ALIBABA CLOUD

阿里云

SSL证书服务

产品简介

文档版本：20200831

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

1.什么是阿里云SSL证书

阿里云SSL证书（SSL Certificates）由阿里云联合中国及中国以外地域多家数字证书管理和颁发的权威机构，在阿里云平台上直接提供的服务器数字证书，并且给您提供额外的一键式HTTPS、证书扩展服务和证书托管等增值服务，帮助您以最小的成本将您的服务从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。

证书类型

阿里云SSL证书提供DV证书、OV证书和EV证书三种类型。有关证书的选型案例请参见证书选型案例。

数字证书	适用网站类型	公信等级	认证强度	安全性
DV SSL	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
OV SSL	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
EV SSL	大型企业、金融机构等	最高	严格认证	最高（地址栏绿色）

功能特性

功能模块	为您提供的价值	功能详情
网站HTTPS化	防劫持、防篡改、防监听。	使用SSL证书可实现网站的HTTPS化，对网站用户与网站间的交互访问全链路数据进行加密，从而实现传输数据的防劫持、防篡改、防监听。
	提升网站的搜索排名。	使用SSL证书实现HTTPS加密的网站在搜索引擎显示结果中的排名将会更高，有利于提升网站的搜索排名和站点的可信度。
	提升网站的访问流量。	使用SSL证书实现网站的HTTPS化，可以强化网站在用户侧的身份可信程度，使网站用户能更安心地访问网站，从而提升网站的访问流量。
证书高效管理	提高证书运维效率。	提供上传证书和私钥功能，实现在阿里云平台统一管理各种数字证书、提交审核、查看证书绑定域名和到期时间、修改证书名称、删除已过期的证书等一站式服务，帮助您有效提高证书运维效率。
	一键部署SSL证书到其他阿里云产品。	提供在阿里云平台上一键部署SSL证书到其他阿里云产品的功能，帮助您实现低成本部署SSL证书。具体请参见已签发证书部署到阿里云产品。
	证书便捷吊销。	按照标准的证书吊销流程，经过CA认证中心审核后，安全、快捷地吊销服务器SSL证书。具体请参见吊销证书。

提供的增值服务

阿里云SSL证书除了为您提供SSL证书外，还为您提供一键HTTPS、证书扩展服务和证书托管的增值服务。

增值服务	为您提供的价值	详细介绍
一键式HTTPS	SSL证书支持一键式HTTPS服务，帮助您自动解决SSL证书安装部署、证书到期更新、证书私钥安全存储及TLS加速等问题，无需您进行手动操作，避免因证书安装和更新等复杂操作带来的问题。	一键式HTTPS
证书扩展服务	阿里云提供的SSL证书扩展服务，新增了支持通过API调用的方式申请和签发证书，使您不再只能使用控制台进行证书申请和签发。同时，您还可以通过证书扩展服务一次性下单购买不限数量的SSL证书。	证书扩展服务
证书托管服务	证书托管服务可以帮助您自动延长证书的有效期，避免因证书更新不及时从而导致浏览器将您的网站识别为不安全的网站。	证书托管服务

支持的国家和地域

阿里云SSL证书适用于以下国家和地域：

- 中国内地所有地域
- 澳大利亚（悉尼）
- 日本（东京）
- 德国（法兰克福）
- 阿联酋（迪拜）
- 印度（孟买）

相关咨询

如有证书购买、证书类型选择等相关问题，请联系阿里云SSL证书售前咨询。

2.为什么在阿里云购买证书

阿里云支持多个证书品牌，为您提供不同类型的SSL证书。

与知名品牌合作

对接中国和国际上最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。

提供多种证书类型

对接中国和国际上最值得信赖的第三方数字证书颁发机构（CA），为您提供OV、EV、DV等各种不同类型的证书。证书类型和品牌选择范围广泛，可满足您在各种不同应用场景下的需求。

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。

一键部署到云产品

和阿里云产品深度集成，支持一键将SSL证书部署到已经开通的阿里云产品中（例如：SLB和CDN），以最低成本和方便快捷的方式轻松运维和管理不同的证书。

支持一键式HTTPS

支持一键式HTTPS，对整个网站的所有网页提供HTTPS加密。可通过CNAME快速接入，满足等保合规需求。

支持API

支持通过API批量执行证书购买、申请、下载和部署等操作。

退款条件

SSL证书支持五天无理由退款。

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。

提升网站用户访问网站的安全性

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，浏览器地址栏会展示该网站所属企业的真实身份，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。

阿里云CDN、SCDN、DCDN或SLB服务上使用HTTPS协议

您如果购买了阿里云CDN、SCDN、DCDN或SLB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。

一键式HTTPS支持对网站下所有页面进行HTTPS加密

阿里云SSL证书服务支持一键式HTTPS，帮助您实现网站的所有页面都支持HTTPS访问。一键式HTTPS可解决SSL证书安装部署、证书到期更新、证书私钥安全存储及TLS加速等问题。

