

阿里云

SSL证书服务 动态与公告

文档版本：20220711

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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.【重要】DigiCert更新DV SSL中间证书的说明	06
2.【通知】网站代理HTTPS停止新购、续费和升级	07
3.【变更】关于GeoTrust DV证书名称变更的通知	08
4.【通知】申请通配符证书不再支持文件验证	09
5.【通知】GlobalSign中间CA迁移导致续费签发证书不受信任问题	10
6.【变更】关于调整GeoTrust多域名规格SSL证书售价的通知	12
7.【公告】关于近期收到非阿里云官方通知“国际品牌证书无法使用”等信...	13
8.【通知】SSL证书服务下线切换到海外地域功能	14
9.【通知】国际站DigiCert品牌证书临时下架	15
10.【变更】关于调整DigiCert部分规格SSL证书售价的通知	16
11.【变更】关于阿里云SSL证书服务的名称变更的通知	17
12.【变更】关于域名所有权验证策略调整的通知	18
13.【新功能】云盾证书增值服务（包年）	19
14.【变更】关于证书部署到阿里云产品计费方式变更的通知	23
15.关于近期接收到的“TLS/SSL版本较低，需要更换证书”的陌生电话的...	25
16.【重要】GlobalSign更新DV SSL中间根证书说明	26
17.历史公告	27
17.1.【售卖变更通知】针对SSL证书有效期调整，阿里云售卖页面调整细...	27
17.2.【变更通知】SSL证书2年有效期变更及影响通知	27
17.3.新冠疫情期间购买SSL证书赠送申请和安装服务	28
17.4.【2020年5月3日】DigiCert系统定期维护通知	29
17.5.【2020年4月23日】Symantec品牌证书标识变更通知	30
17.6.【2020年3月16日】DigiCert系统维护更新公告	30
17.7.【2020年3月8日】DigiCert系统维护更新公告	31
17.8.【2019年12月23日】Symantec接口升级通知	31
17.9.【2019年11月9日】Digicert系统升级更新公告	31

17.10. 【2019年9月22日】Digicert系统维护更新公告	31
17.11. 【2019年4月6日】Digicert数据迁移用户公告	31
17.12. Symantec SSL数字证书升级的影响与处理方案	32
17.13. 【2018年11月17日】Symantec接口维护通知	34
17.14. 【2017年12月1日】Symantec与DigitalCert合并相关证书签发时..	34
17.15. 关于免费证书吊销延迟的说明公告	34
17.16. 免费证书购买方式变更通知	34
17.17. 【通知】国际站SSL证书服务将支持购买DigiCert品牌证书	35

1.【重要】DigiCert更新DV SSL中间证书的说明

尊敬的阿里云数字证书管理服务用户：

接DigiCert厂商通知，其DV证书应用的以下中间证书将于2023年05月31日到期。因此，使用以下中间证书签发的DV证书有效期最长为2023年05月31日。

- RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1
- GeoTrust TLS DV RSA Mixed SHA256 2020 CA-1

DigiCert厂商在2022年05月24日启用了以下新的中间证书，新的中间证书到期日为2030年。

- RapidSSL Global TLS RSA4096 SHA256 2022 CA1
- GeoTrust Global TLS RSA4096 SHA256 2022 CA1

影响及解决方案

- 如果您通过续费签发的DigiCert、GeoTrust DV证书有效期应该为2023年05月31日之后，由于中间证书在2023年05月31日过期，导致您的已签发证书有效期为2023年05月31日，缺失2023年05月31日后的有效期。您需要在[数字证书管理服务控制台SSL证书页面](#)，查看您的证书有效期是否已被自动补齐（即更新为2023年05月31日之后的有效期）。
 - 是：如果该证书已部署在您的Web服务器或阿里云产品中，您必须重新安装有效期更新后的证书。安装证书的具体操作，请参见[SSL证书安装指南](#)。
 - 否：您需要重新签发证书才能更新该证书的有效期。数字证书管理服务会协助您重新签发证书，您需要在SSL证书页面的[证书管理](#)或[免费证书](#)页签下，将鼠标移动至需要重新签发的证书有效期限列的图标上，查看证书有效期缺失的说明，并使用钉钉扫码加入钉钉群。技术支持工程师会在钉钉群中联系您，并协助您尽快重新签发证书。
- 如果您的服务端和客户端绑定了旧的中间证书，您需要尽快解除和旧中间证书之间的绑定，并重新绑定新的中间证书。

通常情况下，您在数字证书管理服务控制台下载的SSL证书已经包含了中间证书，所以您可以重新安装有效期更新后的SSL证书。

根证书和中间证书都有其生命周期，给您带来不便，敬请谅解。

感谢您对阿里云的支持与关注！

2.【通知】网站代理HTTPS停止新购、续费和升级

尊敬的阿里云用户：

由于阿里云内部服务迁移，自2022年05月12日起，数字证书管理服务已停止新购网站代理HTTPS实例。

即日起至2022年09月30日，已购买的网站代理HTTPS实例不受影响，可以正常使用，仍支持续费、升级等操作。

 **注意** 由于无法新购网站代理HTTPS实例，建议您关注已购实例的到期时间并及时续费，避免因续费不及时导致实例被释放影响您的业务。

数字证书管理服务将于2022年09月30日，停止支持网站代理HTTPS实例的续费和升级。

给您带来不便，敬请谅解。

感谢您对阿里云的支持与关注！

3.【变更】关于GeoTrust DV证书名称变更的通知

尊敬的阿里云用户：

由于接到DigiCert关于售卖SSL证书时要清晰标识子品牌名称的通知，数字证书管理服务计划于2022年01月下旬将GeoTrust品牌DV证书更名为RapidSSL品牌DV证书。关于后续上线GeoTrust品牌DV证书的计划，请等待后续通知。

