阿里云
SSL证书服务

常见问题

文档版本：20200708

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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。
	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。
	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。	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

法律声明.....I
通用约定.....I
1 SSL证书常见问题概览..... 1
2 证书相关概念..... 5
2.1 什么是SSL证书？.....5
2.2 SSL证书有什么优势？.....5
2.3 什么是公钥和私钥？.....5
2.4 HTTPS与HTTP有什么不同？.....7
2.5 主流数字证书都有哪些格式？.....7
3 证书应用场景..... 11
3.1 哪些网站必须启用HTTPS加密？..... 11
3.2 阿里云SSL证书私钥保护原理是怎样的？.....11
4 证书收费和开通问题..... 13
4.1 SSL证书收费方式.....13
4.2 开通证书服务可以购买绑定了IP的证书吗？.....13
5 免费证书相关问题..... 14
5.1 申请免费证书..... 14
6 证书续费或升级相关问题..... 16
6.1 Symantec SSL数字证书升级的影响与处理方案..... 16
6.2 证书如何续费？..... 18
6.3 证书续费时选错了证书类型如何处理？.....18
7 证书地域相关问题..... 19
7.1 SSL证书地域说明..... 19
7.2 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？..... 19
8 证书有效期相关问题..... 20
8.1 如何收到证书到期的系统通知？..... 20
8.2 SSL证书快过期了怎么办？..... 21
8.3 吊销证书和删除证书有什么区别？.....21
8.4 证书订单时间和签发时间问题.....22
8.5 证书到期后，直接续费能继续服务吗？.....23
8.6 证书到期前，如何选择续费时间？.....23
8.7 吊销证书一直处于“审核中”状态怎么办？.....23
8.8 SSL证书服务控制台是否支持删除证书？.....23
9 选择证书相关问题..... 24
9.1 各类SSL证书的区别和网页展示效果.....24
9.2 多通配符域名和混合域名证书的申请方法.....24
9.3 如何选择：证书类型、证书品牌、保护域名数量？.....26
9.4 通配符域名证书都支持哪些域名？.....27

9.5 Digicert和GeoTrust证书支持苹果ATS和Android的哪些版本？ 28
10 申请证书相关问题 29
10.1 收费证书申请补全信息注意事项 29
10.2 证书订单异常问题 29
10.3 为什么收到了CA中心的通知，但订单状态没有变化？ 30
10.4 域名证书申请注意事项 30
10.5 不会申请证书或验证文件、资料不合规怎么办？ 31
10.6 证书配置的txt解析是否可以删除？ 31
10.7 购买证书后，如何提交或修改域名？ 31
10.8 未开启网站服务前是否可以申请HTTPS证书？ 31
10.9 OSS用户申请SSL证书注意事项 31
11 证书域名相关问题 33
11.1 如何填写证书申请中绑定的域名？ 33
12 证书审核相关问题 35
12.1 已购证书提交申请审核后需要做什么？ 35
12.2 证书审核加急服务 36
12.3 免费证书一直在审核中怎么办？ 36
13 证书部署到Web服务器上的相关问题 38
13.1 苹果ATS证书的选择及配置 38
14 证书部署到云产品相关问题 41
14.1 证书部署到云产品FAQ 41
14.2 如何将证书应用到阿里云的产品中？ 42
14.3 证书安装配置出错或网站无法访问怎么办？ 44
15 证书生效相关问题 45
15.1 服务器IP地址更换后原来的SSL证书能否生效？ 45
16 一键式HTTPS相关问题 46
16.1 一键式HTTPS套餐到期该怎么办？ 46
16.2 如何根据QPS阈值选择一键式HTTPS资源包套餐？ 46
16.3 网站QPS超过套餐内最大QPS后怎么办？ 47
16.4 已启用HTTPS服务的网站可以更换HTTPS套餐吗？ 48
16.5 证书到期后没有及时续费会怎么样？ 48

1 SSL证书常见问题概览

本文档介绍了阿里云SSL证书服务的各类常见问题、应用场景和对应的解决方案。

证书相关概念FAQ

什么是SSL证书?

SSL证书有什么优势?

什么是公钥和私钥?

HTTPS与HTTP有什么不同?

主流数字证书都有哪些格式?

证书应用场景

哪些网站必须启用HTTPS加密?

证书收费和开通问题

SSL证书收费方式

#unique_11

开通证书服务可以购买绑定了IP的证书吗?

证书地域相关问题

SSL证书地域说明

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?

证书有效期相关问题

SSL证书快过期了怎么办?

#unique_16

如何收到证书到期的系统通知?

证书订单时间和签发时间问题

吊销证书和删除证书有什么区别?

证书到期后，直接续费能继续服务吗?

SSL证书服务控制台是否支持删除证书?

#unique_22

证书到期前，如何选择续费时间？

吊销证书一直处于“审核中”状态怎么办？

如何选择证书

各类SSL证书的区别和网页展示效果

多通配符域名和混合域名证书的申请方法

如何选择：证书类型、证书品牌、保护域名数量？

通配符域名证书都支持哪些域名？

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

#unique_30

申请证书相关问题

收费证书申请补全信息注意事项

证书订单异常问题

#unique_33

#unique_34

为什么收到了CA中心的通知，但订单状态没有变化？

域名证书申请注意事项

#unique_37

证书配置的txt解析是否可以删除？

未开启网站服务前是否可以申请HTTPS证书？

购买证书后，如何提交或修改域名？

不会申请证书或验证文件、资料不合规怎么办？

证书域名相关问题

#unique_42

如何填写证书申请中绑定的域名？

#unique_44

#unique_45

#unique_46

#unique_47

证书审核相关问题

证书审核加急服务

#unique_49

#unique_50

#unique_51

#unique_52

已购证书提交申请审核后需要做什么?

免费证书一直在审核中怎么办?

配置和部署证书相关问题

#unique_55

#unique_56

Tomcat服务器安装SSL证书

#unique_58

#unique_59

#unique_60

#unique_61

#unique_62

#unique_63

苹果ATS证书的选择及配置

#unique_65

#unique_66

证书部署到云产品相关问题

证书部署到云产品FAQ

如何将证书应用到阿里云的产品中?

OSS用户申请SSL证书注意事项

证书生效相关问题

#unique_70

服务器IP地址更换后原来的SSL证书能否生效?

#unique_72

#unique_73

一键式HTTPS服务相关问题

#unique_74

一键式HTTPS套餐到期该怎么办?

如何根据QPS阈值选择一键式HTTPS资源包套餐?

网站QPS超过套餐内最大QPS后怎么办?

已启用HTTPS服务的网站可以更换HTTPS套餐吗?

证书到期后没有及时续费会怎么样?

浏览器访问相关问题

#unique_80

#unique_81

#unique_82

#unique_83

其他常见问题

Symantec SSL数字证书升级的影响与处理方案

#unique_85

证书安装配置出错或网站无法访问怎么办?

2 证书相关概念

2.1 什么是SSL证书？

SSL证书就是遵守SSL安全套接层协议的服务器数字证书，而SSL安全协议最初是由美国网景Netscape Communication公司设计开发，全称为安全套接层协议（Secure Sockets Layer）。

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，它为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。由于此协议很好地解决了互联网明文传输的不安全问题，很快得到了业界的支持，并已经成为国际标准。