4.证书选型案例

本文档介绍了各行各业证书选型的案例，为您选择证书类型时提供参考。

行业	常规推荐的证书类型	案例	业务特征
金融、银行	EV	中国银行	• 希望企业身份信息展示在网站地址栏 • 对数据传输保密性有很高要求
教育、政府、互联网	OV通配符证书	• 外交部 • 淘宝、天猫 • 新浪、今日头条 • 上海黄金交易所 • 国家电网 • 用友软件 • 浪潮 • 阿里云	• 网站后期有多个新增站点的需求 • 无需政府、公司名称展示在网站地址栏
个人业务	DV	个人博客等	• 无数据传输业务 • 纯信息或内容展示的网站

5.常见术语

本文档介绍了阿里云SSL证书服务相关的技术术语。

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。

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（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。

有关证书私钥的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。

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。

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.常见问题

6.1. SSL证书有什么优势？

本文档介绍了对比传统的加密方式，SSL证书所拥有的优势。

传统的加密方式 优势

- **简单快捷**：只需要申请一张证书，部署在服务器上，就可以在有效期内不用做其他操作。
- **显示直观**：部署SSL证书后，通过HTTPS访问网站，能在地址栏或地址栏右侧直接看到加密锁标志，直观地表明网站是加密的。使用EV证书，还能直接在地址栏看到公司名称。
- **身份认证**：这是别的加密方式都不具备的，能在证书信息里面看到网站所有者公司信息，进而确认网站的有效性和真实性，不会被钓鱼网站欺骗。
- **快速签发**：一键申请快捷高效。支持在一个平台下购买签发多个不同品牌的SSL数字证书。阿里云负责加速审核SSL证书的签发。
- **轻松一键部署**：支持一键将数字证书部署在阿里云已经开通的云产品中（SLB、CDN、SCDN和DCDN），以最小成本在云上应用。

6.2. 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。

证书 SSL 私钥 非对称加密
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。

有关私钥的原理请参见阿里云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，请参见证书格式转换。

  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。

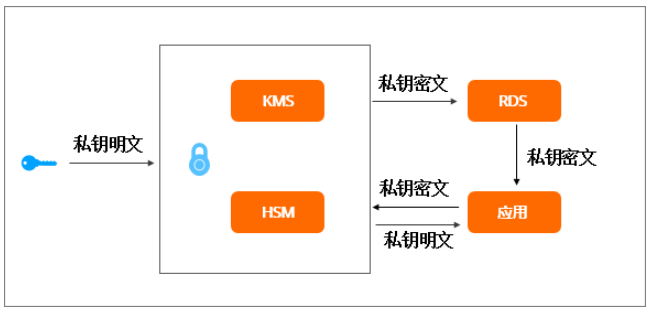
6.3. 阿里云SSL证书私钥保护原理是怎样的？

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。

阿里云 SSL证书 私钥保护
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，私钥明文内容永远不会在磁盘中保存，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。



6.4. 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。

6.5. 主流数字证书都有哪些格式？

主流Web服务软件

一般来说，主流的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。

如何判断证书文件是文本格式还是二进制格式？

您可以使用以下方法简单区分带有后缀扩展名的证书文件：

- *.DER或*.CER文件： 这样的证书文件是二进制格式，只含有证书信息，不包含私钥。
- *.CRT文件： 这样的证书文件可以是二进制格式，也可以是文本格式，一般均为文本格式，功能与 *.DER及*.CER证书文件相同。
- *.PEM文件： 这样的证书文件一般是文本格式，可以存放证书或私钥，或者两者都包含。 *.PEM 文件如果只包含私钥，一般用*.KEY文件代替。
- *.PFX或*.P12文件： 这样的证书文件是二进制格式，同时包含证书和私钥，且一般有密码保护。

