阿里云
CA证书服务

常见问题

文档版本：20181023

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。
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。	`swich` *`{stand | slave}`*

目录

1 Symantec SSL数字证书升级重签提示

预计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的Symantec品牌数字证书。

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。

> 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。

- 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。

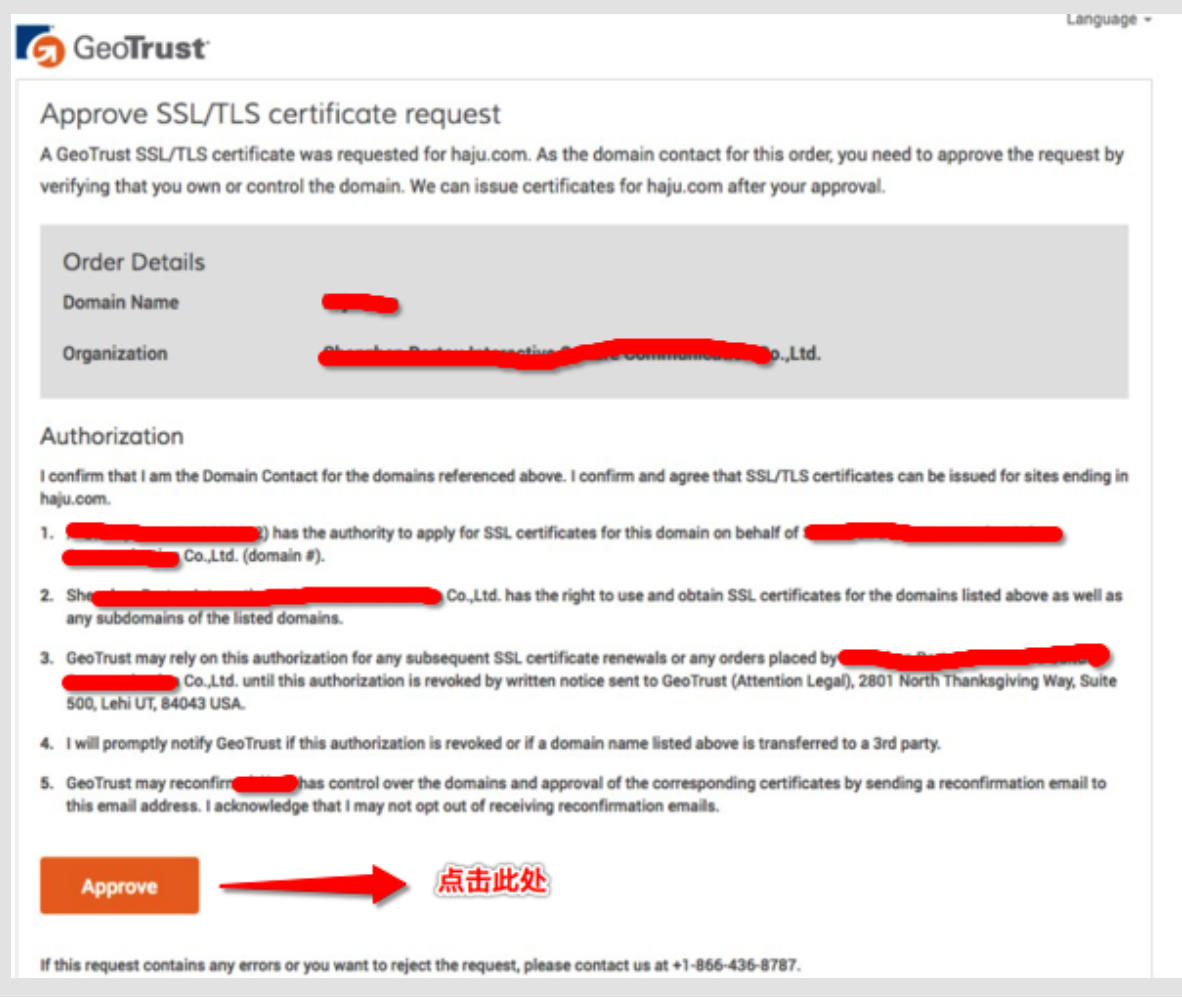
> 说明：
> 属于以下时间范围的Symantec数字证书不受本次根证书升级计划影响：
>
> - 2016年6月1日前签发且2018年3月前到期的数字证书
> - 2016年6月1日后签发且2018年9月前到期的数字证书

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：
  > 如果您在云盾证书服务管理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。

