

云证书管理服务

API 参考

文档版本 01
发布日期 2025-10-29



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目 录

1 使用前必读.....	1
2 如何调用 API.....	3
2.1 构造请求.....	3
2.2 认证鉴权.....	5
2.3 返回结果.....	7
3 API 概览.....	9
4 API 说明.....	10
4.1 管理 SSL 证书.....	10
4.1.1 证书生命周期管理.....	10
4.1.1.1 查询证书列表.....	10
4.1.1.2 导入证书.....	17
4.1.1.3 获取证书详情.....	21
4.1.1.4 删除证书.....	28
4.1.1.5 导出证书.....	31
4.1.2 证书部署管理.....	34
4.1.2.1 推送证书.....	34
4.1.2.2 批量推送证书.....	37
4.1.2.3 部署证书.....	41
4.2 管理私有证书.....	45
4.2.1 私有 CA 管理.....	45
4.2.1.1 查询 CA 列表.....	46
4.2.1.2 创建 CA.....	53
4.2.1.3 查询 CA 配额.....	61
4.2.1.4 查询 CA 详情.....	65
4.2.1.5 删除 CA.....	71
4.2.1.6 导出 CA 的证书签名请求（CSR）.....	74
4.2.1.7 禁用 CA.....	77
4.2.1.8 启用 CA.....	80
4.2.1.9 导出 CA 证书.....	83
4.2.1.10 导入 CA 证书.....	87
4.2.1.11 恢复 CA.....	91
4.2.1.12 吊销 CA.....	94

4.2.2 私有证书管理.....	98
4.2.2.1 查询私有证书列表.....	98
4.2.2.2 申请证书.....	104
4.2.2.3 通过 CSR 签发证书.....	112
4.2.2.4 解析 CSR.....	118
4.2.2.5 查询私有证书配额.....	122
4.2.2.6 查询证书详情.....	126
4.2.2.7 删除证书.....	131
4.2.2.8 导出证书.....	134
4.2.2.9 吊销证书.....	138
4.2.3 证书吊销处理.....	142
4.2.3.1 查看是否具有委托权限.....	142
4.2.3.2 创建委托.....	145
4.2.3.3 查询 OBS 桶列表.....	148
5 权限和授权项.....	153
5.1 权限及授权项说明.....	153
5.2 SSL 证书管理.....	154
5.3 私有证书管理.....	154
A 附录.....	157
A.1 状态码.....	157
A.2 错误码.....	157
A.2.1 SSL 证书管理错误码.....	157
A.2.2 私有证书管理错误码.....	166
A.3 获取项目 ID.....	173
B 修订记录.....	174

1 使用前必读

概述

欢迎使用云证书管理服务（Cloud Certificate Manager，CCM）。云证书管理服务是一个为云上海量证书颁发和全生命周期管理的服务，可以应用在云平台、车联网、IoT 等多个场景。它可以提供SSL证书管理和私有证书管理功能。

调用说明

云证书管理服务提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见[如何调用API](#)。

终端节点

终端节点（Endpoint）即调用API的[请求地址](#)，CCM部署时不区分物理区域，为全局级服务。因此，CCM的终端节点如[表 云证书管理服务的终端节点](#)所示。您可以从[地区](#)和[终端节点](#)中查询服务的终端节点。

表 1-1 云证书管理服务的终端节点

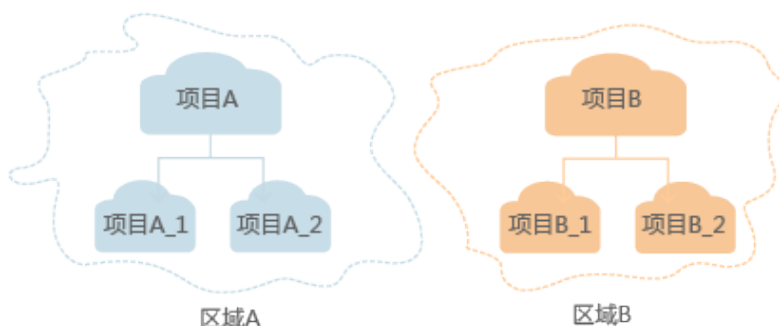
区域名称	区域	终端节点（Endpoint）	协议类型	包含微服务
所有	ALL	scm.my-kualalumpur-1.myhuaweicloud.com	HTTPS	SCM
所有	ALL	ccm.my-kualalumpur-1.myhuaweicloud.com	HTTPS	PCA

基本概念

- 账号
用户注册时的账号，账号对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。由于账号是付费主体，为了确保账号安全，建议您不要直接使用账号进行日常管理工作，而是创建用户并使用创建的用户进行日常管理工作。

- 用户
由账号在IAM中创建的用户，是云服务的使用人员，具有身份凭证（密码和访问密钥）。
在下，您可以查看账号ID和用户ID。通常在调用API的鉴权过程中，您需要用到账号、用户和密码等信息。
- 区域（Region）
从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）
一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。
- 项目
区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中创建资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

图 1-1 项目隔离模型



API 版本选择建议

SSH密钥对提供了V2.1和V2两个版本，建议您使用V2.1版本，能够更好的满足您的需求。

2 如何调用 API

2.1 构造请求

本节介绍如何构造REST API的请求，并以调用IAM服务的获取用户Token说明如何调用API，该API获取用户的Token，Token可以用于调用其他API时鉴权。