SSL证书由浏览器中受信任的根证书颁发机构在验证服务器身份后颁发，具有网站身份验证和加密传输双重功能。

2.2 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 。

- **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。

2.3 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

> **说明：**
> 建议您使用2,048位加密长度的SHA256摘要算法。

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**

  1. 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。

  2. 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。

2.4 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。

2.5 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：

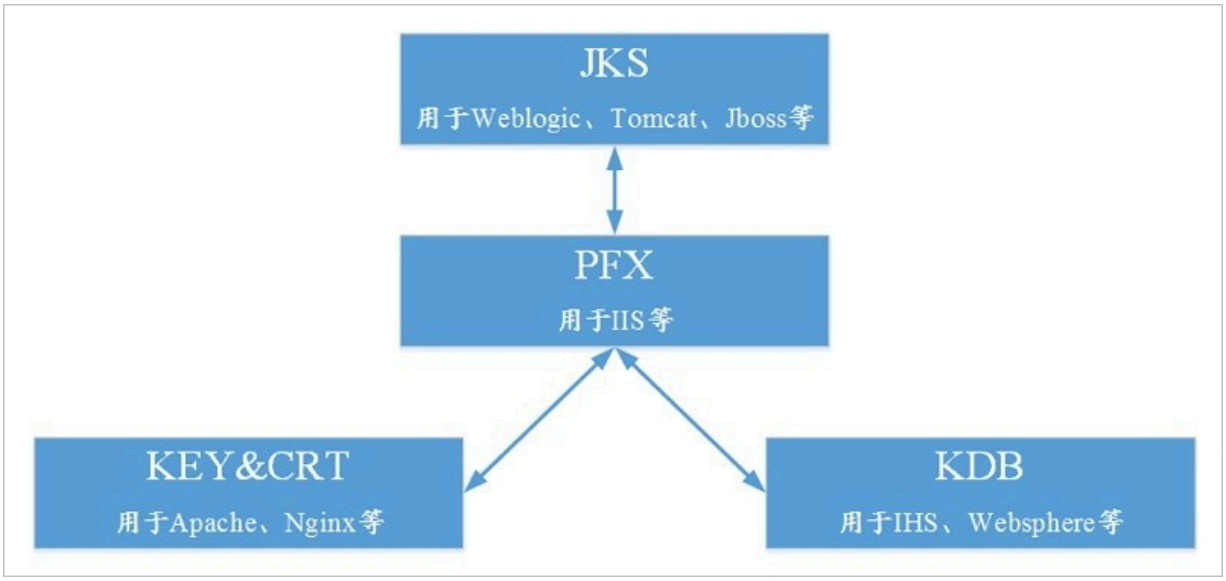
```
—–BEGIN CERTIFICATE—–
MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh.....
—–END CERTIFICATE—–
```

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。

3 证书应用场景

3.1 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。

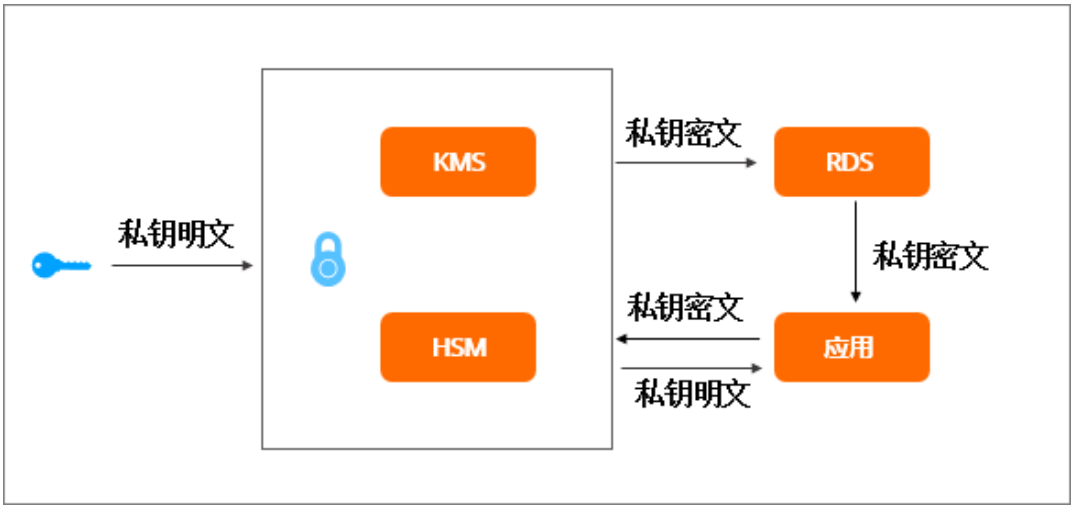
3.2 阿里云SSL证书私钥保护原理是怎样的？

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#unique_90。

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。


KMS
HSM
私钥明文
私钥密文
RDS
私钥密文
应用
私钥密文
私钥明文

4 证书收费和开通问题

4.1 SSL证书收费方式

SSL证书根据域名数量、购买年限、服务器数量收费，详情请参考#unique_92。

4.2 开通证书服务可以购买绑定了IP的证书吗？

公网IP是可以的。但是绑定了IP的证书，不支持应用在IE11以下版本的浏览器中。

5 免费证书相关问题

5.1 申请免费证书

阿里云SSL证书服务支持申请和签发免费证书。本文档介绍免费证书相关的常见问题和回答。

什么情况下可以申请免费证书？

申请免费证书前，请确认您已购买免费证书。

> **注意：**
> 您需要前往阿里云SSL证书购买页面先选择**单域名** > **DV SSL** > **免费版** > **DigiCert**，如果不按照此提示选择可能无法找到免费证书。

以下情况您可申请免费证书。

- 您的免费证书配额还有余额，也就是免费证书配额不为0。详细内容请参见我可以申请多少个免费证书？
- 您要保护的域名是在阿里云申请的、并且已通过阿里云完成域名的解析，您才可以申请免费证书。

  > **说明：**
  > 由于免费证书在阿里云平台中个人用户及测试用途的签发量非常大，为了提升您自动化签发证书的体验，需要把域名及云解析迁入阿里云，才可申请免费证书。

- 您需要保护的域名和网站为个人站点，并且每张免费证书只能绑定一个明细子域名。如果您需要使用一张证书绑定一个明细子域名，您可以申请免费证书。

  > **说明：**
  > - 如果您需要使用一张证书绑定多个域名或者通配符域名，免费证书无法满足该要求，您需要申请收费证书。
  > - 免费证书无SLA保证，建议商业化的网站签发收费证书。

我可以申请多少个免费证书？

每个阿里云用户最多可申请20张免费证书。如果您的阿里云账号下有免费证书过期后被删除或者未过期时被吊销并删除，就会释放出相应数量的免费证书配额，您可以重新再申请对应数量的免费证书。

> **说明：**

删除证书是指在阿里云SSL证书控制台中删除证书。已吊销但未删除证书以及已过期但未删除证书都会占用免费证书配额。

有关吊销和删除证书的详细内容，请参见吊销证书和删除证书有什么区别？

例如：您的阿里云账号下已申请了20张免费证书，此时您的免费证书可用配额为0，所以您无法再申请更多免费证书。但是，一段时间之后，您有2个免费证书过期了，您删除了这2张免费证书，此时您的免费证书可用配额为2个，所以您还可以重新申请2张免费证书。

我需要保护的域名是否适合使用免费证书？

免费证书仅适用于个人网站业务或测试用户。建议商业化的网站或企业、机构等网站使用收费证书。

免费证书安装与收费证书有什么区别吗？

免费证书安装与收费证书在安装操作上没有区别。

6 证书续费或升级相关问题

6.1 Symantec SSL数字证书升级的影响与处理方案

预计从2018年10月中旬，Google Chrome浏览器将不再信任Symantec及GeoTrust品牌的部分数字证书。为此Symantec针对Chrome浏览器发布了一项根证书升级计划。为了避免与Google Chrome浏览器相关的任何兼容性问题，建议您尽快参考本文档中的说明替换您购买的Symantec品牌证书。

受影响范围

属于以下时间范围内的Symantec品牌数字证书将受本次Symantec根证书升级计划影响，需要在指定时间前替换现有数字证书。

- 签发时间在2016年6月1日前且到期时间在2018年3月18日后的数字证书：

  您需要在2018年3月18日前完成证书替换，并且将替换后的证书重新部署。
- 签发时间在2016年6月1日后且到期时间在2018年9月13日后的数字证书：

  您需要在2018年9月13日前完成证书替换，并且将替换后的证书重新部署。

说明：
根据Symantec官方消息，自2017年12月1日起Symantec已经启用新的证书签发体系，在该时间点之后签发的数字证书完全符合谷歌的建议，将不再存在兼容性问题。

