

阿里云

SSL证书服务

API参考 (2020-04-07)

文档版本：20210105

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> <i>Instance_ID</i>
[] 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.API概览	05
2.调用方式	06
3.公共参数	07
4.CreateCertificateRequest	09
5.CreateCertificateWithCsrRequest	11
6.DeleteCertificateRequest	15
7.DescribePackageState	17
8.DescribeCertificateState	20

1.API概览

本文汇总了SSL证书服务提供的与证书资源包相关的API。

 **注意** 您只有已经购买证书资源包后，才可以使用本文罗列的API。关于如何购买证书资源包，请参见[购买证书资源包](#)。

证书资源包

API	描述
DescribePackageState	查询已经购买的证书资源包中DV证书的总个数和使用情况。
CreateCertificateRequest	提交DV证书申请（由系统自动创建CSR）。
CreateCertificateWithCsrRequest	使用已有的CSR提交DV证书申请。
DescribeCertificateState	查询已提交的证书申请的审核状态。
DeleteCertificateRequest	删除审核失败的证书申请。

2.调用方式

您可以通过发送HTTP GET请求调用SSL证书API，并按照接口说明在请求中加入相应的请求参数。调用接口后系统会返回处理结果。请求和返回结果都使用UTF-8字符集进行编码。

请求结构

SSL证书系统的API是RPC风格，您可以通过发送HTTP GET请求调用SSL证书的API。

其请求结构如下：

```
http://Endpoint/?Action=xx&Parameters
```

其中：

- Endpoint：SSL证书的API的服务接入地址为 *cas.aliyuncs.com*。
- Action：要执行的操作，如使用DescribeCertificateState查询证书申请状态。
- Version：要使用的API版本，SSL证书的API版本是 *2020-04-07*。
- Parameters：请求参数，每个参数之间用“&”分隔。

请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情请参见 [公共参数](#)。

下面是一个调用DescribeCertificateState接口查询证书申请状态的示例：

 说明 为了便于用户查看，本文档中的示例都做了格式化处理。

```
http(s)://cas.aliyuncs.com/?Action=DescribeCertificateState
&OrderId=123451222
&<公共请求参数>
```

3. 公共参数

本文档介绍了每个接口都需要使用的请求参数和返回参数。

公共请求参数

公共请求参数表

名称	类型	是否必须	描述
Format	String	否	返回消息的格式。取值： <ul style="list-style-type: none">JSON (默认值)XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值： 2020-04-07。
AccessKeyId	String	是	访问服务使用的密钥ID。
Signature	String	是	签名结果串。
SignatureMethod	String	是	签名方式，取值： HMAC-SHA1。
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间按照ISO8601标准，格式为YYYY-MM-DDThh:mm:ssZ。 例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。
SignatureVersion	String	是	签名算法版本，取值： 1.0。
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。 在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源所有者账户，即登录用户名。

示例

```
http(s)://cas.aliyuncs.com/?Action=DescribeCertificateState
&OrderId=123451222
&<公共请求参数>
```

公共返回参数

API返回结果采用统一格式，调用成功返回的数据格式有XML和JSON两种，可以在发送请求时指定返回的数据格式，默认为JSON格式。每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId。

- 返回 2xx HTTP状态码表示调用成功。
- 返回 4xx 或 5xx HTTP状态码表示调用失败。

公共返回参数示例如下：

- XML格式

```
<?xml version="1.0" encoding="utf-8"?>
  <!--结果的根结点-->
  <接口名称+Response>
    <!--返回请求标签-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!--返回结果数据-->
  </接口名称+Response>
```