您也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，例如：

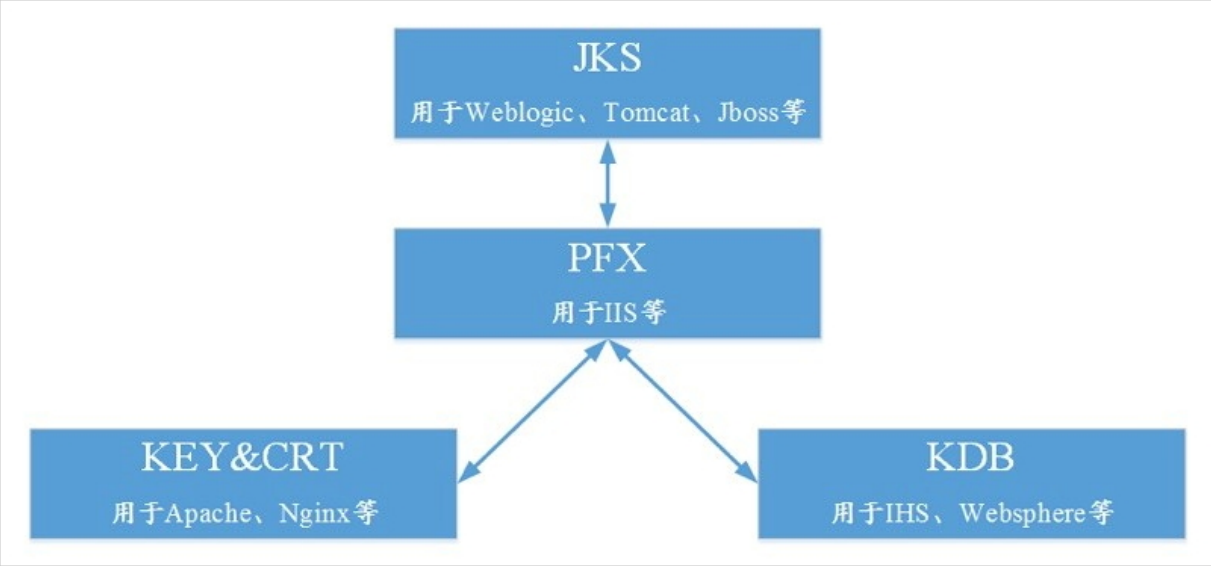
```
—-BEGIN CERTIFICATE—-
MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh.....
—-END CERTIFICATE—-
```

那么，该证书文件是文本格式的。

- 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。

证书格式转换

以下证书格式之间是可以互相转换的。



您可使用以下方式实现证书格式之间的转换：

> 说明 云盾证书服务统一使用 PEM 格式的数字证书文件。

- 将JKS格式证书转换成PFX格式

  您可以使用JDK中自带的Keytool工具，将JKS格式证书文件转换成PFX格式。例如，您可以执行以下命令将*server.jks*证书文件转换成*server.pfx*证书文件：

```
keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx
-srcstoretype JKS -deststoretype PKCS12
```

- 将PFX格式证书转换为JKS格式

  您可以使用JDK中自带的Keytool工具，将PFX格式证书文件转换成JKS格式。例如，您可以执行以下命令将*server.pfx*证书文件转换成*server.jks*证书文件：

  ```
  keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks
  -srcstoretype PKCS12 -deststoretype JKS
  ```

- 将PEM、KEY、CRT格式证书转换为PFX格式

  您可以使用 OpenSSL工具，将KEY格式密钥文件和CRT格式公钥文件转换成PFX格式证书文件。例如，将您的KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）拷贝至OpenSSL工具安装目录，使用OpenSSL工具执行以下命令将证书转换成*server.pfx*证书文件：

  ```
  openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
  ```

- 将PFX转换为PEM、KEY、CRT

  您可以使用 OpenSSL工具，将PFX格式证书文件转化为KEY格式密钥文件和CRT格式公钥文件。例如，将您的PFX格式证书文件拷贝至OpenSSL安装目录，使用OpenSSL工具执行以下命令将证书转换成*server.pem*证书文件KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）：

  - `openssl pkcs12 -in server.pfx -nodes -out server.pem`
  - `openssl rsa -in server.pem -out server.key`
  - `openssl x509 -in server.pem -out server.crt`

  > **说明** 此转换步骤是专用于通过Keytool工具生成私钥和CSR申请证书文件的，并且通过此方法您可以在获取到PEM格式证书公钥的情况下分离私钥。在您实际部署数字证书时，请使用通过此转换步骤分离出来的私钥和您申请得到的公钥证书匹配进行部署。

6.6. 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。您可以直接登录阿里云SSL证书控制台为快到期的证书进行续费。

新购证书是指您阿里云SSL证书购买页面购买新的证书。

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。

6.7. 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，用户可以通过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，参考多通配符域名和混合域名证书的申请方法。

6.8. 各类SSL证书的区别和网页展示效果

本文档介绍了不同类型SSL证书在安全性、公信等级、适用的网站类型和生效显示上的区别。

DV SSL OV SSL EV SSL 阿里云SSL证书

SSL证书的区别

数字证书	适用网站类型	公信等级	认证强度	安全性
DV SSL	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
OV SSL	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
EV SSL	大型企业、金融机构等	最高	严格认证	最高（地址栏绿色）

阿里云签发的Digicert证书，在原有OV、EV证书的基础上，推出了专业版OV证书、增强版Pro EV证书，与原有的OV和EV证书的区别主要在于专业版OV和增强版EV证书支持ECC椭圆加密算法。

