资产的SSL证书状态，方便您为网站开启HTTPS。	查看网站SSL证书状态
申请信息管理	联系人管理	自动保存您使用过的证书申请联系人信息，或者由您手动添加联系人，方便您在申请证书时直接选择已有联系人。	管理联系人
	公司管理	自动保存您使用过的证书申请公司信息，或者由您手动添加公司，方便您在申请证书时直接选择已有公司。	管理公司信息
证书统一管理	上传证书	上传已有证书到数字证书管理服务中进行统一管理（例如，一键部署到支持的阿里云产品）。	上传证书
	管理CSR	支持使用CSR管理工具生成CSR或上传已有的CSR，实现统一管理CSR。	管理CSR

支持选购的证书类型

阿里云数字证书管理服务支持购买DV证书、OV证书和EV证书三种类型的证书。不同类型证书的安全性和适用的网站类型不同，具体如下表所示。

证书类型	适用网站类型	公信等级	认证强度	安全性	支持的证书品牌
DV域名型	个人网站	一般	CA机构审核个人网站真实性、不验证企业真实性	一般	DigiCert、GlobalSign
OV企业型	政府组织、企业、教育机构等	高	CA机构审核组织及企业真实性	高	DigiCert、Entrust、GlobalSign
EV企业增强型	大型企业、金融机构等	最高	严格认证	最高	DigiCert、Entrust

选购证书时，您还可以参考以下信息：阿里云支持的证书品牌、支持的加密算法。

2.产品优势

数字证书管理服务是由阿里云联合全球多家数字证书颁发机构（ CA），在阿里云平台上直接提供的证书全生命周期管理服务。本文介绍数字证书管理服务的多项特征，帮助您更好的了解数字证书管理服务。

与知名品牌合作

对接国际上值得信赖的第三方数字证书颁发机构（CA），确保证书认证的可信力和加密强度，保障网站用户的数据安全。

快速签发SSL证书

无需切换到不同CA系统，在阿里云官网就可以购买和签发多个不同品牌的SSL数字证书。阿里云可加速SSL证书的审核和签发。

云上云下证书统一管理

数字证书管理服务支持对云上云下证书进行统一管理。已签发的第三方证书上传到数字证书管理服务控制台后，即可享受和阿里云付费证书相同的证书管理能力，包括：查看证书、证书到期提醒、证书托管等。

提供证书托管服务

支持托管在数字证书管理控制台购买的证书。在证书即将到期时为您自动申请新证书，并为新签发的证书补齐旧证书剩余的有效期，避免浪费旧证书的剩余有效期，同时降低您的运维成本。

支持丰富的API功能

支持通过API批量执行证书购买、申请等操作。

支持申请全额退款

未消耗证书订单实例包含的证书个数时，支持28天无理由全额退款。

支持私有CA（PCA）服务

您可以使用PCA服务搭建企业内的证书颁发机构，实现企业内部私有证书的管理和签发，保障企业内部通信数据的安全传输。可用于企业对内使用和企业合规使用两种场景：

- 企业对内使用：企业内部应用（例如，内部的OA、HR等系统）可以使用PCA服务的密码技术进行应用间数据安全传输、数据加解密和身份认证。
- 企业合规使用：用于密评或者要求满足电子认证服务相关要求的场景，例如，银企直连、电子签名等。

3.应用场景

阿里云SSL证书服务适用于网站服务和云产品的HTTPS化。

网站数据加密

HTTP协议无法加密数据，导致网站数据可能产生泄露、篡改或钓鱼攻击等问题。安装SSL证书后，网站使用HTTPS协议对网站数据的传输进行加密，包括您网站中的企业应用数据、政务信息、支付环节的数据都能实现加密传输，有效保护敏感数据的传输。

网站服务由HTTP协议转换成HTTPS协议

阿里云用户需要将网站服务由HTTP协议转变成HTTPS协议，可以使用阿里云证书服务申请受信任CA认证中心颁发的数字证书，然后部署在云平台网站，将HTTP访问转换成HTTPS，为网站访问提供认证加密功能。