属于以下时间范围的Symantec数字证书不受本次根证书升级计划影响：

- 2016年6月1日前签发且2018年3月前到期的数字证书。
- 2016年6月1日后签发且2018年9月前到期的数字证书。

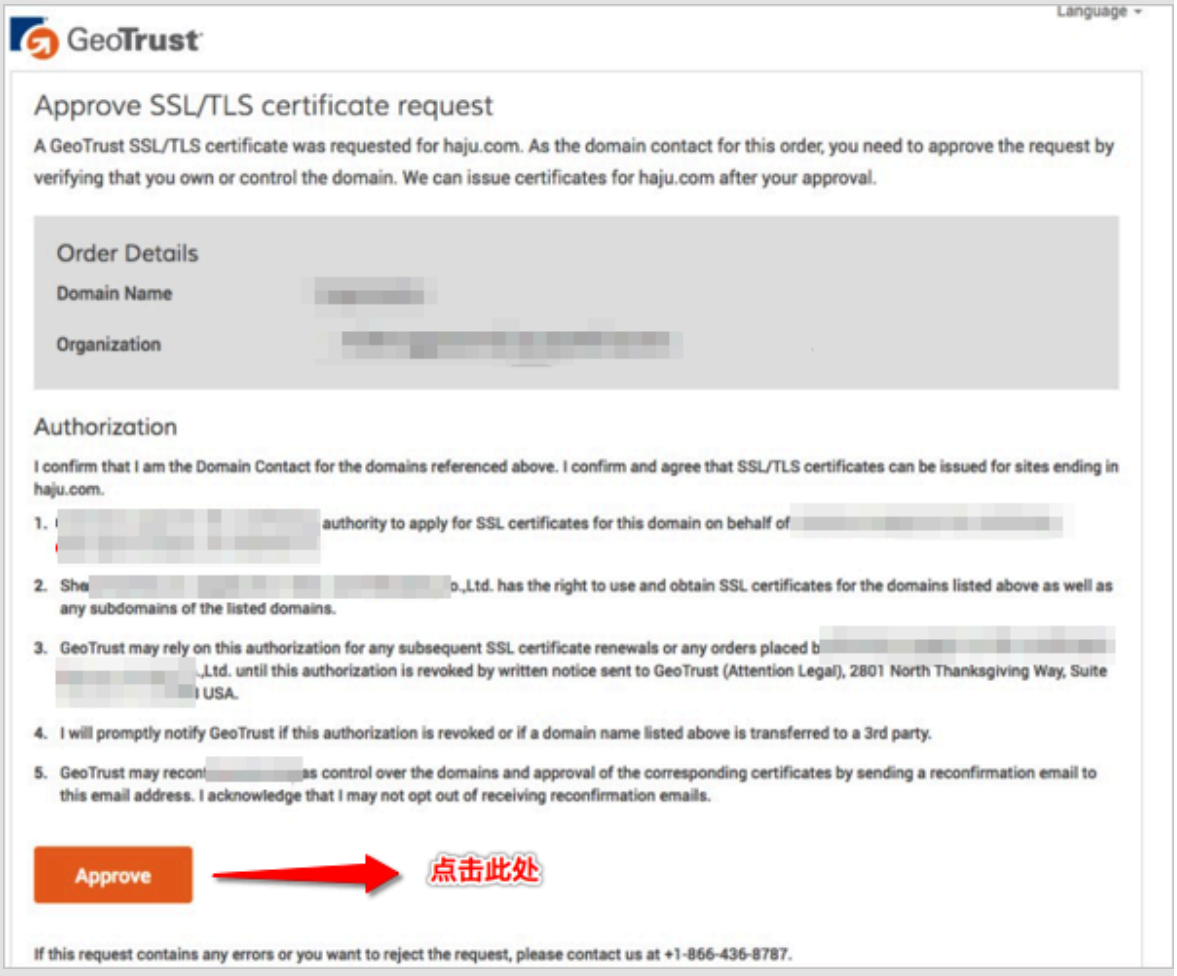
证书替换服务

自2018年6月起，阿里云证书服务已针对受影响范围内的Symantec数字证书启动证书的替换升级服务。

- 对于受影响范围内的OV/EV类型的数字证书，CA认证中心的审核人员将通过电话与您联系，经确认后将重新为您签发新的数字证书。

  说明：

如果您在SSL证书控制台中发现处于审核中状态的OV/EV类型证书订单，请您耐心等待CA中心审核人员的通知。在您收到来自CA认证中心的签发申请确认邮件后，请仔细阅读邮件内容后单击**同意**或**Approve**确认。

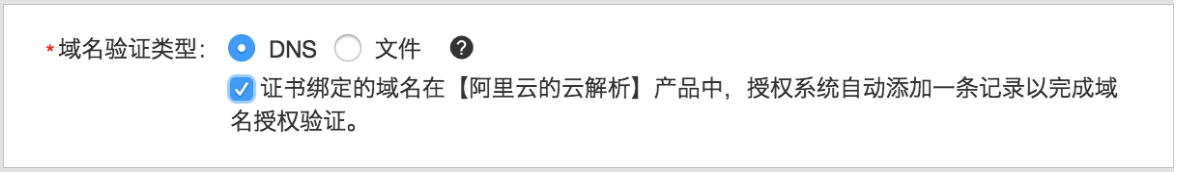


- 对于受影响范围内的DV类型的数字证书，阿里云工作人员将为您提交证书重签申请，您需要在SSL证书控制台中根据进度提示完成域名验证操作。

说明：

如果您原先的DV型数字证书订单符合以下条件，系统将尝试自动添加DNS解析记录帮助您完成域名验证：

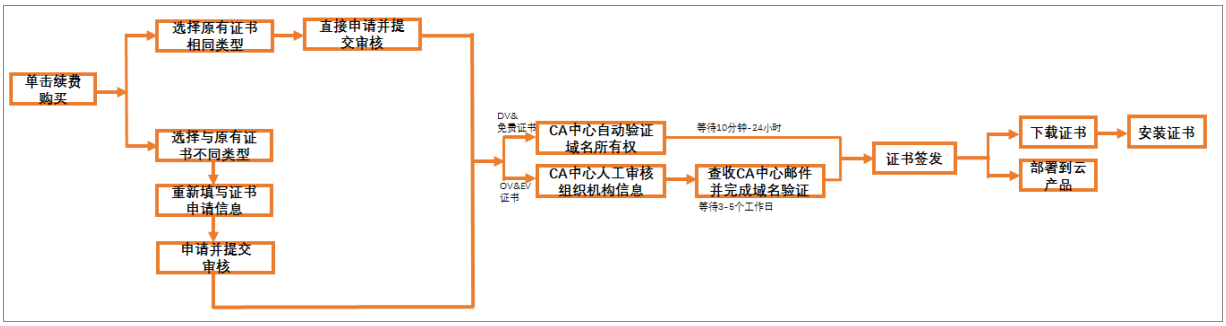
- 通过DNS方式完成域名验证
- 证书绑定的域名由云解析服务管理
- 已授权证书服务系统自动添加DNS解析记录



6.2 证书如何续费？

由于CA中心的规定，阿里云证书服务续费不支持自动续费，也不支持新旧证书在时间上的无缝连续。

证书的续费和新购证书流程一致，需要您在阿里云SSL证书控制台按照如下流程操作。详细操作指导请参见#unique_97。



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。

6.3 证书续费时选错了证书类型如何处理？

证书到期前，如果您为证书续费时选购了错误的证书类型，您可对该续费订单申请退款。

有关证书退款的详细说明，请参见#unique_99。

7 证书地域相关问题

7.1 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。

7.2 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。

8 证书有效期相关问题

8.1 如何收到证书到期的系统通知？

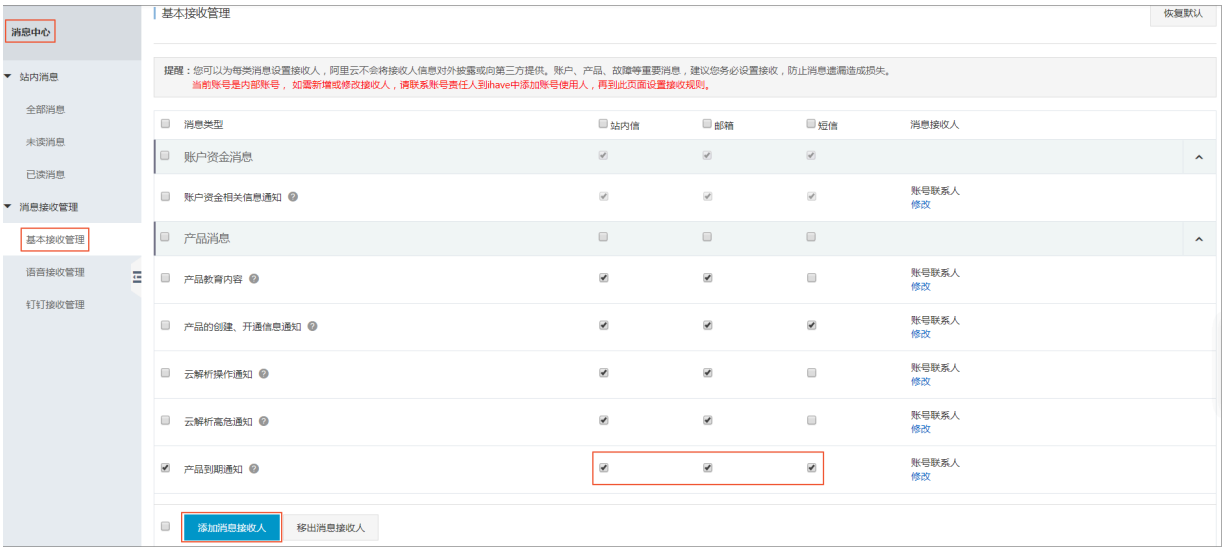
证书到期前一个月，阿里云SSL证书控制台会提示证书到期的信息。您也可以通过消息中心来设置是否需要接收证书相关的系统消息通知。如未设置消息中心的通知，您将不会收到证书到期的站内信、邮箱或手机短信通知。