- JSON格式

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /*返回结果数据*/
}
```


4.CreateCertificateRequest

调用CreateCertificateRequest完成扩展服务DV证书在购买、申请和签发流程。针对批量购买证书的场景，证书扩展服务可通过调用该API实现DV证书下单购买与申请证书一步完成。

 **说明** 您购买了证书扩展服务后，才可以使用该API。具体请参见[证书扩展服务](#)。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	位置	类型	是否必选	示例值	描述
Action	Query	String	是	CreateCertificateRequest	要执行的操作。取值： CreateCertificateRequest 。
Domain	Query	String	是	www.aliyun.com	申请证书时绑定的域名。
Email	Query	String	是	example@alibaba.com	申请人邮箱。
Phone	Query	String	是	1381111****	申请人手机号。
Username	Query	String	是	keller	申请人姓名。
ValidateType	Query	String	是	DNS	域名所有权验证方式。取值： <ul style="list-style-type: none">FILE：文件验证，通过在您域名服务器上创建指定文件来验证该域名的所有权。DNS：手动DNS验证。如果您需要保护的域名是非阿里云域名，您需要到该域名的管理平台中为该域名添加一条TXT类型的DNS记录。例如：如果您购买的是A公司的域名，您需要到A公司的域名管理平台添加DNS记录文件。

返回数据

名称	类型	示例值	描述
----	----	-----	----

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	阿里云为该请求生成的唯一标识符。
OrderId	Long	98987582437920968	订单证书ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateCertificateRequest
&Domain=www.aliyun.com
&Email=example@aliyun.com
&Phone=1381111****
&Username=keller
&ValidateType=DNS
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateCertificateRequestResponse>
  <RequestId>082FAB35-6AB9-4FD5-8750-D36673548E76</RequestId>
  <OrderId>1</OrderId>
</CreateCertificateRequestResponse>
```

JSON 格式

```
{
  "RequestId": "082FAB35-6AB9-4FD5-8750-D36673548E76",
  "OrderId": 1
}
```

错误码

访问[错误中心](#)查看更多错误码。

5.CreateCertificateWithCsrRequest

调用CreateCertificateWithCsrRequest购买、申请和签发自带CSR文件的DV证书。针对批量购买证书的场景，证书扩展服务可通过调用该API一步完成DV证书的购买和申请。

 **说明** 您购买了证书扩展服务后，才可以使用该API。具体请参见[证书扩展服务](#)。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateCertificateWithCsrRequest	要执行的操作。取值： CreateCertificateWithCsrRequest 。
Csr	String	是	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIC1TCCAb0CAQ AwgY8xCzAJBgN VBAYTAKNOMRlw EAYDVQQIDAIHd WFuZ3pob3Ux ETAPBgNVBACMC FNoZW56aGVuM Q8wDQYDVQQKD AZDaGFjdW8xEDA OBgNVBAsMB0lU IERlcHQxZzAVBgN VBAMMDnd3dy5ja GFjdW8ubmV0MR 0wGwYJKoZIhvcN AQkBFg44 MjkyNjY5QHFXLm NvbTCCASlwDQYJ KoZIhvcNAQEBBQ ADggEPADCCAQo CggEBA7 atRvQf9tKo1Nj/M QqzHvJjHNhU+0M MerDq+tRlj+a7Ro 1r6lWNF5MBOZ*** *** -----END CERTIFICATE REQUEST----- </pre>	<p>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）。</p> <p> 说明 该接口的CSR文件由您自己使用OpenSSL或Keytool工具手动生成。</p>

名称	类型	是否必选	示例值	描述
Email	String	是	example@aliyun.com	申请人邮箱。
Phone	String	是	1381111****	申请人手机号。
Username	String	是	keller	申请人姓名。
ValidateType	String	是	DNS	<p>域名所有权验证方式。取值：</p> <ul style="list-style-type: none"> DNS：手动DNS验证。如果您需要保护的域名是非阿里云域名，您需要到该域名的管理平台中为该域名添加一条TXT类型的DNS记录。例如：如果您购买的是A公司的域名，您需要到A公司的域名管理平台添加DNS记录。 FILE：文件验证，通过在您域名服务器上创建指定文件来验证该域名的所有权。
ProductCode	String	否	symantec-free-1-free	<p>证书品牌类型。取值：</p> <ul style="list-style-type: none"> symantec-free-1-free：免费单域名证书 symantec-dv-1-starter：Digicert DV通配符证书 geotrust-dv-w-starter：Geotrust DV通配符证书 geotrust-dv-1-starter：Geotrust DV单域名证书 globalsign-dv-1-personal：Globalsign DV单域名证书 globalsign-dv-w-advanced：Globalsign DV通配符证书