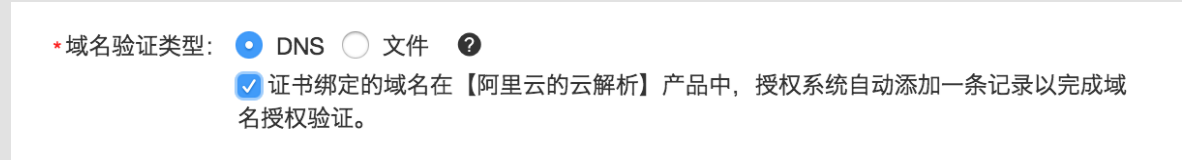


- 对于受影响范围内的DV类型的数字证书，阿里云工作人员将为您提交证书重签申请，您需要在云盾证书服务管理控制台中根据进度提示完成域名验证操作。

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




证书订单的流程如下图，每个环节都有对应的帮助信息，请一定仔细阅读：
补全信息
提交审核
查看进度
颁发证书
下载证书
看到该文字说明您的证书中有需要重签的证书
Symantec针对Chrome浏览器发布了一项根证书升级计划，为了避免与谷歌Chrome相关的任何兼容性问题，建议尽快替换您的证书。
实例中含有(替换)的订单是阿里云为您提交的替换申请，签发后需要您重新安装部署。如果是DV证书请您按照进度页面提示进行配置后才能签发
实例中含有替换字样的订单是需要替换的，请重点关注状态。
实例ID
年限
证书品牌 (所有)
到期时间
证书状态 (全部)
进度
操作
(替换)
1 Year
GeoTrust 通配符 DV
2019-04-10
已签发
--
推送 | 吊销 | 下载 | 到期新购 | 详情
1 Year
GeoTrust 通配符OV
--
待完成
补全
详情

2 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。

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 各种类型SSL数字证书的区别

用于网站HTTPS化的SSL数字证书，当前主要分为DV SSL、OV SSL、EV SSL三种类型的证书。

- DV SSL数字证书部署在服务器上后，用户浏览器访问网站时，展示如下：

- OV SSL数字证书部署在服务器上后，用户浏览器访问网站时，展示如下：

- EV SSL数字证书部署在服务器上后，用户浏览器访问网站时，展示如下：

数字证书	DV SSL	OV SSL	EV SSL
用户建议	个人	组织、企业	大型企业、金融机构
公信等级	一般	高	强
认证强度	网站真实性	组织及企业真实性	严格认证
安全性	一般	中	高
可信度	常规	中	高（地址栏绿色）

5 SSL证书有什么优势

对比传统的加密方式，SSL证书有以下几点优势：

- **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。

6 SSL数字证书如何在各类服务器上部署

1. 登录云盾证书服务管理控制台。
2. 在**我的订单**页，找到已签发的相关类型的证书，单击**下载**。
3. 在**证书下载**页中，选择您的服务器类型，下载该服务器类型的证书，下载完成后按第二步进行证书部署安装，即可实现网站的HTTPS可信访问。

7 证书推送到云产品常见问题

通过云盾证书服务管理控制台中购买数字证书，支持一键推送到CDN、负载均衡（SLB）等阿里云云产品中。

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，请不要将数字证书推送到对应的云产品中，如推送将可能导致推送失败。

说明：

此处负载均衡（SLB）服务除外，即使未开通服务也可推送成功。

当证书成功推送到云产品中，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一些对应的参数配置。另外，您也需要确认您的源站是否已经准备好启用HTTPS服务。

对应云产品的参数配置信息，请参考相应云产品的相关配置文档。

推送到CDN时没有查询到域名

当证书服务向CDN服务推送数字证书时，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。

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证书服务查询到，并实现推送。

推送到负载均衡（SLB）时都会推送到哪些地域？

证书服务会将数字证书往所有的地域都推送一份。取消推送时，证书服务会将已经推送的地域中的数字证书删除掉。

成功推送至负载均衡（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。

8 如何填写证书中绑定的域名

您购买数字证书之后，需要在证书服务管理控制台中补全证书审核资料。而补全信息的第一步就是填写域名信息，正确填写域名信息后才能保证您的数字证书顺利颁发，并正确开启HTTPS服务。

证书服务管理控制台会根据您购买的证书提示您需要输入的域名类型。

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，但 *.*.a.com 则是不正确的。

> 说明：
> 此处一个通配符域名算一个域名。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？

普通域名是相对通配符域名来说的，是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。普通域名能绑定的数量，取决于您证书订单中选择的域名个数。

> 说明：
> 如buy.example.com或next.buy.example.com各个明细子域名都算一个域名。

域名信息与CSR的关系

- 如果您选择自己创建CSR文件，那么CSR文件中的域名信息（CN属性）必须是您证书绑定域名中的一个。当域名信息中有通配符域名和普通域名混合时，请使用普通域名作为CSR文件中的CN属性值。关于CSR文件的更多说明，请参考如何制作*CSR*文件。
- 如果您选择由系统创建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，当域名信息中有通配符域名和普通域名混合时，请将普通域名放在第一个位置。