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，您将接收到您勾选的消息类型相关的通知。

到期续费相关操作参见#unique_97。



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。

8.2 SSL证书快过期了怎么办？

SSL数字证书过期之后将无法继续使用，您需要在证书到期前及时续费，并重新绑定域名和提交审核。

审核通过后，您将获得一张新的数字证书，您需要在您的服务器上安装新的数字证书来替换即将过期的证书。

> **说明：**
> 证书到期前您需预留3-10个工作日重新购买，以免证书审核还未完成之前现有证书已经过期。

详细信息参见#unique_97。

8.3 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#unique_102。

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

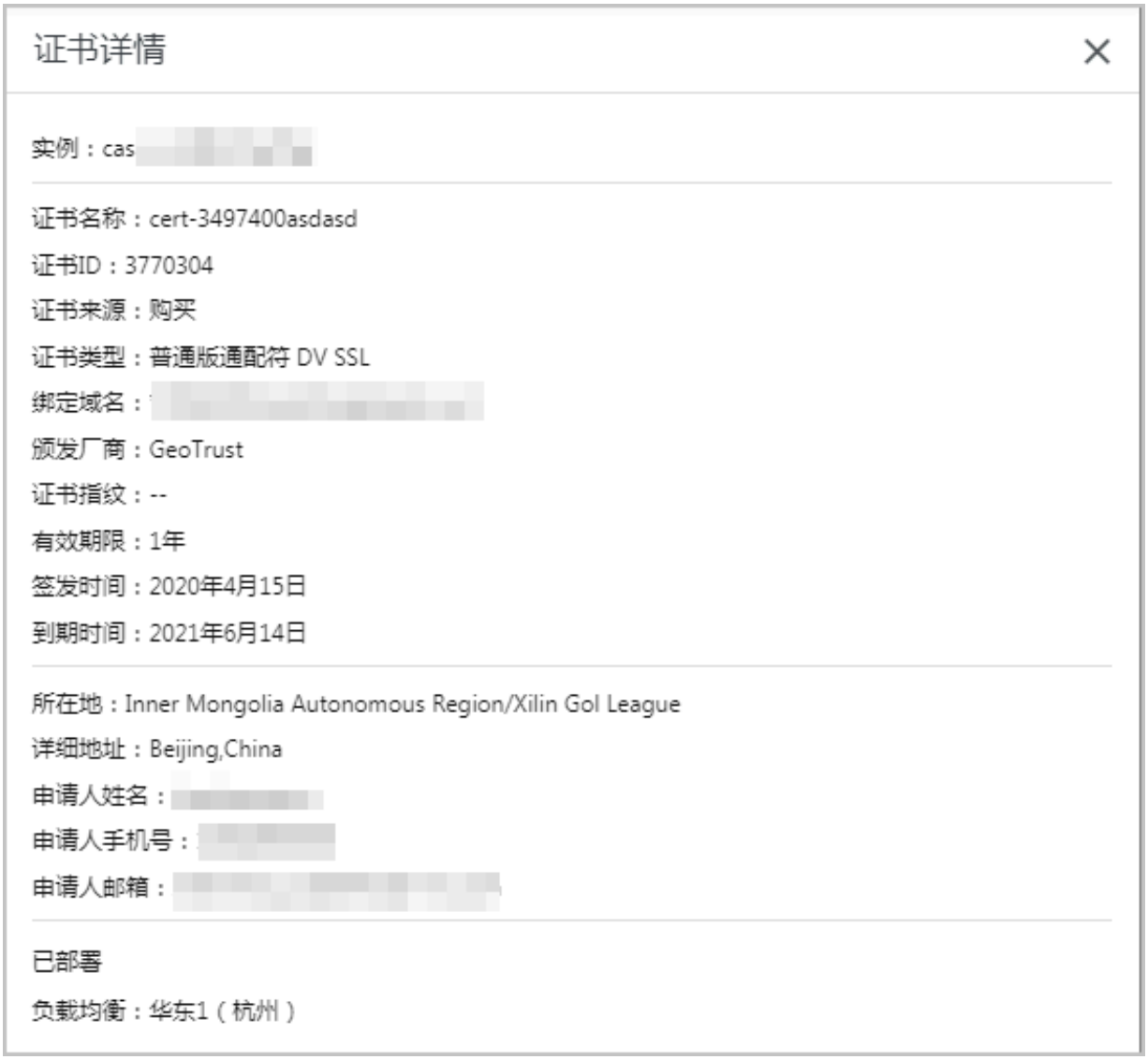
- 未过期的证书只有吊销后才可删除。
- 已过期的证书可以随时删除。

- 手动上传的证书可随时删除。

8.4 证书订单时间和签发时间问题

证书订单时间实际是指您下单购买证书并完成付款的时间；证书签发时间是指您提交证书申请并通过了CA中心的审核验证后，证书最终签发的时间。

SSL证书制作需要一定的周期，证书的有效期以证书的签发时间和结束时间为准，与订单时间无关。由于您购买证书后还需完成证书的申请和审核，并等待证书的签发，才算完成证书申请的完整流程。



说明：

如果您需要尽快使用证书，当您完成证书购买后请尽快提交证书申请直至证书签发，才可使用该证书。如果您仅完成了证书购买而未提交证书申请，您将无法使用该证书。

8.5 证书到期后，直接续费能继续服务吗？

不能。证书到期后，需要重新购买证书、提交证书申请审核、并等待证书重新签发后重新部署到您的Web服务器中。

8.6 证书到期前，如何选择续费时间？

证书有效期之前，您可以选择在证书到期前90天内进行续费。

证书续费相当于重新购买并申请新证书，部署到应用中。对于Digicert和GeoTrust品牌的证书，续费时，虽然重新购买了证书，但是原证书有效期限不会损失（Digicert的通配符DV SSL类型证书除外）。

您可以在证书到期前90天内续费，不仅原证书剩余有效期时间会自动追加到新签发的证书有效期时间上，而且证书机构还会赠送1个月以内的有效期叠加到新签发证书的有效期时间上。

8.7 吊销证书一直处于“审核中”状态怎么办？

收费证书吊销时，用户会收到一封证书吊销的确认邮件。用户通过邮件中的超链接，确认并批准吊销后，证书吊销才能完成。

如果无法进行邮件处理，用户需要提交工单申请强制吊销，强制吊销流程需要2个工作日完成。

8.8 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？

9 选择证书相关问题

9.1 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。

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。

9.2 多通配符域名和混合域名证书的申请方法

如果您申请的证书中需要包含一个或以上的通配符域名及一个或以上的普通域名，请参照本文的操作申请证书。

域名类型的详细解释，请参见如何填写证书中绑定的域名。

- 目前只有Digicert或GeoTrust品牌的专业版OV SSL证书支持该功能，其他类型证书不支持该功能。

- 您需要整理绑定的域名、通配符域名数量、普通域名数量，该证书要求至少要有一个普通域名。

  关于通配符域名的匹配关系，请参见“所有子域名”类型的通配符证书都支持哪些域名。

  说明:
  一定要购买同品牌同时长（例如1年）的证书，否则无法合并证书。

示例

以下举例以您购买3个多域名的Digicert品牌专业版OV SSL为例。

1. 需要购买多域名证书（域名个数选择3）。订单域名类型数量之和与您要绑定的域名类型数量一致即可。

2. 购买成功后，请您不要对订单做任何操作。
3. 提交工单给阿里云。
   - 工单标题： 多域名证书合并
   - 工单内容： 将要合并的订单截屏并提交要合并的域名。如：主域名a.com（显示这张证书颁发给a.com）、追加域名b.com/ a.com、*.p.a.com、 *.p.b.com
   - 工单类型： 加急工单

4. 阿里云审核通过后，与合并相关的订单只会保留一个，您的其它订单将会被关闭，关闭后将无法打开。选择可编辑的订单，去绑定域名，绑定域名的时候会提示填写多少个普通域名和通配符域名。