特此通知，感谢您对阿里云的支持与关注！

相关信息

以下是来自DigiCert证书的相关公告。



4.【通知】申请通配符证书不再支持文件验证

尊敬的阿里云用户：

受最新提案的影响，SSL证书合作厂商调整了签发证书的策略，故阿里云SSL证书服务将不再支持申请通配符证书时使用文件验证的方式。[CA/B](#)

生效时间：2021年11月15日起（SSL证书合作厂商将陆续生效新的通配符证书验证策略）。

变更内容：

通配符域名（例如 `*.aliyundoc.com` 、 `*.abc.aliyundoc.com` 等）不再支持通过文件验证的方式验证域名所有权。

届时，您通过SSL证书服务申请通配符证书时，只能使用DNS验证的方式验证域名所有权。关于DNS验证的更多介绍，请参见[域名所有权验证](#)。

 **注意** 单域名（包含顶级域，例如 `aliyundoc.com` ，和子域名，例如 `www.aliyundoc.com` ）仍支持通过文件验证的方式验证域名所有权，但是使用文件验证方式验证子域名所有权存在失败的可能，建议您使用DNS验证方式。

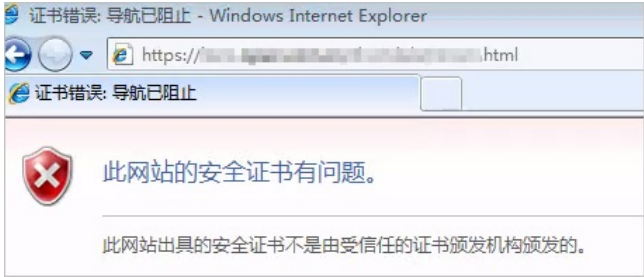
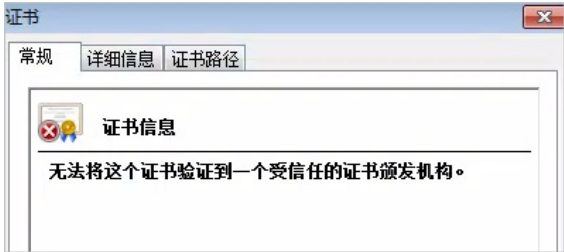
给您带来不便，敬请谅解。

感谢您对阿里云的支持与关注！

5.【通知】GlobalSign中间CA迁移导致续费签发证书不受信任问题

尊敬的阿里云用户：

因GlobalSign厂商于2019年05月27日更新了用于签发SSL证书的中间CA，导致您在2019年05月27日后，通过SSL证书服务续费签发的GlobalSign品牌DV和OV型证书可能出现不受信任的问题。具体说明如下：

项目	说明
受影响证书	自2019年05月27日起，通过SSL证书服务续费签发的GlobalSign品牌DV和OV型证书。如果您在2019年05月27日后，通过SSL证书服务首次购买GlobalSign品牌证书，则证书不受影响。
问题现象	您在服务器上安装续费签发的新证书（替换2019年05月27日前安装的旧证书）后，部分用户在访问您的业务时，收到此网站的安全证书有问题的提示（图1），且证书信息中提示无法将这个证书验证到一个受信任的证书颁发机构（图2）。 证书错误  证书信息报错 
问题原因	受影响证书和2019年05月27日前安装的旧证书关联了不同的根CA（受影响证书关联到GlobalSign R3根、旧证书关联到GlobalSign R1根）。
解决方案	您需要在安装了受影响证书的服务器上配置GlobalSign R1-R3交叉根（用于解决R1根和R3根的兼容性问题）。配置步骤如下： 1. 访问下载根证书和中间证书，下载GlobalSign R1-R3交叉根。 2. 在服务器上配置GlobalSign R1-R3交叉根。 根据您的服务器类型不同，具体配置方法有差异。如果您需要帮助，请提交工单或在数字证书管理服务控制台左侧导航栏，单击有问题？找专家！，然后扫描二维码，进入钉钉服务群联系售后技术支持人员。

感谢您对阿里云的支持与关注！

相关文档

- [GlobalSign中间证书和根证书迁移公告：GlobalSign SSL Products Intermediate and Root Migration](#)

6.【变更】关于调整GeoTrust多域名规格SSL证书售价的通知

尊敬的阿里云用户：

由于接到GeoTrust关于SSL证书的涨价通知，阿里云SSL证书服务计划于2021年10月14日起对GeoTrust品牌多域名规格（包括OV和EV证书类型）SSL证书的售价进行相应调整。关于调整后的具体价格，请以[云盾证书服务购买页](#)为准。

感谢您对阿里云的支持与关注！

7.【公告】关于近期收到非阿里云官方通知“国际品牌证书无法使用”等信息的说明

尊敬的阿里云用户：

如果近期某些自称阿里云合作伙伴的企业通过电话、微信或者钉钉等方式联系您，称“根据中国近期已经发布或者即将发布的法律法规，（包括但不限于《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》），您购买的国际品牌证书将于2021年09月01日起在中国地域无法正常使用”或者其他信息，请不要相信该信息。

为了避免给您造成困扰，阿里云特此发表声明：

- 您收到的以上信息为虚假信息，是某些企业对相关法律法规的过度解读。
- 阿里云从未收到中国监管部门关于国际品牌SSL证书在中国地域使用问题的通知。
如果有中国官方关于国际品牌SSL证书在中国使用限制的规定，阿里云会及时通过官方渠道（[SSL证书服务官方文档](#)）发布公告，不会委托个人或合作伙伴通过其他方式通知您。
- 如果您在阿里云购买的SSL证书（不包含免费版和上传的第三方证书）即将到期，阿里云会在证书到期前7天、前15天、前30天以邮件、[SSL证书控制台](#)站内信、短信的方式通知您及时续费，不会通过其他方式联系您。
- 阿里云合作的CA厂商只有在证书审核阶段的鉴证环节和证书使用过程出现特殊情况（例如私钥泄漏、申请强制吊销等）时才会主动联系您，否则不会以阿里云合作厂商的身份主动联系您。
阿里云合作的CA厂商联系您使用的电话号码（请勿主动联系）和邮箱信息如下表所示，其他号码及邮箱均为虚假信息，请谨慎接听或回复。