提升网站的安全性

如果网站没有安装SSL证书，网站地址以HTTP开头，浏览器会将此类网站标记为不安全的网站。

如果网站已安装SSL证书，浏览器会将该网站标记为安全网站，让您网站的用户可以放心访问您的网站。

对于已安装EV或OV证书的网站，由于CA中心已经审核过企业身份，可以更有效地增强网站用户对该网站的信任，从而提升网站业务的成交率。

在阿里云CDN、SCDN、DCDN或SLB等服务上使用HTTPS协议

您如果购买了阿里云CDN、SCDN、DCDN或SLB等服务，可以通过SSL证书服务将购买的数字证书一键部署在这些产品中，实现云产品的HTTPS化。

4.常见问题

4.1. 什么是公钥和私钥？

公钥（Public Key）与私钥（Private Key）是通过加密算法得到的一个密钥对（即一个公钥和一个私钥，也就是非对称加密方式）。公钥可对会话进行加密、验证数字签名，只有使用对应的私钥才能解密会话数据，从而保证数据传输的安全性。公钥是密钥对外公开的部分，私钥则是非公开的部分，由用户自行保管。

通过加密算法得到的密钥对可以保证在世界范围内是唯一的。使用密钥对的时候，如果用其中一个密钥加密一段数据，只能使用密钥对中的另一个密钥才能解密数据。例如：用公钥加密的数据必须用对应的私钥才能解密；如果用私钥进行加密也必须使用对应的公钥才能解密，否则将无法成功解密。

SSL证书的原理

SSL证书采用公钥体制，即利用一对互相匹配的密钥对进行数据加密和解密。每个用户自己设定一把特定的、仅为本人所知的私有密钥（私钥），并用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。

由于密钥仅为本人所有，可以产生其他人无法生成的加密文件，也就是形成了数字签名。

SSL证书是一个经证书授权中心（CA）数字签名的、包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字证书还有一个重要的特征就是只在特定的时间段内有效。

有关私钥原理的更多信息，请参见阿里云SSL证书私钥保护原理是怎样的？

创建私钥

阿里云SSL证书服务对您私钥的加密算法和长度要求如下。

- 加密算法使用RSA算法
- 加密长度至少2,048位

您可以通过以下两种方式创建您的私钥。

- **使用OpenSSL工具生成私钥**
  i. 您可以从 OpenSSL官网网站 下载最新的OpenSSL工具安装包。

  > **说明** OpenSSL版本必须是1.0.1g或以上版本。

  ii. 安装OpenSSL工具后，在命令行模式下运行 `openssl genrsa -out myprivate.pem 2048` 生成您的私钥文件。生成后的私钥文件名称为*myprivate.pem*，加密长度为2,048。
- **使用Keytool工具生成并导出私钥**

  Keytool工具是JDK中自带的密钥管理工具，可以制作Keystore（jks）格式的证书文件，您可以从 官方地址 下载JDK工具包来获取Keytool工具。

  由于使用Keytool工具制作的公钥和私钥默认是不可以导出的，您需要从已经创建好的*.keystore*文件中导出私钥。关于如何从*.keystore*文件中导出私钥，请参见如何转换证书格式？。

  在导出的文件中，以下部分的内容即是您的私钥：

```
-----BEGIN RSA PRIVATE KEY-----
......
-----END RSA PRIVATE KEY-----
```

或者

```
-----BEGIN PRIVATE KEY-----
.......
-----END PRIVATE KEY-----
```

说明 无论您通过哪种方式生成密钥，请您妥善地保管好您的私钥文件。私钥文件一旦丢失或者损坏，您申请的对应的公钥、及数字证书都将无法使用。

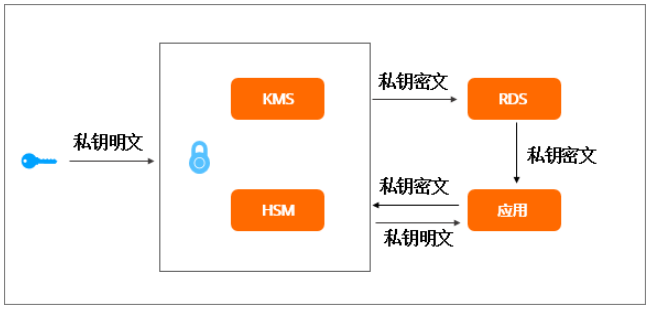
4.2. 阿里云SSL证书私钥保护原理是怎样的？

阿里云证书服务采用密钥管理系统对私钥进行加密存储，以保证您证书私钥的安全。

无论是您上传的证书及私钥，还是申请证书时使用系统创建CSR生成的私钥，阿里云证书服务都会采用经过权威机构认证的密钥管理系统进行加密存储。

阿里云密钥管理系统KMS（Key Management Service）是一款安全管理类产品，可保护证书密钥的数据安全性、完整性和可用性，满足您多应用、多业务的密钥管理需求，同时符合监管和等保合规要求。有关密钥管理系统的详细介绍，请参见什么是密钥管理服务。