9 chrome浏览器提示错误

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED 错误

2016年11月左右，陆续接到用户反馈chrome 53版本，qq浏览器9.5.1版本（内置chrome53内核）在访问HTTPS网站时，出现上述NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED错误。该问题为Google Chrome 53版本浏览器的BUG，导致显示HTTPS网站异常，如果采用非53版本的chrome浏览器就可避免上述报错。

请参考*Symantec*的官网说明。

10 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。隐私保护的关闭方式，请参考设置域名隐私保护。

11 多通配符域名和混合域名证书申请方法

如果需要一张证书中包含一个或以上的通配符域名及一个或以上的普通域名，请按照以下操作流程进行。关于域名类型的解释，请参考如何填写证书中绑定的域名。

1. 只有专业版OV SSL证书支持该功能，其他类型证书不支持该功能。
2. 整理需要绑定的域名，通配符域名多少，普通域名多少，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，请参考"所有子域名"类型的通配符证书都支持哪些域名。

   > 说明：
   > 一定要购买同品牌证书（且同时长，比如1年），否则无法合并。

示例

以下举例以2个通配符域名和3个普通域名，以Symantec品牌专业版OV SSL为例。

1. 需要购买2个通配符证书，及多域名证书（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，不要对订单做任何操作。
3. 提交工单给我们。
   - 工单标题： 多域名证书合并
   - 工单内容： 将要合并的订单截屏。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. 审核通过后，与合并相关的订单只会保留一个，其它订单将会被关闭，且无法打开。选择可编辑的订单，去绑定域名，绑定域名处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。具体请参考如何填写证书中绑定的域名。

   建议在CSR生成步骤中选择系统创建CSR。如果自己创建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，请参考如何制作*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。

12 苹果ATS - 证书选择及配置

自2017年1月1日起，根据苹果要求，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。同时，苹果要求使用的不仅是一个简单的HTTPS协议连接，而且必须要满足iOS9中的新增特性。

说明：

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协议包含四个方面的要求。

证书颁发机构的要求

建议您使用Entrust品牌的OV型及以上数字证书。

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是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创建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。
  - 如果您选择自己创建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

传输协议必须满足TLS1.2。需要在Web服务器上开启TLSv1.2，通常要求：

- 基于OpenSSL环境的Web服务器，需要使用OpenSSL 1.0及以上版本，推荐使用OpenSSL 1.0.1及以上版本。
- 基于Java环境的Web服务器，需要使用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服务版本满足，默认均开启TLSv1.2。

详细Web服务器配置要求说明如下：

- Apache 、 Nginx Web服务器需要使用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，需要修改注册表以开启TLSv1.2。

下载并导入*ats.reg* 注册表脚本后，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，建议使用IBM Domino Server 9.0.1 FP5版本。更多信息请参考：
  - *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服务器需要使用Java7及以上版本来支持TLSv1.2。

  说明：

  Weblogic 10.3.6中存在多个SHA256兼容问题，建议最低使用Weblogic 12版本，或为Weblogic 10.3.6配置前端Apache或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，请参考 *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协议及加密套件应该如何配置：

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，请参考 *Enabling TLS 1.2 on IIS 7.5 for 256-bit cipher strength*。您也可以使用*IIS Crypto*可视化配置插件进行配置。

ATS检测工具

您可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`

13 订单提交审核后需要做什么

当数字证书订单提交审核后，您可以在云盾证书服务管理控制台中我的订单页面，单击该订单的进度查看您接下来需要做什么。

OV、EV类型证书

如果您购买的是OV或EV类型证书，您只需要耐心等待，CA中心一般会在三到七个工作日之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。

14 订单提交很久了，为什么还是审核中

如果您购买的是OV或EV证书

请您耐心等待。一般情况下，OV或EV型证书的审核申请需要三至七个工作日完成。

审核期间，请您务必保持手机畅通。CA中心在审核过程中如发现问题，将会通过电话与您联系。如无法及时联系到您，那么该订单的审核进度将可能会延迟。

15 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，Entrust可能会发送一封邮件告知您申请证书的进展或者证书已经颁发下来了。此时，阿里云证书服务控制台中的订单状态可能依然没有发生变化。您需要再等一段时间才能看到订单的状态发生变化。因为Entrust给阿里云推送的结果会比系统发邮件的结果延迟一段时间。

16 有些电脑浏览器或手机浏览器提示证书不可信怎么办

如果遇到电脑浏览器或手机浏览器提示证书不可信的问题，请确认您所购买的数字证书品牌和提示证书不可信的终端类型。

部分品牌的数字证书在某些终端上是不被支持的，请参考该品牌的数字证书的相关介绍。

目前市场上的主流设备都是兼容Symantec、GeoTrust品牌的数字证书的。

排查步骤

排除数字证书与终端不兼容的问题后，建议您按以下步骤进行检查：

1. 使用以下工具进行检查：
   - *Symantect CryptoReport SSL/TLS certificate checker*
   - *GeoCerts SSL Checker*