合作CA厂商	电话号码	邮箱
北京天威诚信电子商务服务有限公司  说明 该厂商提供以下证书品牌： ◦ DigiCert ◦ GeoTrust ◦ vTrus	010-68778970	aliyun_service@itrus.cn
CFCA	010-80864444	sunjie@cfca.com.cn
GlobalSign	+63开头，无固定电话号码	vetting-cn@globalsign.com
WoSign	0755-26027839	Audit7@wotrus.com

如果您无法判断收到信息的真实性，请您记录对方联系方式和信息详细内容，及时通过[工单](#)反馈给阿里云。

对任何冒充阿里云欺骗客户的企业或个人，阿里云保留追究法律责任的权利。

感谢您对阿里云的支持与关注！谢谢！

8.【通知】SSL证书服务下线切换到海外地域功能

尊敬的阿里云用户：

由于中国站售卖的SSL证书在海外地域使用时存在版本不兼容问题，可能给您带来数据安全风险，为此SSL证书服务已下线切换到海外地域功能。



本次调整不会影响您正常使用SSL证书服务。更多信息，请等待后续通知。

给您带来不便，敬请谅解。

9.【通知】国际站DigiCert品牌证书临时下架

尊敬的阿里云用户：

由于阿里云与DigiCert品牌证书联合调整，为了不影响您的使用体验，阿里云将于2021年08月03日00时起，在国际站SSL证书服务中临时下架DigiCert品牌证书的下单入口。届时，您将无法在国际站证书购买页面选购该品牌证书。在此期间，您仍可选购GlobalSign、EnTrust品牌证书。

后续DigiCert品牌证书重新在国际站上线后，您可再次选购。关于重新上线时间，请等待后续通知。

注意

- 已经购买但仍未提交申请的国际站DigiCert品牌证书，请您提交[工单](#)申请退款。
- 已经提交申请且在审核中、已经签发的国际站DigiCert品牌证书不受影响。

给您带来不便，敬请谅解。

10.【变更】关于调整DigiCert部分规格SSL证书售价的通知

尊敬的阿里云用户：

由于接到DigiCert关于SSL证书的涨价通知，阿里云SSL证书服务计划对DigiCert品牌部分规格SSL证书的售价进行相应调整。关于受影响的SSL证书规格和具体调整计划，请等待后续通知。

感谢您对阿里云的支持与关注！

相关信息

以下是来自DigiCert的证书价格调整通知。

价格调整声明

Digicert 承诺提供全球领先的 TLS/SSL 证书安全技术，定期审查我们的服务、产品和行业状况，为反映鉴证规则变更带来的成本上涨及产品功能的提升，我们决定自2021年4月5日起，对部分产品的终端零售价格进行了调整，并保持良好的性价比。本次涉及到的调价产品包含 GeoTrust TrueBusiness ID OV 系列产品，感谢理解，希望得到客户一如既往的信任与支持。



11.【变更】关于阿里云SSL证书服务的名称变更的通知

尊敬的阿里云用户：

阿里云SSL证书服务致力于持续为广大用户带来更好的体验。

自2021年06月01日起，SSL证书服务将更名为**数字证书管理服务**（原名为“SSL证书服务”）。

特此通知，感谢您对阿里云的支持与关注！

12.【变更】关于域名所有权验证策略调整的通知

尊敬的阿里云用户：

受最新提案的影响，阿里云SSL证书服务将对域名所有权的验证策略（文件验证方式）进行调整。[CA/B](#)

生效时间：2021年09月21日起。

变更内容：

- 通配符域名（例如，*.example.com、*.1.example.com等）不再支持通过文件验证的方式进行域名所有权验证。
届时，您通过SSL证书服务申请通配符证书时，只能使用DNS验证的方式验证域名所有权。关于DNS验证的更多介绍，请参见[域名所有权验证](#)。
- 单域名（包含顶级域和子域名，例如，example.com、www.example.com等）仍支持通过文件验证的方式进行域名所有权验证，但是使用文件验证时，所有单域名都必须单独完成验证。
届时，如果您使用文件验证方式验证域名所有权，必须分别对顶级域（例如，example.com）和相关子域名（例如，www.example.com）进行验证。关于文件验证的更多介绍，请参见[域名所有权验证](#)。

相关信息：[Domain validation policy changes in 2021](#)

给您带来不便，敬请谅解。如果您有任何疑问，请提交[工单](#)或者通过钉钉售后服务群联系我们。

13.【新功能】云盾证书增值服务（包年）

阿里云SSL证书服务后续将推出云盾证书增值服务（包年）。您可以通过预付费购买云盾证书增值服务（包年），享有超值的服务权益。本文介绍了云盾证书增值服务（包年）提供的具体权益。

② 说明 关于云盾证书增值服务（包年）的具体发布时间，请等待后续通知。

云盾证书增值服务（包年）分为4999元/年的基础版、14999元/年的高级版。下表描述了不同增值服务（包年）版本包含的具体权益及与付费版证书用户、免费版证书用户享有的权益对比。其中，√表示支持、×表示不支持。