阿里云证书服务采用多种规格的非对称加密方式保存证书私钥，私钥明文内容不会保存在磁盘中，仅在需要的时候出现在应用内存中。例如：您下载证书时，证书服务会对私钥密文解密并以明文的形式展示在您服务器的内存中，并通过浏览器的HTTPS下载到您本地计算机。



4.3. HTTPS与HTTP有什么不同？

HTTP是过去很长一段时间我们经常用到的一种传输协议。HTTP协议传输的数据都是未加密的，这就意味着用户填写的密码、账号、交易记录等机密信息都是明文，随时可能被泄露、窃取、篡改，从而被黑客加以利用，因此使用HTTP协议传输隐私信息非常不安全。

HTTPS是一种基于SSL协议的网站加密传输协议，网站安装SSL证书后，使用HTTPS加密协议访问，可激活客户端浏览器到网站服务器之间的SSL加密通道（SSL协议），实现高强度双向加密传输，防止传输数据被泄露或篡改。简单讲，HTTPS=HTTP+SSL，即HTTPS是HTTP的安全版。

4.4. 常见SSL证书都有哪些格式？

常见Web服务软件

常见的Web服务软件，通常都基于OpenSSL和Java两种基础密码库。

- Tomcat、Weblogic、JBoss等Web服务软件，一般使用Java提供的密码库。通过Java Development Kit（JDK）工具包中的Keytool工具，生成Java Keystore（JKS）格式的证书文件。

- Apache、Nginx等Web服务软件，一般使用OpenSSL工具提供的密码库，生成PEM、KEY、CRT等格式的证书文件。
- IBM的Web服务产品，如Websphere、IBM Http Server（IHS）等，一般使用IBM产品自带的iKeyman工具，生成KDB格式的证书文件。
- 微软Windows Server中的Internet Information Services（IIS）服务，使用Windows自带的证书库生成PFX格式的证书文件。

证书文件格式

以下表格介绍了文件的常见格式，您可以参考以下表格区分带有后缀扩展名的证书文件。

文件后缀	文件类型	说明
.DER或.CER	二进制格式	只含有证书信息，不包含私钥。
*.CRT	二进制格式或文本格式	只含有证书信息，不包含私钥。
*.PEM	文本格式	一般存放证书或私钥，或同时包含证书和私钥。*.PEM文件如果只包含私钥，一般用*.KEY文件代替。
.PFX或.P12	二进制格式	同时包含证书和私钥，且一般有密码保护。

> **说明** 证书格式之间是可以互相转化的。具体操作，请参见如何转换证书格式？。

您可以使用记事本直接打开证书文件。如果显示的是规则的数字字母（如下所示内容），那么该证书文件是文本格式。

```
--BEGIN CERTIFICATE--
MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh......
--END CERTIFICATE--
```

- 如果存在`--BEGIN CERTIFICATE--`，则说明这是一个证书文件。
- 如果存在`--BEGIN RSA PRIVATE KEY--`，则说明这是一个私钥文件。

需要在服务器中安装证书时，您可以根据服务器类型在数字证书管理服务控制台下载对应类型的证书。具体操作，请参见下载证书到本地。

4.5. 到期续费证书和新购证书有什么区别？

到期续费是阿里云SSL证书为您提供的功能，可以有效保障您提前为证书续费而不损失证书过期前剩余未使用的有效期，避免因证书更新不及时导致该证书绑定的网站展示为不安全的网站。您可以直接为快到期的证书进行续费。

新购证书是指您购买新的证书。

到期续费证书和新购证书有以下区别：

- 到期续费证书的有效期会叠加上证书过期前尚未使用的有效期。

> **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。

- 到期续费证书比新购证书签发速度更快。
- 到期续费的证书无需您重新填写申请信息，新购的证书需要填写证书申请信息。

> **说明** 由于阿里云SSL证书服务已为您保存了申请证书的历史信息，到期证书完成续费后申请证书时，会自动填充您之前申请同类证书时填写的历史信息。

4.6. 通配符域名证书都支持哪些域名？

阿里云SSL证书支持通配符域名证书，用户可以使用通配符域名证书保护服务器的单个主域名和该主域名下同级别的所有子域名。通配符DV类型和专业版OV类型证书都支持通配符域名。

如果您拥有多个同级别子域名服务器，使用通配符域名证书无需为每个子域名单独购买和安装证书。

购买**通配符域名**证书需要注意**通配符域名**证书匹配域名的规则：

- 通配符域名证书只能匹配同级别的子域名，不能跨级匹配。

  例如：*.example.com的域名证书匹配abc.example.com、sport.example.com、good.example.com等子域名，但是不匹配mycard.good.example.com、mycalc.good.example.com等下级域名。