   如果检查结果中的证书品牌、证书类型、域名与您购买的不一致，请仔细检查服务器上数字证书的配置。

   如果检查结果显示证书链不完整，请检查数字证书相关配置是否正确。

   > **说明：**
   > 证书服务提供的PEM格式数字证书包含两段内容，两段内容中的任何一段都不能丢失。如果两段内容之间存在空白行，请删除空白行。配置修改完成后重启Web服务，并重新检查。

2. 确保您的数字证书配置中已关闭了不安全的协议，如SSLv3等有已知隐患的协议。
3. 检查您的网页中是否引用了一些HTTP资源。部分浏览器对HTTPS站点引用HTTP资源的情况会认为是不安全的。
4. 如果一个域名有多台服务器，请您确认是否每台服务器都正确部署了证书。

17 订单误关闭-信息填写错误该怎么办？

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？

- 如果有错误的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。

18 审核失败 - 主域名不能为空

问题描述

如果您在申请数字证书时选择自己上传CSR文件，可能收到“审核失败 – 主域名”不能为空的返回结果。

问题原因

在创建CSR文件时，未正确填写Common Name字段。

解决方法

重新制作并上传CSR文件，确保正确填写Common Name字段。

说明：

Common Name字段必须是证书绑定的域名中的一个。

为保证CSR文件内容正确，强烈建议您使用系统提供的系统生成CSR文件功能。同时，使用系统自动生成CSR文件功能，在数字证书颁发后还可支持不同格式的证书下载。

19 如何将证书应用到阿里云的产品中

推送至阿里云其它产品

数字证书签发后，您可以通过推送功能将数字证书一键推送到阿里云其它云产品。

目前已支持的阿里云产品包括：CDN、Web应用防火墙、高防IP、及负载均衡。

如果您在推送到阿里云其它云产品过程中遇到问题，请参考证书推送到云产品常见问题。

说明：

在将数字证书推送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，否则将无法完成推送。

下载数字证书并配置到其它产品

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

1. 登录云盾证书服务管理控制台。
2. 在我的证书订单列表中，选择您已签发的数字证书，单击下载。
3. 选择**Nginx/Tengine**，单击下载证书**for Nginx**，即可下载 PEM 格式证书文件至本地。
4. 然后，您可到其它产品的控制台中上传数字证书并进行配置。

20 申请证书审核失败的原因及处理方法

单位的电话号码不能为空或不正确

当您申请OV、EV类型数字证书时，如果您未填写单位电话号码，将收到该审核失败信息。

可能原因：OV、EV类型证书产品，单位电话号码为必填字段。当单位电话号码为空、或填写不符合规则时，需要重新填写。

解决方法：请填写能够及时联系到您的单位电话号码，以确保在CA中心进行组织信息验证时能够联系到您。

CSR（证书请求文件）已用于其他订单，请更新CSR后重新提交

证书的请求文件已用于其他订单。

可能原因：出于证书密钥安全考虑，在请求一个全新的订单时，不允许使用之前已使用过的CSR信息。

解决方法：如果之前已使用一个CSR文件成功提交过订单，在后续的新订单中，请重新生成新的CSR文件。确保每张SSL证书都有其唯一的密钥对，有助于提升证书应用中的安全性。