> 说明 研究表明，160位的ECC椭圆密钥与1024位的RSA密钥安全性相同。

浏览器展示效果说明

SSL数字证书主要分为DV SSL、OV SSL、EV SSL三种类型。不同类型的SSL证书部署到网站所在的服务器上后，该网站在浏览器地址栏会展示以下不同的效果。

6.9. Digicert和GeoTrust证书支持苹果ATS和Android的哪些版本？

Digicert和GeoTrust支持Android的哪些主流版本？

Digicert和GeoTrust兼容Android系统2.3.3及以上所有版本。

> 说明 Android 4.4至5.0之间的部分版本，由于Android碎片化问题导致部分Android机型存在兼容性问题（通常是较老版本）。

Geotrust专业版OV SSL证书支持苹果ATS和Android的哪些版本？

GeoTrust专业版OV SSL证书，支持苹果iOS以及MAC系统，同时也支持Android 4.4及以上版本的系统。

> 说明 Android 4.4至5.0之间的部分版本，由于Android碎片化问题导致部分Android机型存在兼容性问题（通常是较老版本）。

6.10. SSL证书地域说明

您可在SSL证书控制台切换证书实例所在地域（region），您的证书数据将会保存到对应的region中。

证书购买和签发后安装部署不受地域的限制。

6.11. 中国的服务器支持共用中国以外地域服务器申请的证书吗？

支持。证书会绑定域名，如果中国与中国以外地域的两个服务器使用的域名一致，是支持共用一套证书的。

6.12. 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。

6.13. 未开启网站服务前是否可以申请HTTPS证书？

未购买服务器，并且未开启网站服务前，只要已拥有域名，就可以提前申请HTTPS证书（收费证书与免费证书都可申请）。但如果您申请证书时还未购买服务器，证书验证时将不支持选择**文件验证**的方式。

> **说明** 提交申请验证时，如果选择**文件验证**的方式，需要在服务器中上传相关验证文件。

6.14. 如何收到证书到期的系统通知？

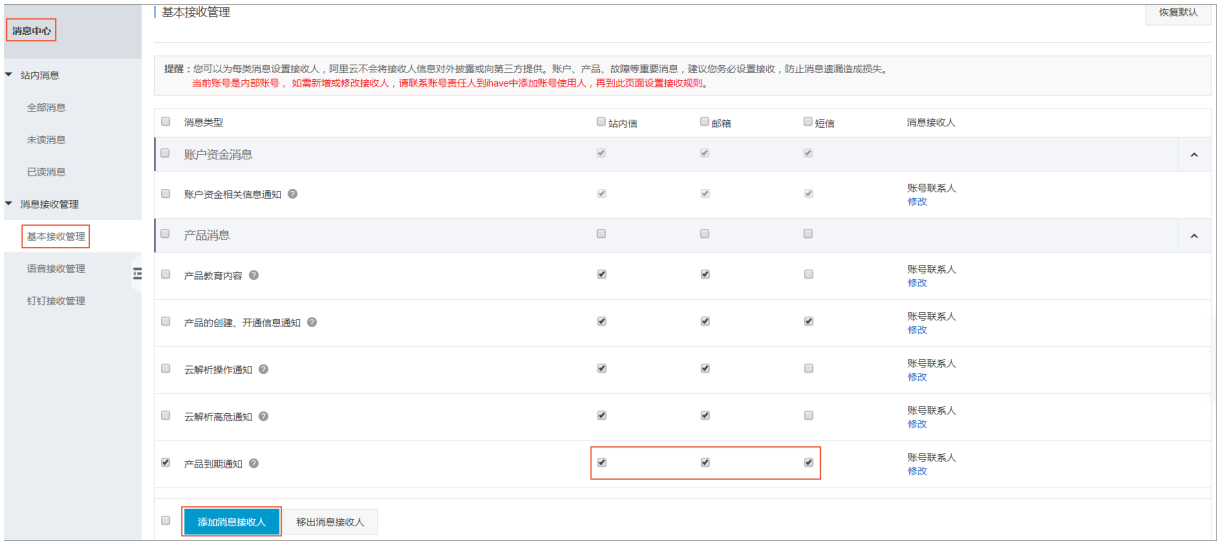
证书到期前一个月，阿里云SSL证书控制台会提示证书到期的信息。您也可以通过消息中心来设置是否需要接收证书相关的系统消息通知。如未设置消息中心的通知，您将不会收到证书到期的站内信、邮箱或手机短信通知。

您可在消息中心控制台**基本接收管理**页面，对是否需要接收相关消息通知和消息通知的类型进行自定义设置。可选的通知类型有站内信、邮箱和手机短信。

单击**添加消息接收人**可增加其他联系人接收消息通知。

基本接收管理设置完成后，您将接收到您选择的消息类型相关的通知。

到期续费相关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。