类型	权益说明	高级版增值 服务 14999 元/年	基础版增值 服务 4999元/ 年	付费版 SSL证书 用户	免费版 SSL证书 用户
技术支持	智能客服 ，由智能机器人帮助您解答产品使用问题。	√	√	√	√
	人工客服，由阿里云售后工程师通过 工单 系统为您解答产品使用问题（包含证书安装指导、证书域名解析设置等）。	√	√	√	×
	专属客服，由阿里云售后工程师通过 VIP钉钉服务群 ，为您解答产品使用问题（包含证书安装指导、证书域名解析设置等）及处理紧急需求（例如，人工追加域名、快速吊销、加速审核等）。	√	√	×	×
	在默认消息提醒的基础上，提供可定制的消息提醒。 默认消息提醒仅支持通过邮件、站内信、短信方式，向与阿里云账号绑定的联系人发送标准消息提醒（包含证书过期、产品新功能发布等） 可定制的消息提醒包含： - 自定义消息接收人（例如，由您指定某个证书相关消息的联系人，该联系人可能不是证书申请者）。 - 自定义消息接收方式。在默认通知方式（邮件、站内信、短信）基础上，增加钉钉消息通知。 - 更多的消息类型。在标准消息提醒的基础上，支持更多样的消息提醒类型（例如，私钥泄露报警、域名监控异常）。	√	√	× 仅支持默认消息提醒。	× 仅支持默认消息提醒。

类型	权益说明	高级版增值服务 14999元/年	基础版增值服务 4999元/年	付费版SSL证书用户	免费版SSL证书用户
证书服务	购买SSL证书订单实例后，支持申请退款的时间。  注意 只有在订单实例完整（例如，实例购买后未使用，或者已用于提交证书申请，但是由于审核失败、吊销等原因，获得了证书次数返还）的前提下，才可以申请退款。	购买后30天内，订单实例完整的前提下支持申请退款。	购买后30天内，订单实例完整的前提下支持申请退款。	购买后7天内，订单实例完整的前提下支持申请退款。	不涉及。
	单张证书绑定多个通配符域名时，赠送与通配符域名个数相同的顶级域。 例如，假设您为域名*.aliyun.com和*.alibabacloud.com合并申请一张证书，则默认签发的证书绑定了*.aliyun.com、*.alibabacloud.com和aliyun.com（或者alibabacloud.com，仅能二选一）；使用该权益后，假设您为域名*.aliyun.com和*.alibabacloud.com合并申请一张证书，则签发的证书将同时绑定*.aliyun.com、*.alibabacloud.com、aliyun.com和alibabacloud.com。  说明 您需要提交工单或者通过VIP钉钉服务群申请，才可以获得赠送的顶级域。	√	√	√ 仅赠送1个顶级域。	×
	默认20张/年免费证书的基础上，额外赠送免费证书的申请额度。	√ 额外赠送80张/年。	√ 额外赠送20张/年。	×	×
	不限次数，免费部署证书（包含阿里云证书、上传的第三方证书）到阿里云产品。	√	√	√	√ 阿里云免费证书支持免费部署，上传的第三方证书需要付费部署，价格：30元/次。

类型	权益说明	高级版增值 服务 14999 元/年	基础版增值 服务 4999元/ 年	付费版 SSL证书 用户	免费版 SSL证书 用户
	开启托管服务的前提下，不限次数，免费自动部署证书（包含阿里云证书、上传的第三方证书）到阿里云产品。 自动部署的前提是原证书已经手动部署到阿里云产品，且开启了托管服务。SSL证书服务会在原证书到期前自动续费更新原证书，并将续费证书自动部署到对应的云产品。	√	√	× 每开通一次托管服务，赠送5次自动部署。支持支付费用获得更多自动部署的次数，价格：30元/次。	× 每开通一次托管服务，赠送5次自动部署。支持支付费用获得更多自动部署的次数，价格：30元/次。
	阿里云证书在关联了同一个企业用户的多个阿里云账号之间共享使用。	√	√	×	×
	证书有效期内，如果因为未妥善保管导致证书私钥泄漏，支持免费重新签发证书。 每张证书可以申请重新签发1次。	√	√	×	×
	证书有效期内，如果域名发生变化，支持免费重新签发同一品牌（目前仅支持DigiCert、GeoTrust）的证书。 每张证书可以申请重新签发1次。	√	√	×	×
	免费提供域名维度（仅支持单域名，例如，www.aliyun.com）的HTTPS运行状态监控报告。	√ 支持10个单域名。	√ 支持5个单域名。	√ 支持3个单域名。	√ 阿里云免费证书支持1个单域名，上传的第三方证书不支持。
额外权益	首次开通服务，赠送价值200元SSL证书优惠券5张（开通服务后一次性发放，有效期1年）。 ② 说明 每个SSL证书订单最多只可以使用1张优惠券。具体使用规则，以券面说明为准。	√	√	×	×
	首次开通服务，赠送1个价值1100元的网站HTTPS实例（单域名规格、1年服务时长）。	√	√	×	×

（随产品当前营销策略变化，具体以购买时的说明为准）	权益说明	高级版增值服务 14999元/年	基础版增值服务 4999元/年	付费版SSL证书用户	免费版SSL证书用户
	首次开通服务，赠送价值4000元的1个月的PCA服务（包含1个私有根CA、1个私有子CA、10张私有证书，证书算法为RSA）。	√	×	×	×

14.【变更】关于证书部署到阿里云产品计费方式变更的通知

发布说明

该变更目前已经灰度发布，预计于2021年06月25日对全部用户开放。如果您在部署（上传到SSL证书服务进行统一管理的）第三方证书时，收到需要付费购买资源的提示（如下图所示），表示您已在灰度范围内。



尊敬的阿里云用户：

为了向您提供更优质的服务，SSL证书服务计划调整证书部署功能（即通过[数字证书管理服务控制台](#)，将已签发的阿里云证书、已上传的第三方证书部署到阿里云产品）和到期自动部署的计费规则：

- 阿里云证书（包含付费证书和免费证书）仍支持免费部署。
- 第三方证书部署到阿里云产品将会变更为收费服务。
- 已开启托管服务的证书将支持免费开启到期自动部署。