证书绑定的所有域名（IP）格式不正确

证书中绑定的域名信息错误。

可能原因：合法的域名仅允许包含字母 + 数字 + "-"的任意组合，且域名的最大长度不得超过64 个字符。

解决方法：请检查CSR请求文件及订单中填写的域名信息，确保您使用了正确的域名提交订单。

审核失败 - 主域名不能为空

可能原因：这种情况一般发生在您自行生成CSR文件的情况下，创建CSR文件时未正确填写Common Name字段。

说明：

Common Name必须是绑定域名中的一个。

解决方法：建议您使用系统提供的系统生成CSR文件功能，不但保证了CSR内容的正确，在证书颁发后还能支持不同格式的证书下载。

更多关于主域名不能为空的信息，请查看审核失败 - 主域名不能为空。

21 购买证书开通失败的可能原因

当购买证书去支付的时候收到“开通失败”错误。

可能原因是您没有在阿里云账号系统中进行实名认证。

22 主流数字证书都有哪些格式？

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：

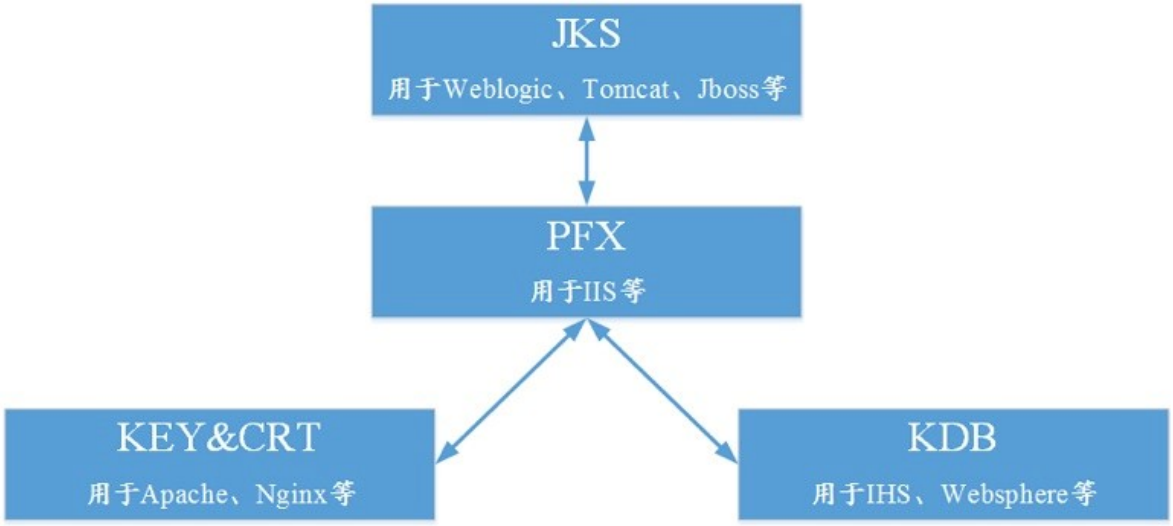
```
—–BEGIN CERTIFICATE—–
MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh......
—–END CERTIFICATE—–
```

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。

23 我获取到的数字证书如何配置在自己的Apache中

通过证书服务申请的数字证书，可以按照通常的方式配置到各种Web服务容器中。但有些数字证书是带有证书链的，在Apache服务器中配置需要按以下步骤进行操作。

1. 检查您的数字证书是否带有证书链

使用文本编辑器打开您的数字证书文件（例如*mycert.pem*）检查您的数字证书是否带有证书链。如果您的证书文件中有三段BEGIN CERTIFICATE信息，说明您的数字证书时包含证书链。

说明：

如果您的数字证书不包含证书链，则无需执行后续操作，直接在Apache服务器中配置即可。

```
-----BEGIN CERTIFICATE-----
xxxxxx...
-----END CERTIFICATE-----


-----BEGIN CERTIFICATE-----
xxxxxx...
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
xxxxxx...
-----END CERTIFICATE-----
```

2. 分离证书链

使用文本编辑器打开您的数字证书文件，复制后两段证书信息（即后两段`-----BEGIN CERTIFICATE-----`）内容到新的文本文件中，并另存为*mycert_chain.pem*，即可分离您的数字证书中的证书链。

3. 修改文件名称

将原证书文件名称修改为*mycert.pem*。这样，您就有了两个pem文件，分别是原证书文件*mycert.pem*和证书链文件*mycert_chain.pem*。

4. 配置Apache

在Apache服务器的配置文件中进行如下配置即可。

```
...
SSLEngine On
SSLCertificateFile conf/ssl.crt/mycert.pem
SSLCertificateKeyFile conf/ssl.key/mycert.key
SSLCertificateChainFile conf/ssl.crt/mycert_chain.pem
```

```
...
```

24 什么是公钥和私钥

什么是公钥和私钥？

公钥和私钥就是俗称的不对称加密方式。公钥（Public Key）与私钥（Private Key）是通过一种算法得到的一个密钥对（即一个公钥和一个私钥），公钥是密钥对中公开的部分，私钥则是非公开的部分。公钥通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。

通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用这个密钥对的时候，如果用其中一个密钥加密一段数据，则必须用另一个密钥才能解密。比如用公钥加密的数据就必须用私钥才能解密，如果用私钥进行加密也必须用公钥才能解密，否则将无法成功解密。

数字证书的原理

数字证书采用公钥体制，即利用一对互相匹配的密钥对进行加密、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），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，这样就产生了别人无法生成的文件，也就形成了数字签名。

数字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。

创建私钥

阿里云证书服务对您的私有密钥的加密算法和长度有如下要求：

- 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

OpenSSL是一个强大且应用广泛的安全基础库工具，您可以从 *http://www.openssl.org/source/* 下载最新的OpenSSL工具安装包。