   说明：
   第一个域名一定是普通域名。具体内容请参见如何填写证书中绑定的域名。

   建议您在生成CSR步骤中选择系统创建CSR。如果手动创建CSR，请将域名列表中的第一个域名即某个普通域名作为CSR的Common Name属性。关于如何制作CSR，详细操作请参见如何制作CSR文件。
5. 提交资料等待审核。
6. 耐心等待3~5个工作日，期间请保持公司电话和申请人手机畅通。

9.3 如何选择：证书类型、证书品牌、保护域名数量？

证书类型的选择

- 如果您的网站主体是个人（即没有企业营业执照），只能申请免费型或DV型数字证书。
- 对于一般企业，建议购买OV及以上类型的数字证书。对于金融、支付类企业，建议购买EV型证书。
- 移动端网站或接口调用，建议您使用OV及以上类型的证书。

说明：
Digicert品牌的EV型证书有服务器IP限制。如果您的一个域名有多个主机IP，建议您购买多张数字证书。如果您同时还使用了阿里云的其它云产品，选择其中一张证书上传到对应的云产品中即可。

品牌选择

- 各数字证书品牌兼容性从强到弱的顺序：Digicert > GeoTrust > CFCA。
- 移动端网站或接口调用相关的应用，建议您选择Digicert品牌。

保护域名数量

- 一个域名：该数字证书只能配置一个具体的域名。
- 多个域名：该数字证书可配置多个具体的域名。这些域名可以是一个顶级域也可以是非顶级域名，例如p1.taobao.com、p1.aliyun.com 等。

- 通配符域名：该数字证书可配置一个通配符域名。通配符域名一般格式为*.aliyun.com。

  通配符域名仅支持同级匹配，例如绑定*.aliyun.com通配符域名的数字证书，支持p1.aliyun.com，但不支持p2.p1.aliyun.com。如果你需要支持p2.p1.aliyun.com的通配符域名数字证书，则还需要购买一张*.p1.aliyun.com的通配符域名证书。

说明：

- 通配符域名的数字证书中，仅根域名包含域名主体本身。例如：
  - *.aliyun.com的通配符域名数字证书包含了aliyun.com。
  - *.p1.aliyun.com的通配符域名数字证书不包含p1.aliyun.com。
- 具体的域名中如果填写的是www域名，则包含了主域名本身。例如：
  - www.aliyun.com域名绑定的数字证书包含了aliyun.com。
  - www.p1.aliyun.com域名绑定的数字证书不包含p1.aliyun.com。
- 您的数字证书一旦颁发后，将无法修改域名信息等。

9.4 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别子域名。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）。如需一张证书能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。

9.5 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）。

10 申请证书相关问题

10.1 收费证书申请补全信息注意事项

在申请收费证书时，您需要补全信息，请注意以下几个关键信息的准确性，信息准确可保证证书在第一时间签发。

公司名称：公司名称要与营业执照上的公司名称保持完全一致。

公司电话：非常重要，公司电话最好写成第三方公共信息平台（114）上可查到的电话或者工商局登记的电话，鉴证人员通过该电话直接或间接（请接电话人员提供证书联系人电话号码）联系到证书联系人，与证书联系人确认证书申请事宜和信息，请保持电话畅通。

申请确认Email

- 非常重要，请确保该邮箱地址为申请证书的联系人邮箱地址。
- 当涉及到签证域名相关信息确认时，需要保证域名管理员邮箱可对签证信息进行回复。
- 如果在申请证书时，联系人、电话为域名管理员，申请确认Email为域名管理员邮箱（后续相关证书签信息的确认、变改都会发到该域名管理员邮箱），这样会使得签证流程最顺利。
- 当申请的证书为EV证书时，邮箱必需为企业邮箱或者收费邮箱，不能为免费邮箱。
- 域名需关闭域名保护功能，这样签证人员才可以查到你的域名对应的域名管理员邮箱。

10.2 证书订单异常问题

由于操作失误，将订单关闭了，该怎么办？

请提交工单，与技术支持人员确认是否能重新开启该证书订单。

订单已经提交了，但是有信息填写错误，该怎么办？

- 如果错误信息不影响证书的审核、证书的颁发及使用，可不修改。
- 如果确实需要进行修改，请提交工单，与技术支持人员确认是否能重新开启该证书订单，并修改相应信息。

说明:

请您务必正确填写信息，谨慎操作。

申请证书时出现订单处理异常，该怎么办？

购买了证书后，如果单击**申请证书**后控制台提示“订单处理异常”，您可以更换浏览器重新申请证书。

10.3 为什么收到了CA中心的通知，但订单状态没有变化？

在资料审核环节和证书颁发环节，CA中心可能会发送一封邮件通知您申请证书的进展。如果您发现阿里云证书控制台中的订单状态还没有发生变化，此时需要您再耐心等待一段时间才能看到订单的状态变化。因为CA中心给阿里云推送的订单状态会有延迟。

10.4 域名证书申请注意事项

自动签发

您可以在域名服务控制台自动签发域名关联证书，而无需在申请证书后配置证书签发验证文件。自动签发有如下前提条件：

- 域名在阿里云万网。
- 云解析在阿里云。

  如果云解析不在阿里云，证书申请后，无法完成自动签发。如果用户无配置DNS解析能力，建议把DNS解析转入阿里云，授权后台自动进行DNS验证解析记录配置，这样才可完成签发。否则，需用户自行去阿里云SSL证书控制台，购买DV收费证书后，根据控制台进度中DNS验证解析配置要求，去第三方的DNS解析控制台配置指定的TXT验证解析，用于证明用户对该域名的管理权，才可签发证书。

  当有大量的证书签发需求时，建议您把DNS解析转入阿里云，可以大量简化证书申请及管理工作量。
- 域名经过实名认证。
- 域名在有效期内。

免费证书

- 域名及解析需在阿里云，才可签发免费证书。

  免费证书在阿里云平台中个人用户及测试用途的签发量非常大，为了改善用户自动化签发交互体验，需请用户把域名及云解析迁入阿里云，才可完成免费证书签发。
- 免费证书无SLA保证，建议商业化的网站签发收费证书。

证书相关问题，请提云盾证书服务工单联系我们。感谢您对阿里云的支持！

10.5 不会申请证书或验证文件、资料不合规怎么办？

如果您急需对证书选型、验证证书申请文件或在申请证书过程中任何操作上的指导，都可申请SSL证书辅助服务。

您可前往阿里云云市场购买证书申请技术辅助服务。

10.6 证书配置的txt解析是否可以删除？

客户证书申请完成后，可以删除证书配置的txt解析。

证书申请完成后，删除证书配置的txt解析，对证书无影响。

10.7 购买证书后，如何提交或修改域名？

选择购买GeoTrust的高级版EV SSL类型证书，并选择保护域名5个，并下单成功。您可在SSL证书服务控制台，申请证书时，填写5个待绑定的保护域名，然后提交审核。

- 证书签发后，30天内，如果需要变更域名，您需要取消订单并重新下单申请签发证书。
- 证书签发后，超过30天之后，不能删除主域名，只能删除附加域名，且删除附加域名不会退款。不支持域名更改操作，只支持域名删除和新增操作。

10.8 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。

10.9 OSS用户申请SSL证书注意事项

本文档介绍了阿里云OSS用户申请SSL证书的注意事项。

您可以登录OSS管理控制台对证书进行以下操作：

- 申请签发新的SSL证书。
- 上传已有证书进行托管。

OSS用户申请SSL证书的具体操作，请参见#unique_105。

付费版本GeoTrust通配符DV SSL证书

GeoTrust是全球第二大数字证书颁发机构。该类型证书可以保护1个通配符域名的同级所有子域名，采用SHA-256和2,048位加密技术。支持文件或DNS方式验证域名授权。系统自动检查域名授权配置，无需人工审核。

说明：

如果您的域名解析不在阿里云，您申请证书后，您的证书将无法完成自动签发，需要您登录阿里云SSL证书控制台按照**状态**提示自行配置。

如果您无法配置DNS解析，建议把DNS解析转入阿里云，授权后台自动进行DNS验证解析记录配置，这样就能完成签发。否则，需要您登录阿里云SSL证书控制台购买DV收费证书后，根据控制台进度中DNS验证解析的配置要求，去第三方的DNS解析控制台配置指定的TXT验证解析，用于证明您对该域名的管理权，方可签发证书。