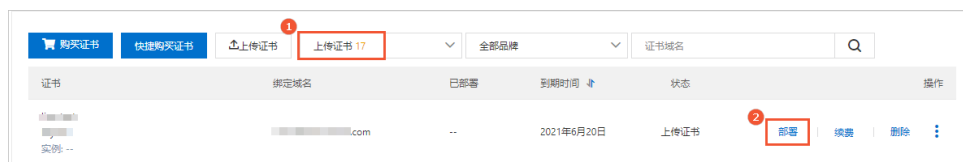
生效时间：2021年05月25日。

变更内容

调整后的具体计费规则如下表所示：

证书类型	部署到阿里云产品	开启到期自动部署
阿里云证书 (通过SSL证书服务购买并签发的证书，包含免费证书和付费证书)	免费	
第三方证书 (通过第三方证书服务平台购买并签发的证书；出于业务需要，上传到SSL证书服务进行统一管理)	收费，30元/次 通过部署操作，每将一张证书部署到一个关联的阿里云产品上的一个域名，计作一次。 计费示例： ● 将1张已上传的第三方证书部署到已接入Web应用防火墙的3个域名上，表示3次部署，部署费用为90（30*3）元。 ● 将1张已上传的第三方证书分别部署到已接入DDoS高防的1个域名和已接入Web应用防火墙的同1个域名，表示2次部署，部署费用为60（30*2）元。	每开启一次托管服务，将获得5次免费开启到期自动部署的机会。超出免费使用额度后，使用到期自动部署会收费，30元/次。

上述计费规则调整生效后，您在[数字证书管理服务控制台](#)的概览页面，为已上传的第三方证书进行部署操作时（如下图所示），将会生成对应的部署服务订单。您必须完成订单购买，才可以完成部署操作。



如果您已经为证书开启了托管，则可以在[托管服务](#)页面，为已经托管的证书免费开启到期自动部署（不再有部署资源次数的限制）。更多信息，请参见[开启到期自动部署](#)。



15.关于近期接收到的“TLS/SSL版本较低，需要更换证书”的陌生电话的说明

尊敬的阿里云SSL证书用户：

如果您近期收到了陌生人电话联络，告知您的证书因TLS/SSL版本较低（例如，使用了TLS 1.0、SSL 1.0、SSL 2.0）或者证书不兼容某个TLS/SSL协议版本（例如，TLS 1.3）等原因导致安全性低，要求您重新购买证书，请不要相信该信息。

您通过阿里云SSL证书服务购买并签发的SSL证书默认兼容所有TLS/SSL协议版本（目前包含TLS 1.0、1.1、1.2和1.3），且您在安装证书到Web服务时，可以设置要应用的TLS/SSL协议版本。

例如，由于TLS 1.0安全性较低，您可以在Web服务的证书配置中，将TLS 1.0协议从SSL Protocol配置去掉（表示服务器拒绝客户端使用TLS 1.0协议与服务器通信）；您也可以修改Web服务的证书配置，新增TLS 1.3协议。具体配置方法与您使用的Web服务类型有关，更多信息，请参见[SSL证书安装指南](#)。

16.【重要】GlobalSign更新DV SSL中间根证书说明

GlobalSign于2021年1月21日，更新了DV SSL中间根证书，具体公告如下：

亲爱的阿里云用户，您好：

为了符合Certificate Authority Browser Forum（证书管理局）对于SSL证书的安全规范和要求，GlobalSign已对DV SSL的中间根证书进行了升级。旧的中间证书（型号：GlobalSign RSA DV SSL CA 2018）已经被更换为新的中间证书（型号：GlobalSign GCC R3 DV TLS CA 2020）。本次升级提高了DV SSL证书的安全性能。

由于开发新的中间证书的过程包含多方的审核、测试，导致我们在通知上出现了延迟。我们对此表示歉意。

我们将配合阿里云，帮助每一位用户重新签发证书。您只需要按照原来的安装方式，把重新签发的证书安装到您的服务器，无需更换公钥和私钥。

非常感谢大家一直以来对GlobalSign的支持。对于此通告，我们再次表示歉意。

谢谢

GlobalSign APAC

阿里云解决方案

由于GlobalSign DV SSL中间根证书的更新，导致2021年1月21日0时0分0秒前通过阿里云SSL证书服务签发的GlobalSign DV SSL证书已被吊销。GlobalSign将于2021年1月22日前，对所有涉及重新签发的DV SSL证书进行批量签发，阿里云会使用新签发的证书覆盖原有证书。

如果您使用了GlobalSign的DV SSL证书，需要前往[数字证书管理服务控制台](#)重新下载新签发的证书，并将新签发的证书重新安装到服务器，替换原有的证书，才能恢复网站的HTTPS访问。

在安装过程中遇到问题时，请联系我们获取一对一加急技术指导。

阿里云补偿方案

所有涉及到重新安装GlobalSign DV SSL证书的用户，在下次使用GlobalSign证书时，将享受1次原价基础上的5折优惠。

17.历史公告

17.1.【售卖变更通知】针对SSL证书有效期调整，阿里云售卖页面调整细则

尊敬的阿里云用户，您好：

从2020年9月1日起，苹果系统、谷歌和火狐浏览器计划调整受信SSL证书的有效期策略，上述系统或浏览器中受信SSL证书的最长有效期将从825天缩短至398天。对此，各CA厂商也将缩短SSL证书的最长有效期。具体影响详见【变更通知】[SSL证书2年有效期变更及影响通知](#)。