说明：

要求OpenSSL版本必须是1.0.1g或以上版本。

安装OpenSSL工具后，在命令行模式下运行`openssl genrsa -out myprivate.pem 2048`即可生成您的私钥文件。

- myprivate.pem即为您的私钥文件。
- 2,048指定加密长度。

使用Keytool工具导出私钥

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 *http://www.oracle.com/technetwork/java/javase/downloads/index.html* 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，需要您从已经创建好的.keystore文件中导出私钥。关于如何从.keystore文件中导出私钥，请参考主流数字证书都有哪些格式中的转换方法。

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，请您完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。

25 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。

26 为什么要使用无密码保护的私钥

阿里云其它云产品在使用数字证书的过程中需要您提供私钥，如果您的私钥是加载密码保护的，那么其它云产品在加载您的数字证书时将无法使用您的私钥，可能导致数字证书解密失败，HTTPS服务失效。因此，需要您提供无密码保护的私钥及该私钥对应的证书文件。

在您生成私钥时，请去掉密码保护后再进行上传。关于私钥的信息，请参考什么是公钥和私钥。

如何去除私钥密码保护

如果您的密钥已经加载密码保护，可以通过*OpenSSL* 工具运行以下命令去掉密码保护：

```
openssl rsa -in encryedprivate.key -out unencryed.key
```

其中，

- `encryedprivate.key` 是带密码保护的私钥文件。
- `unencryed.key` 是去掉了密码的私钥文件，扩展名为key或者pem均可。

什么样的私钥是有密码保护的

将您的私钥文件用文本编辑器打开，如果私钥文件是如下样式，则说明该私钥是已加载密码保护的：

- PKCS#8私钥加密格式

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
......BASE64 私钥内容......
-----END ENCRYPTED PRIVATE KEY-----
```

- Openssl ASN格式

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,4D5D1AF13367D726
......BASE64 私钥内容......
-----END RSA PRIVATE KEY-----
```

说明：

用Keytool工具生成的密钥都是带有密码保护的，您可以转换成无密码的密钥文件。关于具体转换方式，请参考主流数字证书都有哪些格式。

27 如何制作CSR文件

在申请数字证书之前，您必须先生成证书私钥和证书请求文件（Certificate Signing Request，简称CSR）。CSR文件是您的公钥证书原始文件，包含了您的服务器信息和您的单位信息，需要提交给CA认证中心进行审核。

说明：

建议您使用系统提供的系统创建CSR功能，避免出现内容不正确而导致的审核失败。关于审核失败详细信息，请参考审核失败 - 主域名不能为空。

手动生成CSR文件的同时会生成私钥文件，请务必妥善保管和备份您的私钥。

您手动生成CSR文件时，一般需要输入以下信息：

说明：

输入的中文信息需要使用UTF8编码格式。

- Organization Name(O)： 申请单位名称法定名称，可以是中文或英文。
- Organization Unit(OU)： 申请单位的所在部门，可以是中文或英文。
- Country Code(C)： 申请单位所属国家，只能是两个字母的国家码。例如，中国只能是CN。
- State or Province(S)： 申请单位所在省名或州名，可以是中文或英文。
- Locality(L)： 申请单位所在城市名，可以是中文或英文。
- Common Name(CN)： 申请SSL证书的具体网站域名。

说明：

证书服务系统对CSR文件的密钥长度有严格要求，密钥长度必须是2,048位，密钥类型必须为RSA。如果申请证书是多域名或者通配子域名，在**Common Name**或**What is your first and last name?**字段只需要输入一个域名即可（通配子域名可以输入*.example.com等）。

使用OpenSSL工具生成CSR文件

1. 安装*OpenSSL*工具。
2. 执行命令`openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout myprivate.key -out mydomain.csr`生成CSR文件。其中，
   - `-new` 指定生成一个新的CSR。
   - `-nodes` 指定私钥文件不被加密。

- `-sha256` 指定摘要算法。
- `-keyout` 生成私钥文件。
- `-newkey rsa:2048` 指定私钥类型和长度。

3. 生成CSR文件*mydomain.csr*。

```
Generating a 2048 bit RSA private key
....+++
.....................................................................+++
writing new private key to 'myprivate.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
[Country Name (2 letter code) [CN]:CN
[State or Province Name (full name) []:ZheJiang
[Locality Name (eg, city) [Default City]:HangZhou
[Organization Name (eg, company) [Default Company Ltd]:HangZhou xxx Technologies,Inc.
[Organizational Unit Name (eg, section) []:IT Dept.
[Common Name (eg, your name or your server's hostname) []:www.example.com
[Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
[A challenge password []:
[An optional company name []:
```

需要输入的信息说明如下：

字段	说明	示例
Country Name	ISO国家代码（两位字符）	CN
State or Province Name	所在省份	ZheJiang
Locality Name	所在城市	HangZhou
Organization Name	公司名称	HangZhou xxx Technologies, Inc.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	www.example.com
Email Address	不需要输入	-
A challenge password	不需要输入	-