如果您有大量的证书签发需求，建议您把DNS解析转入阿里云，可以大量简化您的证书申请及管理的工作量。

免费版DigiCert单域名DV SSL证书

您的域名及解析需在阿里云，才可签发免费证书。个人用户及测试用途的免费证书在阿里云平台中的签发量非常大，为了改善您自动化签发的交互体验，请您把域名及云解析迁入阿里云，方可完成免费证书的签发。

说明：

通过OSS控制台在一天内签发的免费证书的数量最多为20张。当您一天的配额用完时，只能等到第二天（24小时后）才可以继续签发新的免费证书。因此您的阿里云实名认证账号，一年签发的免费证书最多为7,300张。上述免费证书的数量限制仅限制从OSS、域名、DNS等云产品申请免费证书；从阿里云售卖系统购买的免费证书，您最多可以申请20张。

由于免费证书无SLA保证，建议您的正式商用网站签发收费的证书。

如果您有证书相关的其他问题，请您登录阿里云SSL证书控制台提交工单联系我们。

11 证书域名相关问题

11.1 如何填写证书申请中绑定的域名？

当您完成SSL证书购买后，需要在阿里云SSL证书控制台补全证书申请的审核资料。

SSL证书控制台会根据您购买的证书提示您需要输入的域名类型和数量。

说明：

当您申请证书时需正确填写证书绑定的域名信息，才能保证您的数字证书顺利颁发并成功开启HTTPS服务。

什么是通配符域名？

通配符域名是指以 *. 号开头的域名。例如：*.a.com 是正确的通配符域名， *.*.a.com 则是错误的通配符域名。

说明：

一个通配符域名只能算一个域名。关于通配符的匹配关系，请参考“所有子域名”类型的通配符证书都支持哪些域名？

什么是普通域名？

普通域名是相对于通配符域名来命名的，是指一个具体的域名或者说不是通配符域名。例如：www.a.com 或 a.com 都算一个普通域名。

普通域名能被证书绑定的数量，取决于您证书订单中选择的域名个数。

域名信息与CSR的关系

- 手动填写CSR文件

  CSR文件中的域名信息（CN属性）必须是您证书绑定域名中的其中一个。当您的域名信息中同时有通配符域名和普通域名时，请您使用普通域名作为CSR文件中的CN属性值。关于CSR文件的更多说明，请参见如何制作CSR文件？

- 系统生成CSR文件

  系统会自动选择您填写的第一个域名作为CSR文件中的CN属性值。因此，当您的域名信息中同时有通配符域名和普通域名时，请您将普通域名放在第一个域名的位置。

注意事项

如果您已购买免费类型和DV类型的证书，当您填写的域名是当前主域名的子域名，选择文件验证域名所有权类型时，CA中心返回的域名是您的主域名。例如：您申请证书的时候填写证书绑定的域名是www.aliyun.com，那么需要验证的域名是aliyun.com。

12 证书审核相关问题

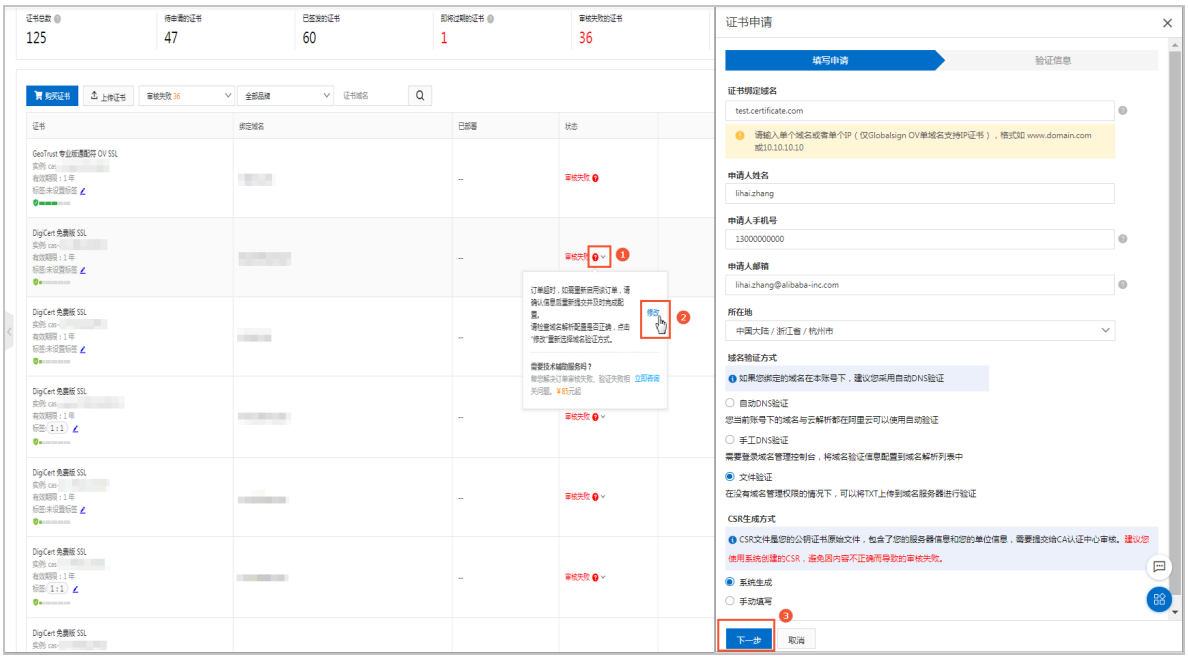
12.1 已购证书提交申请审核后需要做什么？

您购买SSL证书后需申请证书并提交审核，审核通过后才能使用该证书并将证书部署到您的服务器上。

当您的证书订单提交审核后，CA中心工作人员会联系您确认证书审核的相关信息。请您随时保持手机畅通（提交审核时填写的个人手机号码），并及时查看您的邮箱（提交审核时填写的邮箱），以免错过CA中心发送的确认通知。

当您的证书订单提交审核后，您可以登录阿里云SSL证书控制台，在**未签发**的证书页面，查看您证书审核申请的状态和后续流程。您的证书订单提交审核后，包含以下两种状态：

- **审核中**：证书申请为审核中的状态时，您需等待审核完成。证书状态为**已签发**后才能使用该证书。有关证书审核时长详细内容，请参见OV、EV证书审核时长和DV、免费证书审核时长。
- **审核失败**：证书审核失败时，您需根据该证书状态栏的提示信息，确认证书审核失败的原因，并根据失败原因提示修改证书申请信息，修改完成后您需要重新提交申请。 鼠标移动到该证书的状态栏可查看证书审核失败的原因说明，具体如何处理请参见#unique_49。



- ①：单击审核失败的提示按钮，查看证书审核失败的原因说明。
- ②：根据证书审核失败的原因说明，修改证书的申请信息。
- ③：证书的申请信息修改完成后，单击**下一步**重新提交申请。

OV、EV类型证书审核时长

如果您购买的是OV或EV类型证书，您需要耐心等待3~7个工作日。CA中心会在3~7个工作日内完成您的证书订单审核。

如果审核期间有任何问题，CA中心的客服人员会通过电话联系您并指导您进行相关操作，请务必确保您的联系电话在审核期间保持畅通。如果CA中心无法及时联系到您，那么该订单的审核进度将可能会延迟。您的**及时回复**将能**有效缩短**SSL证书的验证时间。

DV型或免费型证书审核时长

您需要按照证书订单进度页面的提示完成域名授权验证配置，并提交审核。域名授权验证完成后，CA中心将会在1~2个工作日内签发您的证书。

如果您的域名中包含某些敏感词（例如bank、pay、live等），可能会触发人工审核机制，审核时间会比较长，请您耐心等待。

有关域名授权配置的更多内容请参见如何配置域名授权验证。

说明:
免费型证书申请后会在1~2个工作日内签发。根据CA中心审核流程耗时不同，您的证书有可能会在几个小时内就完成签发，也有可能需要2个工作日才能完成签发，请您耐心等待。

12.2 证书审核加急服务

如果您需要加快证书审核流程，可申请证书审核加急的第三方服务。

您可前往阿里云云市场购买SSL证书初审加急服务。

说明:
DV证书用户暂不支持证书审核加急。

12.3 免费证书一直在审核中怎么办？

本文档介绍了申请免费证书审核的时长，以及证书申请提交审核后，您需要及时完成的操作。

DV型或免费型证书审核时长

您需要按照证书订单进度页面的提示完成域名授权验证配置，并提交审核。域名授权验证完成后，CA中心将会在1~2个工作日内签发您的证书。

如果您的域名中包含某些敏感词（例如bank、pay、live等），可能会触发人工审核机制，审核时间会比较长，请您耐心等待。

有关域名授权配置的更多内容请参见如何配置域名授权验证。

说明:

免费型证书申请后会在1~2个工作日内签发。根据CA中心审核流程耗时不同，您的证书有可能会在几个小时内就完成签发，也有可能需要2个工作日才能完成签发，请您耐心等待。

证书申请验证时长说明

- 超过1小时的订单，每小时检验一次域名所有权，检测通过后，会立即签发证书。
- 1小时内的订单，每10分钟验证一次。
- CA机构通过自动化无人工干预系统完成审核，请及时自助完成域名所有权验证流程，详细内容请参见#unique_44

  当您的证书订单提交审核后，CA中心工作人员会联系您确认证书审核的相关信息。请您随时保持手机畅通（提交审核时填写的个人手机号码），并及时查看您的邮箱（提交审核时填写的邮箱），以免错过CA中心发送的确认通知。

13 证书部署到Web服务器上的相关问题

13.1 苹果ATS证书的选择及配置

自2017年1月1日起，根据苹果公司要求，所有iOS应用必须使用ATS（App Transport Security），即iOS应用内的连接必须使用安全的HTTPS连接。

说明：

您的阿里云的CDN、SLB服务中的HTTPS配置完全符合ATS的要求。

苹果ATS针对HTTPS协议有如下四个方面的要求。

证书颁发机构的要求

- 建议您使用DigiCert、GeoTrust品牌的OV型及以上数字证书。
- 对于个人用户，建议您使用DV型数字证书，不推荐使用免费证书。
- CFCA品牌的数字证书只在最新的苹果设备上才支持，因此不推荐您选择CFCA品牌。

证书的哈希算法和密钥长度的要求

- 哈希算法：上述推荐的证书品牌中使用的哈希算法都是SHA256或者更高强度的算法，符合ATS的要求。
- 密钥长度：
  - 如果您选择使用系统生成CSR的方式，系统生成的密钥采用的是2,048位的RSA加密算法，完全符合ATS的要求。
  - 如果您选择手动填写CSR文件，请确保使用2,048位或以上的RSA加密算法。

传输协议的要求

您的Web服务器上的传输协议必须满足TLS1.2，需要您在Web服务器上开启TLSv1.2，要求如下：

- 基于OpenSSL环境的Web服务器，需要您使用OpenSSL 1.0及以上版本，推荐您使用OpenSSL 1.0.1及以上版本。
- 基于Java环境的Web服务器，需要您使用JDK 1.7及以上版本。
- 其他Web服务器，除IIS7.5以及Weblogic 10.3.6比较特殊外，只要Web服务器版本满足要求，默认均开启TLSv1.2。

Web服务器的详细配置要求如下：

- Apache、Nginx Web服务器需要您使用OpenSSL 1.0及以上版本来支持TLSv1.2。

- Tomcat 7及以上版本Web服务器需要您使用JDK 7.0及以上版本来支持TLSv1.2。
- IIS 7.5 Web服务器默认不开启TLSv1.2，需要您修改注册表来开启TLSv1.2。

  下载并导入ats.reg 注册表脚本后，需要您重启或注销服务器，即可使TLSv1.2 生效。
- IBM Domino Server 9.0.1 FP3 Web服务器支持TLSv1.2。根据ATS要求，建议您使用IBM Domino Server 9.0.1 FP5版本。更多信息请参见：
  - IBM Notes and Domino wiki
  - IBM HTTP SSL Server Questions and Answers
- IBM HTTP Server 8.0及以上版本支持TLSv1.2。根据ATS要求，建议您使用IBM HTTP Server 8.5及以上版本。
- Weblogic 10.3.6及以上版本Web服务器需要您使用Java 7及以上版本来支持TLSv1.2。

  说明：
  Weblogic 10.3.6中存在多个SHA256兼容性问题，建议您使用Weblogic 12及以上版本，或者需要你为Weblogic 10.3.6配置前端Apache和Nginx的HTTPS代理或SSL前端负载。
- Webspere V7.0.0.23及以上版本、Webspere V8.0.0.3及以上版本、Webspere V8.5.0.0及以上版本支持TLSv1.2。关于如何配置Webspere服务器支持TLSv1.2，请参见Configure websphere application server SSL protocol to TLSv1.2。

签字算法的要求

签字算法必须满足如下算法要求：

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

配置示例

以下通过举例方式说明不同Web服务器的ATS协议及加密套件的配置方法。

说明：

示例中只列举了与ATS协议有关的属性，请不要完全复制以下配置用于您的实际环境。

Nginx配置文件片段

Nginx配置文件中ssl_ciphers及ssl_protocols属性与ATS协议有关。

```
server {
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!
MD5:!ADH:!RC4;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
}
```