  *.good.example.com匹配mycard.good.example.com、mycalc.good.example.com等子域名。
- 通配符域名证书支持的域名包含一级域名。
- 通配符域名证书只支持一个通配符主域名，不支持多个主域名。
- 通配符域名证书目前仅支持通配符类型的域名、不支持普通域名（非通配符域名）。

  如需一张证书包含多个通配符域名和一个或一个以上普通域名，请参考如何申请多通配符域名证书、混合域名证书？。

4.7. 哪些网站必须启用HTTPS加密？

在越来越重视信息安全的今天，HTTPS协议站点无疑已经成为主流。就目前形势而言，以下网站必须启用HTTPS协议加密：

- 电商平台及其相关支付系统网站
- 银行系统、金融机构等高私密性网站
- 政府、高校、科研机构及其相关网站
- 以搜索引擎为主要流量来源的网站
- 以邮箱为主的企业交流平台

长远来看，HTTPS协议网站已是必然趋势。启用HTTPS协议加密是当今网站建设的关键要点。不仅局限于上述网站类型，启用HTTPS协议加密既是网站安全的必然需要，也是公司发展的提前布局。

5.基本概念

本文档介绍了使用阿里云数字证书管理服务时需要了解的基本概念。

数字证书

数字证书是一个经权威授权机构数字签名，包含公开密钥的拥有者信息以及公开密钥的文件，是权威机构颁发给网站的可信凭证。最简单的证书包含一个公开密钥、证书名称以及证书授权中心的数字签名。

数字证书的一个重要特征：只在特定的时间段内有效。

CA认证中心

CA认证中心（CA机构），即证书授权中心（Certificate Authority）或称证书授权机构。

CA认证中心作为电子商务交易中受信任的第三方，承担公钥体系中公钥合法性检验的责任。

证书有效期

自2020年09月01日起，全球CA颁发的证书有效期最长为一年。您通过阿里云数字证书管理服务申请的证书，有效期都是一年。

SSL

安全套接层SSL（Secure Sockets Layer）协议是一种可实现网络通信加密的安全协议，可在浏览器和网站之间建立加密通道，保障数据在传输的过程中不被篡改或窃取。

SSL证书

SSL证书采用SSL协议进行通信，是由权威机构颁发给网站的可信凭证，具有网站身份验证和加密传输双重功能。

SSL证书指定了在应用程序协议（例如，HTTP、Telnet、FTP）和TCP/IP之间提供数据安全性分层的机制。它是在传输通信协议（TCP/IP）上实现的一种安全协议，采用公开密钥技术为TCP/IP连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。

SSL证书采用公钥体制，即利用一对互相匹配的密钥对进行数据加密和解密。每个用户自己设定一把特定的、仅为本人所知的私有密钥（私钥），并用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。

SSL证书部署到Web服务器后，您通过Web服务器访问网站时将启用HTTPS协议。您的网站将会通过HTTPS加密协议来传输数据，可帮助您的Web服务器和网站间建立可信的加密链接，从而保证网络数据传输的安全。

关于证书私钥的详细介绍，请参见什么是公钥和私钥？。

HTTPS

HTTPS也就是HTTP+SSL，基于SSL协议的网站加密传输协议，是HTTP的安全版。

您的网站安装SSL证书后，将会通过HTTPS加密协议来传输数据，HTTPS加密传输协议可激活客户端浏览器到网站服务器之间的SSL加密通道（SSL协议），从而实现高强度双向加密传输，防止传输数据被泄露或篡改。

域名

域名是IP地址的代称，由一串用半角句号（.）分隔的名称组成，在数据传输时用来标识一台服务器或服务器组。

单域名是最简单的域名，例如，*www.aliyundoc.com*。

通配符域名是指对应一个主域名及其所有次级子域名的域名。例如*.aliyundoc.com。*.aliyundoc.com*可以匹配*aliyundoc.com*（主域名）、*www.aliyundoc.com*（下一级子域名）、*example.aliyundoc.com*（下一级子域名）等，不支持匹配*www.example.aliyundoc.com*。

通配符证书

通配符证书也叫泛域名证书，证书绑定的域名为通配符域名（例如*.aliyundoc.com）时，即称该证书为通配符域名证书。

多通配符证书是指绑定多个通配符域名的证书。数字证书管理服务只支持申请单个通配符域名的证书，不支持申请多通配符域名的证书。您可以通过合并多个相同品牌、类型的证书，生成多通配符证书。具体操作，请参见证书合并申请。