返回数据

名称	类型	示例值	描述
OrderId	Long	98987582437920968	订单证书ID。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	阿里云为该请求生成的唯一标识符。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateCertificateWithCsrRequest
&Csr=-----BEGIN CERTIFICATE REQUEST----- MIIC1TCCABoCAQAwgY8xCzAJBgNVBAYTAkNOMRIwEAYDVQQIDAI
HdWFuZ3pob3Ux ETAPBgNVBAcMCFNoZW56aGVuMQ8wDQYDVQQKDAZDaGFjdW8xEDA0BgNVBAcMB0lU IERl
cHQxZmFzAVBgNVBAMMDnd3dy5jaGFjdW8ubmV0MR0wGwYJKoZIhvcNAQkBFg44 MjkyNjY5QHFXLmNvbTCCASI
wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALo7 atRvQf9tKo1NJ/MQqzHvIjHNhU+0MMerDq+tRIJ+a7Ro
1r6IWNF5MB0Z***** -----END CERTIFICATE REQUEST-----
&Email=example@aliyun.com
&Phone=1381111****
&Username=keller
&ValidateType=DNS
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateCertificateWithCsrRequestResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <OrderId>98987582437920968</OrderId>
</CreateCertificateWithCsrRequestResponse>
```

JSON 格式

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "OrderId": "98987582437920968"
}
```

错误码


访问[错误中心](#)查看更多错误码。

HttpCode	错误码	描述
404	NotFoundPackage	没有购买套餐包。
404	NotRemainCount	套餐中不可用的证书数量。
403	CreateCertificateRequestFailed	创建请求失败。

HttpCode	错误码	描述
404	NotFoundOrder	没有找到证书订单。
403	OrderStateError	证书订单状态错误。
403	DeleteFail	删除证书订单失败。
500	Error	发生错误。

6.DeleteCertificateRequest

调用DeleteCertificateRequest删除DV证书申请失败的订单。

 **说明** 您购买了证书扩展服务后，才可以使用该API。具体请参见[证书扩展服务](#)。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteCertificateRequest	要执行的操作。取值： DeleteCertificateRequest 。
OrderId	Long	是	123451222	证书订单ID。

返回数据

名称	类型	示例值	描述
RequestId	String	DD73CB0A-6E99-49AB-9569-5A*****	请求消息的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteCertificateRequest
&OrderId=123451222
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteCertificateRequestResponse>
  <RequestId>082FAB35-6AB9-4FD5-8750-D36673548E76</RequestId>
</DeleteCertificateRequestResponse>
```

JSON 格式

```
{
  "RequestId":"082FAB35-6AB9-4FD5-8750-D36673548E76"
}
```


错误码

访问[错误中心](#)查看更多错误码。

HttpCode	错误码	描述
404	NotFoundPackage	没有购买套餐包。
404	NotRemainCount	套餐中不可用的证书的数量。
403	CreateCertificateRequestFailed	创建请求失败。
404	NotFoundOrder	没有找到订单。
403	OrderStateError	订单状态错误。
403	DeleteFail	删除失败。
500	Error	发生错误。

7. DescribePackageState

调用DescribePackageState查询已经购买的DV证书总数和使用情况。

 **说明** 您购买了证书扩展服务后，才可以使用该API。具体请参见[证书扩展服务](#)。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	位置	类型	是否必选	示例值	描述
Action	Query	String	是	DescribePackageState	要执行的操作。取值： DescribePackageState 。
ProductCode	Query	String	否	symantec-free-1-free	证书品牌类型。取值： <ul style="list-style-type: none"> symantec-free-1-free：免费单域名证书 symantec-dv-1-starter：Digicert DV通配符证书 geotrust-dv-w-starter：Geotrust DV通配符证书 geotrust-dv-1-starter：Geotrust DV单域名证书 globalsign-dv-1-personal：Globalsign DV单域名证书 globalsign-dv-w-advanced：Globalsign DV通配符证书

返回数据

名称	类型	示例值	描述
IssuedCount	Long	1	已经签发的DV证书的数量。

名称	类型	示例值	描述
ProductCode	String	symantec-free-1-free	证书品牌类型。取值： <ul style="list-style-type: none"> • symantec-free-1-free：免费单域名证书 • symantec-dv-1-starter：Digicert DV通配符证书 • geotrust-dv-w-starter：Geotrust DV通配符证书 • geotrust-dv-1-starter：Geotrust DV单域名证书 • globalsign-dv-1-personal：Globalsign DV单域名证书 • globalsign-dv-w-advanced：Globalsign DV通配符证书
RequestId	String	08F45EA0-66A7-4504-9B31-3589F5CE308D	请求消息的ID。
TotalCount	Long	10	已经购买的DV证书总数。
UsedCount	Long	2	已经申请的DV证书数量。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 只要发起CreateCertificateRequest请求就算已经申请了一张证书，不论是否签发。支持重复申请证书。</p> </div>

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePackageState
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePackageStateResponse>
  <RequestId>082FAB35-6AB9-4FD5-8750-D36673548E76</RequestId>
  <TotalCount>1</TotalCount>
  <UsedCount>1</UsedCount>
  <IssuedCount>1</IssuedCount>
  <ProductCode>symantec-free-1-free</ProductCode>
</DescribePackageStateResponse>
```