Tomcat配置文件片段

Tomcat配置文件中的SSLProtocol及SSLCipherSuite属性与ATS协议有关。

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
scheme="https" secure="true"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
SSLCipherSuite="ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL
:!MD5:!ADH:!RC4" />
```

IIS系列Web服务器的配置方法，请参见Enabling TLS 1.2 on IIS 7.5 for 256-bit cipher strength。

您也可以使用可视化配置插件进行配置，请参见IIS Crypto。

ATS检测工具

您可以在苹果电脑中使用系统自带的工具进行ATS检测，执行以下命令即可：`nscurl --ats-diagnostics --verbose 网址`。

14 证书部署到云产品相关问题

14.1 证书部署到云产品FAQ

通过阿里云SSL证书服务管理控制台购买的SSL数字证书，支持一键部署到阿里云CDN、SCDN、DCDN和负载均衡（SLB）中。

如果您没有购买对应的云产品，或您的数字证书所绑定的域名没有在对应的云产品中开通服务，证书部署到云产品可能会失败。

> **说明：**
> 此处负载均衡（SLB）服务除外，即使未开通服务也可部署成功。

SSL证书是否支持跨阿里云账号推送云产品？

不支持。

当证书成功部署到云产品中，就意味着该云产品已经正确启用HTTPS服务了吗？

不是，您还需要到对应的云产品管理控制台中进行对应的参数配置。另外，您也需要确认您的源站是否已经准备好启用HTTPS服务。

云产品的参数配置说明的详细内容，请参见SLB证书管理和CDN证书配置。

部署到CDN时没有查询到域名，为什么？

当证书服务向CDN服务部署数字证书时，首先会查询CDN中可用的域名与数字证书中的域名是否匹配。因此，出现该问题可能的原因是您在CDN管理控制台中没有配置或者启用数字证书绑定的域名。

请您先到CDN管理控制台中添加您的数字证书所绑定的域名，并且设置成启用状态。详细信息参见CDN证书配置文档。

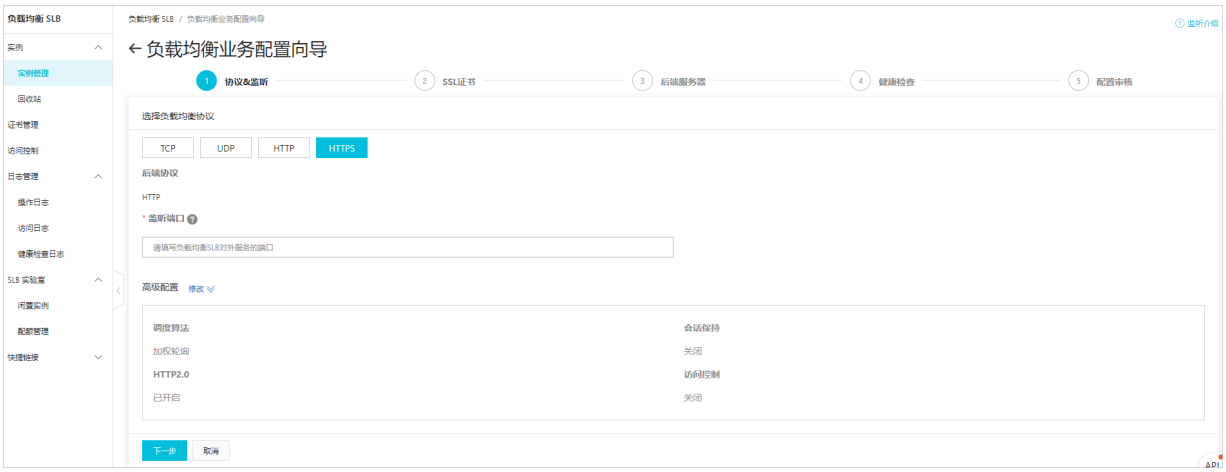
> **说明：**
> CDN管理控制台中的域名列表，域名状态为**正常运行**时才能被SSL证书服务查询到并进行部署。

部署到负载均衡（SLB）时都会部署到哪些地域？

证书服务会将SSL证书在所有的地域都部署一份。取消部署时，证书服务会将已经部署的地域中的数字证书删除掉。

您可以在**负载均衡管理控制台** > **证书管理**中，查看地域。如果列表中没有地域项，单击 ，进入自定义列表项，勾选**地域**，单击**确认**。

成功部署至负载均衡（SLB）各地域之后，您可在**负载均衡管理控制台** > **实例管理**中，选择您的负载均衡实例，单击**管理**。在监听页面，单击**添加监听**，配置监听信息，并选择该数字证书。



说明：

请注意选择的数字证书与绑定域名的对应关系。

在SSL控制台修改证书信息后还需再次部署到云产品吗？

是的，SSL证书名称修改后需重新部署到相关的云产品，修改的证书信息才能同步到云产品中。部署证书的详细指导操作，请参见#unique_112。

如未重新部署，云产品中该证书信息将与修改后的证书信息不一致。

14.2 如何将证书应用到阿里云的产品中？

部署到阿里云其它云产品

数字证书签发后，您可以通过推送功能将数字证书一键部署到阿里云其它云产品。

目前已支持的阿里云产品包括：CDN、SCDN、DCDN和负载均衡（SLB）。

如果您在部署到阿里云其它云产品过程中遇到问题，请参见证书部署到云产品常见问题。

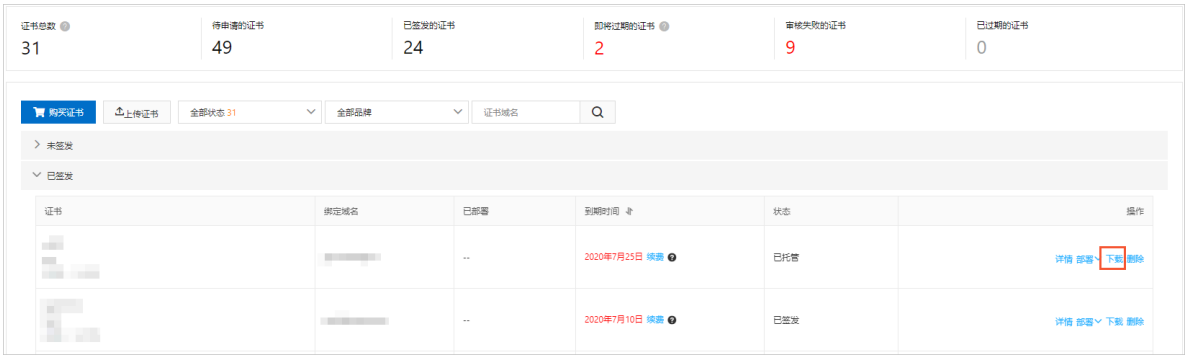
说明：

将数字证书部署到阿里云其它产品之前，请确认该账号已购买了相应的阿里云产品，并且已为该数字证书绑定的域名开通了云产品服务，否则将无法完成部署。

下载数字证书并部署到其它产品

如果您需要将您的数字证书部署到其他产品中，您可通过以下步骤将您的数字证书下载到本地：

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**已签发**证书列表中定位到需要下载的证书，单击**下载**。



4. 在**证书下载**页面对应的**服务器类型**的**操作**栏，单击**下载**，即可下载PEM格式证书文件至本地。

5. 登录相应的云产品控制台，上传数字证书并进行部署。

14.3 证书安装配置出错或网站无法访问怎么办？

如果您需要证书配置支持或出现配置出错以及部署证书后无法访问网站的情况，可申请第三方技术辅助服务。

您可前往阿里云云市场购买证书安装和检测技术服务。

15 证书生效相关问题

15.1 服务器IP地址更换后原来的SSL证书能否生效？

SSL证书都是绑定域名的，不受服务器更换IP地址的影响。只要证书绑定的域名不变，就可以重新解析到新的IP地址，原来的SSL证书仍然可以生效，不需要更换新的证书。

16 一键式HTTPS相关问题

16.1 一键式HTTPS套餐到期该怎么办？

购买了一键式HTTPS套餐后如果一直未启用，该套餐到期后将自动失效。如果应用在网站上，则可能导致当前网站不可访问。为避免您的网站出现不可访问的情况，您需要及时续费套餐。

解决方法

- 原套餐续费的方式实现，到控制台**资源包管理**页面中，找到对应的套餐。

  1. 在阿里云SSL证书控制台打开**一键式HTTPS**页面，单击**资源包管理**。
  2. 在**资源包管理**页面，定位要需要续费的资源包，单击**套餐续费**，按照系统提示完成续费付款。

     完成续费后，该套餐的到期时间会延长到续费的日期。

- 如果需要调整套餐的参数，可采用升级新购的方式。
  - 在阿里云SSL证书控制台打开**一键式HTTPS**页面，单击**资源包管理** > **购买资源包**，按照系统提示完成付款。
  - 在阿里云SSL证书控制台打开**一键式HTTPS**页面，单击**域名管理** > **套餐升级**，选择新的套餐并根据系统提示完成付款。

16.2 如何根据QPS阈值选择一键式HTTPS资源包套餐？

一键式HTTPS服务支持基础版、专业版和企业版套餐，不同版本的套餐支持的网站QPS阈值不同。您需要根据您网站的常规业务情况预估网站的QPS阈值，确定需要选购的套餐版本。

套餐QPS阈值

基本配置	基础版	专业版	企业版
每天业务访问网络流量（QPS） **说明：** 网站QPS指的是当日00:00:00到23:59:59之间访问该网站的每秒请求数。	10 QPS/天	30 QPS/天	100 QPS/天

网站QPS计算方法

一键式HTTPS服务每隔10秒统计一次所保护网站的QPS阈值（即峰值），根据QPS峰值大小排序，选取最高QPS峰值点作为当日该网站的最终QPS峰值。如果您当前业务的实际QPS峰值已经超过了所购买的一键式HTTPS套餐中支持的阈值，您需要升级一键式HTTPS服务套餐。

说明：

只要该网站当日存在访问请求，则QPS峰值最小为1。

相关文档

网站QPS超过套餐内最大QPS后怎么办？

16.3 网站QPS超过套餐内最大QPS后怎么办？

您网站实际QPS峰值超过购买一键式HTTPS服务时套餐的QPS阈值时，该网站可能会出现限速的问题。建议您实时关注网站的QPS阈值并采取对应的应对措施。

问题描述

如果您网站实际QPS峰值超过了购买一键式HTTPS服务时套餐的QPS阈值，一键式HTTPS控制台**网站预警**页面会提示您最大QPS值。

如果24小时内网站的最大QPS值超过了购买套餐QSP阈值的10%，网站会被限速。

说明：

如果24小时内网站的最大QPS值未超出购买套餐QSP阈值的10%，一键式HTTPS服务不会采取任何限制，仅通过邮件、短信和站内信方式为您发送**QPS超量提醒**告警信息。

解决方法

1. 在一键式HTTPS控制台**网站预警**页面单击**查看详情**，查看最大QPS发生前后几个小时内的流量数据。

   说明:
   随着时间的变化，该数据可能会被清理。

2. 确定QPS最大值已超过套餐阈值的10%后，单击**升级套餐**，购买更高规格的资源包套餐。

   说明:
   请及时升级您的套餐，避免出现网站被限速的情况。

16.4 已启用HTTPS服务的网站可以更换HTTPS套餐吗？

启用一键式HTTPS服务后，如果该HTTPS服务套餐无法满足您网站的需求，您可以升级该域名的HTTPS服务套餐。原有的套餐因为已与该网站域名解绑，可以配置到其它网站中使用。

如果购买一键式HTTPS服务时，选择的证书类型是**GeoTrust通配符**或**Digicert DV通配符**（原Symantec）收费证书（即购买了一键式HTTPS服务加一张全新的DV证书的套餐组合），该证书套餐被更换后，其配套购买的证书如果是在有效期内，仍然可以应用到其他网站上。该套餐再次被启用时，套餐内的证书会被标记为**已使用**。如下图所示：

16.5 证书到期后没有及时续费会怎么样？

购买了一键式HTTPS服务后，如果证书到期之前您没有及时购买新证书，阿里云证书服务系统会自动帮您申请一张免费证书并安装该证书，以确保您的网站可以继续工作。您也可以选择自行更换为收费证书。