混合域名证书

混合域名证书是指绑定的域名既包括单域名，也包括通配符域名的证书。例如，绑定的域名为*.aliyundoc.com、demo.example.com，即称该证书为混合域名证书。

数字证书管理服务不支持申请混合域名证书，您可以通过合并多个相同品牌、类型的证书，生成混合域名证书。具体操作，请参见证书合并申请。

Nginx

Nginx是一款轻量级高并发的Web服务器、反向代理服务器和电子邮件（IMAP和POP3）代理服务器，在BSD-like协议下发行。它可以运行在Linux、Windows、FreeBSD、Solaris、AIX、Mac OS等操作系统上，为您提供反向代理、负载均衡、动静分离等服务。

Tengine

Tengine是由淘宝网发起的Web服务器项目，它继承Nginx的所有特性、兼容Nginx的配置。

PuTTY

PuTTY是一款Telnet、SSH、rlogin、纯TCP以及串行接口连接软件，它可以远程管理Linux和Windows操作系统。

Xshell

Xshell是一款强大的安全终端模拟软件，它支持SSH1、SSH2、Microsoft Windows平台的Telnet协议。Xshell可以在Windows界面下远程管理不同系统下的服务器，从而达到比较好的远程控制终端的目的。Xshell支持VT100、VT220、VT320、Xterm、Linux、SCO ANSI、ANSI终端仿真，并提供各种终端外观选项取代传统的Telnet客户端。

CentOS

社区企业操作系统CentOS（Community Enterprise Operating System）是一个基于Red Hat Linux提供的可自由使用源代码的免费版企业级Linux发行版本。

CSR

CSR（Certificate Signing Request）是证书签名请求文件，包含了您的服务器信息和公司信息。申请证书时需要将您证书的CSR文件提交给CA认证中心审核，CA中心对CSR文件进行根证书私钥签名后会生成证书公钥文件（即签发给您的SSL证书）。

6.支持的证书品牌

本文介绍了阿里云数字证书管理服务提供购买的SSL证书的品牌（即对应的CA供应商）和不同品牌支持签发的证书类型。

下表罗列了SSL证书服务支持的SSL证书品牌及不同品牌支持的证书类型。下表中使用的图标说明如下：

- √：表示支持该类型证书。
- ×：表示不支持该类型证书。

> **说明** 关于证书类型的更多介绍，请参见支持的证书类型。

证书品牌	说明	支持的证书类型		
		DV（域名型）	OV（企业型）	EV（企业增强型）
DigiCert	DigiCert（原Symantec）是全球第一大数字证书颁发机构、全球范围内值得信赖的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。	√ 支持单域名、通配符域名	√ 支持单域名、通配符域名	√ 仅支持单域名
Entrust	Entrust作为全球著名的CA厂商，在全球范围内建立起了一个可信的虚拟环境，使任何人在任何地点都能放心地进行数字交易和沟通。 Entrust面向网站、软件开发商和个人提供信任服务，这其中包括签发专门应对网站鉴别和加密的SSL服务器证书，世界500强企业中超过83%的企业使用Entrust SSL证书。	×	√ 支持单域名、通配符域名、多域名	√ 支持单域名、多域名
GlobalSign	GlobalSign是全球较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。	√ 支持单域名、通配符域名	√ 支持单域名、通配符域名、多域名	×

7.支持的加密算法

阿里云SSL证书服务支持RSA、ECC和SM2三种加密算法。本文介绍不同证书品牌支持的加密算法。

以下是阿里云SSL证书服务支持的加密算法的说明。

- **RSA**：目前应用广泛的非对称加密算法，兼容性好。
- **ECC**：椭圆曲线公钥密码算法。相比于RSA，ECC是一种更先进和安全的加密算法（加密速度快、效率更高、服务器资源消耗低），目前已在主流浏览器中得到推广。
- **SM2**：中国国家密码管理局发布的ECC椭圆曲线公钥密码算法，在中国商用密码体系中用来替代RSA算法。

下表罗列了SSL证书服务支持的SSL证书品牌及不同品牌支持的加密算法类型。下表中使用的图标说明如下：

- √：表示支持该类型算法。
- ×：表示不支持该类型算法。

证书品牌	证书类型	RSA	ECC	SM2
DigiCert	DV	√	×	×
	OV	√	√	×
	EV	√	×	×
Entrust	OV	√	×	×
	EV	√	×	×
GlobalSign	DV	√	×	×
	OV	√	√	×