JSON 格式


```
{
  "RequestId": "082FAB35-6AB9-4FD5-8750-D36673548E76",
  "TotalCount": "1",
  "UsedCount": "1",
  "IssuedCount": "1",
  "ProductCode": "symantec-free-1-free"
}
```

错误码

访问[错误中心](#)查看更多错误码。

8.DescribeCertificateState

调用DescribeCertificateState查询DV证书的申请状态。

 **说明** 您购买了证书扩展服务后，才可以使用该API。具体请参见[证书扩展服务](#)。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	位置	类型	是否必选	示例值	描述
Action	Query	String	是	DescribeCertificateState	要执行的操作。取值： DescribeCertificateState 。
OrderId	Query	Long	是	123451222	证书订单ID。

返回数据

名称	类型	示例值	描述
Certificate	String	-----BEGIN CERTIFICATE----- MIIF..... -----END CERTIFICATE-----	当Type取值为 certificate 时，返回PEM格式证书。
Content	String	http://hangzhou.com/.well-known/pki-validation/fileauth.txt	当Type取值为 domain_verify 且ValidateType取值为 FILE 时，返回域名验证URL地址的URI的内容。
Domain	String	www.hangzhou.com	当Type取值为 domain_verify 且ValidateType取值为 FILE 时，返回待验证的域名。
PrivateKey	String	123456abbca	当Type取值为 certificate 时，返回PEM格式证书私钥。
RecordDomain	String	_dnsauth	当Type取值为 domain_verify 且ValidateType取值为 DNS 时，返回主机记录。

名称	类型	示例值	描述
RecordType	String	TXT	当Type取值为domain_verify且ValidateType取值为DNS时，返回验证记录类型。取值： <ul style="list-style-type: none"> TXT：文本记录 CNAME：别名记录
RecordValue	String	20200420000000223 erigacv46uhaubchc m0o7spxi7i2isvjq59 mlx9lucnkqcy	当Type取值为domain_verify且ValidateType取值为DNS时，返回记录值。
RequestId	String	08F45EA0-66A7- 4504-9B31- 3589F5C*****	请求消息的ID。
Type	String	process	证书申请状态类型。取值： <ul style="list-style-type: none"> process：表示证书正在申请中。 verify_fail：表示证书申请失败。您可以删除申请失败的证书，删除后不占用已申请的证书数量。 domain_verify：表示域名正在审核中。 certificate：表示证书已经签发。
Uri	String	/.well-known/pki- validation/fileauth.t xt	当Type取值为domain_verify且ValidateType取值为FILE时，返回待验证的URI。
ValidateType	String	DNS	当Type取值为domain_verify时，返回提交证书申请时选择的验证方式。取值： <ul style="list-style-type: none"> DNS：手动DNS验证。如果您需要保护的域名是非阿里云域名，您需要到该域名的管理平台中为该域名添加一条TXT类型的DNS记录。例如：如果您购买的是A公司的域名，您需要到A公司的域名管理平台添加DNS记录文件。 FILE：文件验证，通过在您域名服务器上创建指定文件来验证该域名的所有权。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeCertificateState
&OrderId=123451222
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeCertificateStateResponse>
  <RequestId>082FAB35-6AB9-4FD5-8750-D36673548E76</RequestId>
  <Type>domain_verify</Type>
  <ValidateType>FILE</ValidateType>
  <Domain>www.hangzhou.com</Domain>
  <Uri>/.well-known/pki-validation/fileauth.txt</Uri>
  <Content>http://hangzhou.com/.well-known/pki-validation/fileauth.txt</Content>
</DescribeCertificateStateResponse>
```

JSON 格式

```
{
  "RequestId": "082FAB35-6AB9-4FD5-8750-D36673548E76",
  "Type": "domain_verify",
  "ValidateType": "FILE",
  "Domain": "www.hangzhou.com",
  "Uri": "/.well-known/pki-validation/fileauth.txt",
  "Content": "http://hangzhou.com/.well-known/pki-validation/fileauth.txt"
}
```

错误码

访问[错误中心](#)查看更多错误码。