完成命令提示的输入后，会在当前目录下生成*myprivate.key*（私钥文件）和*mydomain.csr*（CSR，证书请求文件）两个文件。

说明：

在使用OpenSSL工具生成中文证书时需要注意中文编码格式必须使用UTF8编码格式。同时，需要在编译OpenSSL工具时指定支持UTF8编码格式。

如果您需要输入中文信息，建议您使用Keytool工具生成CSR文件。

使用Keytool工具生成CSR文件

1. 安装Keytool工具，Keytool工具一般包含在Java Development Kit（JDK）工具包中。
2. 使用Keytool工具生成keystore证书文件。

   说明：

   Keystore证书文件中包含密钥，导出密钥方式请参考主流数字证书都有哪些格式。

   a. 执行命令`keytool -genkey -alias mycert -keyalg RSA -keysize 2048 -keystore ./mydomain.jks`生成 `keystore`证书文件。其中，

   - `-keyalg` 指定密钥类型，必须是RSA。
   - `-keysize` 指定密钥长度为 2,048。
   - `-alias` 指定证书别名，可自定义。
   - `-keystore` 指定证书文件保存路径。

```
[Enter keystore password:
[Re-enter new password:
What is your first and last name?
[  [Unknown]:  www.example.com
What is the name of your organizational unit?
[  [Unknown]:  IT Dept.
What is the name of your organization?
[  [Unknown]:  HangZhou xxx Technologies,Inc.
What is the name of your City or Locality?
[  [Unknown]:  HangZhou
What is the name of your State or Province?
[  [Unknown]:  ZheJiang
What is the two-letter country code for this unit?
[  [Unknown]:  CN
Is CN=www.example.com, OU=IT Dept., O="HangZhou xxx Technologies,Inc.", L=HangZhou, ST=Zhe
Jiang, C=CN correct?
[  [no]:  Y

Enter key password for <mycert>
[        (RETURN if same as keystore password):
```

   b. 输入证书保护密码，然后根据下表依次输入所需信息：

问题	说明	示例
What is your first and last name?	申请证书的域名	www.example.com
What is the name of your organizational unit?	部门名称	IT Dept.

问题	说明	示例
What is the name of your organization?	公司名称	HangZhou xxx Technologies ,Ltd.
What is the name of your City or Locality?	所在城市	HangZhou
What is the name of your State or Province?	所在省份	ZheJiang
What is the two-letter country code for this unit?	ISO 国家代码（两位字符）	CN

输入完成后，确认输入内容是否正确，输入Y表示正确。

c. 根据提示输入密钥密码。可以与证书密码一致，如果一致直接按回车键即可。

3. 通过证书文件生成证书请求。

a. 执行命令`keytool -certreq -sigalg SHA256withRSA -alias mycert -keystore ./mydomain.jks -file ./mydomain.csr`生成CSR文件。其中，

- `sigalg`指定摘要算法，使用SHA256withRSA。
- `alias`指定别名，必须与keystore文件中的证书别名一致。
- `keystore`指定证书文件。
- `file`指定证书请求文件（CSR）。

b. 根据提示输入证书密码即可以生成*`mydomain.csr`*。

28 "所有子域名"类型的通配符证书都支持哪些域名

如果您打算购买“所有子域名”类型的通配符证书，需要注意通配符证书匹配域名的规则：

*.example.com的域名证书匹配abc.example.com、sport.example.com、good.example.com等域名，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等域名。

也就是说，通配符域名证书只匹配同级别的通配域名，不能跨级匹配。

目前我们的“所有子域名”数字证书只支持一个含通配符的域名。

29 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。

30 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，服务器更换IP地址没有任何关系，只要域名不变，重新解析到新的IP地址即可，原来的SSL证书照样可以用，不需要更换新的证书。

31 申请SSL证书时应该使用哪个域名申请

关于申请SSL数字证书时应该如何选择申请域名，本文将通过一个简单的示例进行描述。

例如，您的网站为www.domain.com 。

其中，有一个用户登录页面http://www.domain.com/login.asp ，您想要申请一张SSL数字证书确保用户输入用户名、密码时的安全，确保用户信息不会在传输过程中被非法窃取。同时，还有一个用户登录的信息管理页面http://www.domain.com/oa/manage.asp ，您也希望使用SSL数字证书来保障内部管理系统中的机密信息的安全。

这种情况下，您使用域名www.domain.com申请SSL数字证书即可实现对这类页面的保护。

如果您的网站访问量较大，建议您为需要使用SSL数字证书的页面设置一个独立的Web服务器（HTTP server），并使用一个独立的域名来申请SSL数字证书，例如secure.domain.com或ssl.domain.com。

说明：

https:// 的使用必须与申请SSL数字证书的域名一致，否则浏览器可能会出现“安全证书上的名称无效或者与站点名称不匹配”的警告。请根据您网站的具体情况使用合适的域名来申请SSL数字证书。