因为2年期SSL证书停止颁发，阿里云于2020年8月20日起对售卖页面进行以下调整：

- 取消多域名证书购买选项。
如需购买多域名证书，请您选择单个域名类型下OV企业级SSL或EV增强级SSL并选择对应域名个数即可。
- 取消Digicert DV通配符SSL证书规格。
- 新增国产vTrus和WoSign品牌。
vTrus品牌是天威诚信（工信部许可设立的权威CA机构）的自有国产SSL证书品牌，目前可在平台选购该品牌的DV（域名型）SSL证书。该品牌支持绑定通配符域名和单域名，支持RSA算法。
沃通WoSign是工信部许可的权威CA机构，目前可在平台选购该品牌DV（域名型）SSL证书。该品牌支持绑定通配符域名和单域名、支持国密和RSA算法。截止到2020年9月30日，购买该品牌的DV（域名型）国密SSL证书，买1送1，即购买国密证书赠送同规格的RSA证书，帮助您实现双证书部署。
- 停止售卖2年有效期的SSL证书，仅售1年有效期的SSL证书。
如您想降低运维成本或担心忘记更新证书导致业务中断，可选购开通[托管服务概述](#)。目前，证书托管服务的有效期为2年。

② 说明 如果您已在2020年8月20日前已购买了2年有效期的证书，您需要在2020年8月27日前完成证书的签发。详细内容请参见【变更通知】[SSL证书2年有效期变更及影响通知](#)。

感谢您一直以来对阿里云SSL证书的关注和支持，如您有任何疑问可随时联系[阿里云SSL证书售前咨询](#)，阿里云SSL证书产品团队将竭诚为您提供更加便捷的服务！

17.2.【变更通知】SSL证书2年有效期变更及影响通知

尊敬的阿里云客户，您好：

从2020年9月1日起，苹果系统、谷歌和火狐浏览器计划调整受信SSL证书的有效期策略，上述系统或浏览器中受信SSL证书的最长有效期将从825天缩短至398天。对此，各CA厂商也将缩短SSL证书的最长有效期。受此影响，阿里云SSL证书计划于2020年8月20日起，停止售卖2年期SSL证书，具体影响如下：

- 2020年8月13日起，阿里云SSL证书将不再出售DigiCert及GeoTrust品牌下的2年期OV和EV证书。
- 2020年8月20日后，阿里云SSL证书将不再出售单张有效期为2年的SSL证书，即您新购买的SSL证书签发的最长有效期为365天，续费证书的最长有效期将缩短至398天。
- 2020年8月27日之前已经签发的证书不受影响，如果您的证书替换或新增绑定的域名后，新证书的最长有效期也将被限制在398天以内。

如何应对SSL证书的有效期策略变化，降低您的证书运营风险？阿里云SSL证书产品团队提示您：

- 合理利用现有证书规则，规划证书申请的有效生命周期，以防证书过期，导致业务中断。您也可以购买阿里云SSL证书托管服务，只需一次性支付2年的SSL证书费用，在您证书有效期第1年快过期前的30天内，阿里云SSL证书将自动为您重新签发一张新的证书，无需您手动操作。此外，托管服务还提供5次云产品自动部署服务，方便您将证书一键推送到云产品中。
- 有效利用证书管理工具，实现证书自动化管理。您可通过阿里云SSL证书控制台的上传证书功能，实现企业证书一站式管理、更新和全生命周期管理。

感谢您一直以来对阿里云SSL证书的关注和支持，如您有任何疑问可随时联系[阿里云SSL证书售前咨询](#)，阿里云SSL证书产品团队将竭诚为您提供更加便捷的服务！

已购买的2年期证书已无法提交申请该怎么办？

由于全球范围内CA厂家将SSL证书的最长有效期从2年缩短为1年，阿里云为已经购买还未申请证书的订单提供以下处理方案：

- 申请退款：您可以，定位到已购买的2年有效期证书的实例。单击退款，阿里云审核通过后，金额即可原路返回您的付款账户。
 - 申请替换：2020年9月15日前（包括9月15日），您可以，单击右上角工单 > 提交工单，在工单中提供将该证书的实例ID和需要将该证书拆分为2个1年有效期SSL证书的信息，阿里云审核后将10个工作日内为您完成拆分操作。
- 2020年9月16日起，阿里云将陆续对未提交替换申请的2年有效期证书订单执行退款操作。

 **注意** 拆分订单为不可逆操作，拆分后的订单无法申请退款。

17.3. 新冠疫情期间购买SSL证书赠送申请和安装服务

新冠疫情期间，大量用户远程办公，购买企业级OV、EV证书的用户在申请和安装部署环节可能会遇到困难。经阿里云与证书品牌方沟通，在2020年2月5日-2月29日期间，对所有已购买了阿里云OV、EV证书的用户免费提供一对一证书申请和安装配置专家服务。

 **说明** DV证书和免费证书暂不支持此次一对一免费服务，敬请谅解。

参考以下步骤申请此次一对一免费服务。

1. [单击此处](#)选购阿里云OV或EV版本证书。

云盾证书服务(包年)

选择证书类型

专业版OV

增强版OV Pro

高级版EV

增强版EV Pro

通配符DV

免费版(个人) DV

企业级SSL证书, 浏览器上有https提示并有绿锁标记, 1-5个工作日完成申请, 适合中小企业, 个人客户不支持申请。支持多张证书合并为1张。

选择品牌

GeoTrust

GlobalSign

CFCA

Symantec

GeoTrust是全球第二大数字证书颁发机构(CA), 属于DigiCert旗下品牌, 为企业提供低成本SSL数字证书, 性价比较高。全球150多个国家有超过10万用户在使用 GeoTrust 的产品来进行安全保护。

域名类型

通配符(泛域名)

单域名(1个域名)

多域名

保护一个主要域名和无限个同一级的子域名
例如: 申请*.domain.com, 证书将保护domain.com和它的全部同一级子域名(如a.domain.com, b.domain.com...)
.domain.com、.ssl.domain.com 均为泛域名。

选择域名个数

1 个

说明 购买证书时请选择OV或EV类型证书。详细内容请参见[购买SSL证书](#)。

- 在阿里云SSL证书控制台首页证书实例列表中, 定位到已购证书并复制该证书实例名称。证书实例名称是由一串数字和字母组合而成, 以cas-cn开头。例如: cas-cn-v123fqm123ul。