更多信息，请参考如何选择#证书类型-证书品牌-保护域名数量。

32 SSL证书过期了怎么办

SSL数字证书过期之后，将无法继续使用，您需要在您的证书到期前办理续费。续费完成后，证书服务系统将复制当前证书订单的信息到续费订单中，同时自动将续费证书订单提交审核。

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。

33 服务器上装SSL证书会不会影响用户浏览网页的速度

服务器上装SSL证书会增加服务器CPU的处理负担，因为要为每一个SSL连接实现加密和解密，但一般不会影响太大。同时建议您注意以下几点以减轻服务器的负担：

- 仅为需要加密的页面使用SSL，如https://www.domain.com/login.asp，不要把所有页面 都使用https:// ， 特别是访问量最大的首页。
- 尽量不要在使用了SSL的页面上设计大块的图片文件和其他大文件，尽量使用简洁的 文字页面。

34 浏览器是如何检查SSL证书是否工作正常的

SSL数字证书必须由浏览器中“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。

配置完成SSL数字证书后，如果您能使用https:// 方式访问您的网站，则表示网站已经部署了SSL证书。

操作步骤

1. 在浏览器地址栏中，输入https:// + 您的数字证书绑定的域名（如 https://www.aliyun.com ）。
2. 按回车键（Enter）通过HTTPS方式访问您的网站。
3. 网站页面能正常访问，且浏览器地址栏中显示安全锁标志，说明您的SSL数字证书已部署成功。

35 如何在同一服务器上实现多站点多域名HTTPS

假设有这样一个场景，我们有多个站点（例如site1.marei.com，site2.marei.com和site3.marei.com）绑定到同一个IP：PORT，并区分不同的主机头。我们为每一个SSL站点申请并安装了证书。在浏览网站时，用户仍看到证书不匹配的错误。

IIS中实现

问题原因

当一个https的请求到达IIS服务器时，https请求为加密状态，需要拿到相应的服务器证书解密请求。由于每个站点对应的证书不同，服务器需要通过请求中不同的主机头来判断需要用哪个证书解密，然而主机头作为请求的一部分也被加密。最终IIS只好使用第一个绑定到该IP：PORT的站点证书解密请求，从而有可能造成对于其他站点的请求失败而报错。

解决方案

- 第一种解决方案将每个https站点绑定到不同的端口。但是这样的话客户端浏览网页时必须手动指定端口，例如https：//site.domain.com:444
- 第二种解决方案是为每个站点分配一个独立的ip，这样冲突就解决了，甚至主机头也不用添加了。
- 第三种解决方案是使用通配证书。我们采用通配证书颁发给.domain.com，对于我们的示例中，应该采用颁发给.marei.com的证书，这样任何访问该domain的请求均可以通过该证书解密，证书匹配错误也就不复存在了。
- 第四种解决方案是升级为IIS8，IIS8中添加的对于SNI（Server Name Indication）的支持，服务器可以通请求中提取出相应的主机头从而找到相应的证书。

  SNI开启方式请参考*http://www.iis.net/learn/get-started/whats-new-in-iis-8/iis-80-server-name-indication-sni-ssl-scalability*

Nginx中实现

打开Nginx安装目录下*conf*目录中打开*nginx.conf*文件，找到

```
server {
    listen 443;
    server_name domain1;
    ssl on;
    ssl_certificate 磁盘目录/订单号1.pem;
    ssl_certificate_key 磁盘目录/订单号1.key;
    ssl_session_timeout 5m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

```
    ssl_ciphers AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!aNULL
:!eNULL;
    ssl_prefer_server_ciphers   on;
    location / {
        root   html;
        index  index.html index.htm;
    }
}
```

在上述基础上，再添加另一段配置

```
server {
    listen 443;
    server_name dommain2;
    ssl on;
    ssl_certificate 磁盘目录/订单号2.pem;
    ssl_certificate_key 磁盘目录/订单号2.key;
    ssl_session_timeout 5m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!aNULL
:!eNULL;
    ssl_prefer_server_ciphers on;
    location / {
        root html;
        index index.html index.htm;
    }
}
```

通过上述配置在Nginx中支持多个证书。

Apache配置HTTPS虚拟主机共享443端口

```
Listen 443
NameVirtualHost *:443
<VirtualHost *:443>
  ……
ServerName www.example1.com
SSLCertificateFile     common.crt;
SSLCertificateKeyFile  common.key;
SSLCertificateChainFile  ca.crt
  ……
</VirtualHost>
<VirtualHost *:443>
  ……
ServerName www.example2.com
SSLCertificateFile     common2.crt;
SSLCertificateKeyFile  common2.key;
SSLCertificateChainFile  ca2.crt

  ……
</VirtualHost>
```