SSL证书					
证书总数 3	已签发的证书 1	待申请的证书 1	即将过期的证书 0	审核失败的证书 1	已过期的证书 0
购买证书 上传证书 一键式HTTPS					
已付款 1	全部品牌	证书域名	Q		
证书	品牌/类型	状态	绑定域名	有效期至	已部署
Symantec 免费版 SSL 实例: cas-9az... 证书未设置标签	Symantec 免费版 SSL	审核失败	20181121	1年	--
Symantec 增强型 OV SSL 实例: cas-cn-v123fqm123ul 证书未设置标签	Symantec 增强型 OV SSL	已付款	2.2.2.2	1年	--

- 单击此处进入[阿里云证书云市场专家服务页面](#)。
- 在云市场证书专家服务页面, 单击右上角[联系客服旺旺号](#), 将已复制的证书实例名称发送给服务商旺旺客服, 申请免费的套餐1 申请辅助+标准安装服务(5x8)。
- 根据旺旺客服提供的提示信息和指导, 完成证书安装配置。

说明 免费专家服务支持时间为2月5日-2月29日。最新的服务支持情况将根据此次疫情变化调整, 请随时关注阿里云SSL证书公告。

17.4. 【2020年5月3日】DigiCert系统定期维护通知

尊敬的阿里云用户:

接DigiCert通知，DigiCert将在北京时间2020年5月3日15:00~17:00对系统进行定期维护。尽管DigiCert已制定了预案来保障您服务的正常运行，但在此期间您的某些DigiCert服务可能无法使用。DigiCert将尽快恢复服务的正常访问，以确保您业务不会受到影响。

如果您在此系统维护时间内购买DigiCert（原Symantec品牌）和GeoTrust证书，可能受到如下影响：

- 除了GeoTrust DV订单以外，您可以正常提交收费类型的OV或EV订单、免费DV订单、通配符DV证书的购买订单，但订单的审核、签发会延迟到系统维护结束后进行处理。
- 您在提交GeoTrust DV订单时，会返回服务不可用的错误提示，您需要等待系统服务恢复稳定后才能正常提交订单。

阿里云SSL证书团队将在系统维护期间及维护结束后对您提交的订单进行持续跟踪和处理，确保您提交的订单都能及时得到处理。感谢您的支持和理解。

17.5. 【2020年4月23日】Symantec品牌证书标识变更通知

尊敬的阿里云用户：

由于CA认证机构DigiCert收购Symantec安全认证业务的原因，DigiCert将于2020年4月30日起，在全球范围内停止使用赛门铁克（Symantec）品牌，原Symantec品牌证书将正式更名为DigiCert品牌证书。因此，阿里云SSL证书团队将配合此次Symantec品牌标识变更，于2020年5月1日前，对阿里云售卖的Symantec品牌下所有规格证书标识全部替换为DigiCert标识。品牌标识变更示意图如下：



此外，DigiCert以遵守与NortonLifeLock Inc.（原称为赛门铁克公司）之间的协议，并更新了诺顿安全认证签章。签章示意图如下：



以上变更对您已在阿里云订购的Symantec证书的使用不会产生任何影响。

警告 如果您的网页或任何文件资料中已经使用了Symantec品牌信息，请于2020年5月1日前更换，否则可能面临相关法律责任。

在此期间，如您有任何异议，请随时与我们联系，阿里云SSL证书团队将一如既往竭诚为您服务。

17.6. 【2020年3月16日】DigiCert系统维护更新公告

DigiCert计划于北京时间2020年3月16日09:00至18:00对系统进行维护更新。

尽管DigiCert有冗余措施来保持服务的连续运行，但在此期间某些DigiCert服务可能会不可用。阿里云Symantec及GeoTrust证书服务方面，会存在以下影响。

- 收费类型OV/EV类型证书订单可正常提交，但订单的处理、签发在系统维护期间可能会有所延迟。
- 收费及免费DV类型证书订单，在系统维护期间将无法提交申请签发和申请吊销，需要等待系统更新维护结束、服务稳定后才能正常提交订单。

17.7. 【2020年3月8日】DigiCert系统维护更新公告

Digicert计划于北京时间2020年3月8日16:00-18:00对系统进行维护更新。

尽管DigiCert有冗余措施来保持服务的连续运行，但在此期间某些DigiCert服务可能会不可用。阿里云Symantec及GeoTrust证书服务方面，会存在以下影响。

- 收费类型OV/EV类型证书订单可正常提交，但订单的处理、签发在系统维护期间可能会有所延迟。
- 收费及免费DV类型证书订单，在系统维护期间将无法提交申请签发和申请吊销，需要等待系统更新维护结束、服务稳定后才能正常提交订单。

17.8. 【2019年12月23日】Symantec接口升级通知

【2019年12月19日】接到通知：CA中心计划于北京时间2019年12月23日23:00至2019年12月24日00:00，对CA中心接口进行升级更新。

CA中心接口升级更新期间，申请Symantec免费证书和Symantec DV通配符证书可能无法正常签发。敬请谅解！

17.9. 【2019年11月9日】Digicert系统升级更新公告

【2019年11月8日】接到通知：Digicert计划于北京时间2019年11月9日16:00至19:00，对系统进行升级更新。

系统升级更新期间，对于GeoTrust及Symantec品牌的DV和免费类型证书，提交的证书申请可能会失败。请知晓。

17.10. 【2019年9月22日】Digicert系统维护更新公告

【2019年9月16日】接到通知：DigiCert计划于北京时间2019年9月22日14:30至20:30，对系统进行维护更新。

系统维护更新期间，对于免费版DV、收费版DV类型证书，将无法提交申请签发和申请吊销；对于所有品牌的OV、EV类型证书，申请签发和申请吊销不受影响，但会推迟到更新结束后进行。

17.11. 【2019年4月6日】Digicert数据迁移用户公告

【2019年4月6日】刚接到DigiCert通知，对方正在迁移接口，在这期间所有Symantec品牌DV证书及免费证书将无法提交申请。如果遇到申请失败，请稍后尝试或等控制台公告。
DigiCert 计划于北京时间4月6日23:30 - 4月7日11:30对CA系统进行一次数据迁移，即完成对Symantec/GeoTrust系统及数据的切换。受此影响，在此期间将无法提交 Symantec/GeoTrust 品牌证书的订单申请。

从3月19日起，可能会出现提交订单出错或失败的情况。如遇该情况，请稍后重试。

详细信息请参见[DigiCert公告](#)。

给您带来不便，敬请谅解。

17.12. 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。

② 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。

GeoTrust

Approve SSL/TLS certificate request

A GeoTrust SSL/TLS certificate was requested for haju.com. As the domain contact for this order, you need to approve the request by verifying that you own or control the domain. We can issue certificates for haju.com after your approval.

Order Details

Domain Name: [Redacted]

Organization: [Redacted]

Authorization

I confirm that I am the Domain Contact for the domains referenced above. I confirm and agree that SSL/TLS certificates can be issued for sites ending in haju.com.

1. I, [Redacted], authority to apply for SSL certificates for this domain on behalf of [Redacted].

2. She [Redacted] o.Ltd. has the right to use and obtain SSL certificates for the domains listed above as well as any subdomains of the listed domains.

3. GeoTrust may rely on this authorization for any subsequent SSL certificate renewals or any orders placed by [Redacted] .Ltd. until this authorization is revoked by written notice sent to GeoTrust (Attention Legal), 2801 North Thanksgiving Way, Suite [Redacted] USA.

4. I will promptly notify GeoTrust if this authorization is revoked or if a domain name listed above is transferred to a 3rd party.

5. GeoTrust may reconfirm [Redacted] as control over the domains and approval of the corresponding certificates by sending a reconfirmation email to this email address. I acknowledge that I may not opt out of receiving reconfirmation emails.

Approve

点击此处

If this request contains any errors or you want to reject the request, please contact us at +1-866-436-8787.

- 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。

② 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

* 域名验证类型：☒ DNS ☐ 文件 ②

☒ 证书绑定的域名在【阿里云的云解析】产品中，授权系统自动添加一条记录以完成域名授权验证。



17.13. 【2018年11月17日】Symantec接口维护通知

今日收到 symantec 方面接口维护通知，在接口维护期间 Symantec、Geotrust 品牌证书DV及免费证书会出现提交失败的现象。

请暂时不要提交相关订单，待恢复后再进行提交。

2018年11月17日

17.14. 【2017年12月1日】Symantec与DigitalCert合并相关证书签发时效受影响

Digicert于2017年12月1日，完成对Symantec证书服务的并购。此后，所有新申请Symantec/GeoTrust 品牌证书，切换到Digicert+Symantec交叉认证PKI体系下签发。新根证书同时拥有两个根CA的兼容性，即兼容性更高。阿里云平台的Symantec/GeoTrust 已签发的旧根，也会按计划更新到新交叉根下。

从2017年12月1日到2017年12月20日，预计在此期间，OV/EV证书签发时间需要5~10个工作日；DV证书的签发，需要1~4个工作日。如果签发失败，建议您重新提交后等待鉴证系统签发队列签发。

Symantec免费证书预计要在本月底才能逐步恢复。

给您带来的不便之处，万分抱歉！在此期，如需紧急签发证书，建议更换为GlobalSign证书品牌，提工单要求加速签发GlobalSign证书。

17.15. 关于免费证书吊销延迟的说明公告

近日接到用户针对阿里云证书吊销延时的反馈，阿里云SSL证书服务就该问题进行了调查。详情如下：

Symantec被收购后，DigiCert对证书吊销系统进行了调整。该调整引起2019年11月01日~2020年11月30日签发的原Symantec证书，在阿里云证书控制台发起吊销后，吊销流程无法完成的问题。

阿里云SSL证书服务团队与CA中心就该问题进行了紧急沟通，目前已不支持通过控制台吊销免费证书。阿里云提供一次性申请20张免费证书额度的服务，满足您的业务需求。更多信息，请参见[申请免费DV试用证书](#)。

给您带来的不便，敬请谅解！

感谢您一直以来对阿里云SSL证书服务的关注和支持。如果您有任何疑问，请提交[工单](#)。阿里云SSL证书服务团队将竭诚为您服务！

17.16. 免费证书购买方式变更通知

为解决用户无法获知免费证书剩余额度的问题，从2021年1月1日起，阿里云SSL证书服务将为每个实名的个人主体或者企业主体提供1个自然年内，免费领取一次包含20张免费证书的资源包。

详细说明如下：

- 实名个人主体或企业主体（包括该企业的所有阿里云账号）下，1个自然年内只能领取一次包含20张免费证书的资源包（共包含20张免费证书）。
- 自然年是每年的01月01日~12月31日。
- 每年12月31日24:00:00，未领取的免费证书资源包额度将会清零。您需要等到第二年的1月1日00:00:00后申请领取当年的免费证书资源包。

关于如何领取免费的证书资源包，请参见[步骤一：领取免费证书额度](#)。

17.17. 【通知】国际站SSL证书服务将支持购买DigiCert品牌证书

尊敬的阿里云SSL证书用户：

阿里云SSL证书服务将于2021年05月12日在开放售卖DigiCert品牌SSL证书，支持的DigiCert证书规格包括：DV单域名、DV通配符域名、OV单域名（普通及Pro版本）、OV通配符域名（普通及Pro版本）、EV单域名（普通及Pro版本）。不同规格证书的具体价格，以购买页结算为准。

Digicert（原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。Digicert的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。

如果您的业务部署在中国内地以外的地域，推荐您通过国际站SSL证书服务选购证书。如需获得更多关于证书选型的建议，请提交[工单](#)。