请求 URI

请求URI由如下部分组成。

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

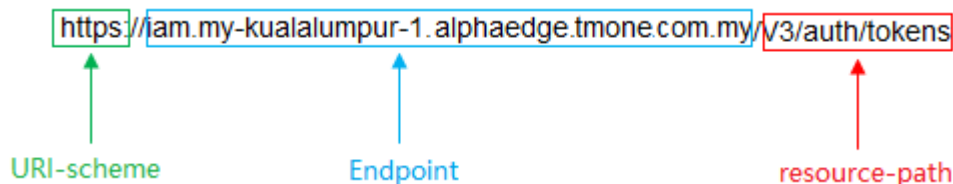
尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

- **URI-scheme:**
表示用于传输请求的协议，当前所有API均采用HTTPS协议。
- **Endpoint:**
指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从[地区和终端节点](#)获取。
例如IAM服务在“my-kualalumpur-1”区域的Endpoint为“iam.my-kualalumpur-1.alphaedge.tmone.com.my”。
- **resource-path:**
资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
- **query-string:**
查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“?”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取IAM在“my-kualalumpur-1”区域的Token，则需使用“my-kualalumpur-1”区域的Endpoint（iam.my-kualalumpur-1.alphaedge.tmone.com.my），并在[地区和终端节点](#)的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

`https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens`

图 2-1 URI 示意图



说明

为查看方便，在每个具体API的URI部分，只给出resource-path部分，并将请求方法写在一起。这是因为URI-scheme都是HTTPS，同一个服务的Endpoint在同一个区域也相同，所以简洁起见将这两部分省略。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **GET**：请求服务器返回指定资源。
- **PUT**：请求服务器更新指定资源。
- **POST**：请求服务器新增资源或执行特殊操作。
- **DELETE**：请求服务器删除指定资源，如删除对象等。
- **HEAD**：请求服务器资源头部。
- **PATCH**：请求服务器更新资源的部分内容。当资源不存在的时候，PATCH可能会去创建一个新的资源。

在获取用户Token的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

请求消息头

附加请求头字段，如指定的URI和HTTP方法所要求的字段。例如定义消息体类型的请求头“Content-Type”，请求鉴权信息等。

如下公共消息头需要添加到请求中。

- **Content-Type**：消息体的类型（格式），必选，默认取值为“application/json”，有其他取值时会在具体接口中专门说明。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用获取用户Token接口的响应值，该接口是唯一不需要认证的接口。

说明

API同时支持使用AK/SK认证，AK/SK认证是使用SDK对请求进行签名，签名过程会自动往请求中添加Authorization（签名认证信息）和X-Sdk-Date（请求发送的时间）请求头。

AK/SK认证的详细说明请参见[AK/SK认证](#)。

对于获取用户Token接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

对于获取用户Token接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中 ***username***为用户名，***domainname***为用户所属的账号名称，***********为用户登录密码，***xxxxxxxxxxxxxxxxxxxx***为project的名称，您可以从[地区和终端节点](#)获取。

说明

scope参数定义了Token的作用域，下面示例中获取的Token仅能访问project下的资源。您还可以设置Token作用域为某个账号下所有资源或账号的某个project下的资源，详细定义请参见获取用户Token。

POST https://iam.my-kualalumpur-1.alphaedge.tmon.com.my/v3/auth/tokens
Content-Type: application/json

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "*****",
          "domain": {
            "name": "domainname"
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "xxxxxxxxxxxxxxxxxxxx"
      }
    }
  }
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用[curl](#)、[Postman](#)或直接编写代码等方式发送请求调用API。对于获取用户Token接口，返回的响应消息头中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

2.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

Token 认证

说明

Token的有效期为24小时，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

Token在计算机系统中代表令牌（临时）的意思，拥有Token就代表拥有某种权限。Token认证就是在调用API的时候将Token加到请求消息头，从而通过身份认证，获得操作API的权限。

Token可通过调用获取用户Token接口获取，调用本服务API需要全局级别的Token，即调用获取用户Token接口时，请求body中auth.scope的取值需要选择domain，如下所示。

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "*****",
          "domain": {
            "name": "domainname"
          }
        }
      }
    },
    "scope": {
      "domain": {
        "name": "domainname"
      }
    }
  }
}
```

获取Token后，再调用其他接口时，您需要在请求消息头中添加“X-Auth-Token”，其值即为Token。例如Token值为“ABCDEFGH....”，则调用接口时将“X-Auth-Token: ABCDEFGH....”加到请求消息头即可，如下所示。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmon.com.my/v3/auth/tokens
Content-Type: application/json
X-Auth-Token: ABCDEFGH....
```

AK/SK 认证

说明

AK/SK签名认证方式仅支持消息体大小12MB以内，12MB以上的请求请使用Token认证。

AK/SK认证就是使用AK/SK对请求进行签名，在请求时将签名信息添加到消息头，从而通过身份认证。

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK(Secret Access Key)：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。详细的签名方法和SDK使用方法请参见[API签名指南](#)。

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

2.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见[状态码](#)。

对于获取用户Token接口，如果调用后返回状态码为“201”，则表示请求成功。

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于获取用户Token接口，返回如[图2-2](#)所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 2-2 获取用户 Token 响应消息头

```
connection → keep-alive
content-type → application/json
date → Tue, 12 Feb 2019 06:52:13 GMT
server → Web Server
strict-transport-security → max-age=31536000; includeSubdomains;
transfer-encoding → chunked
via → proxy A
x-content-type-options → nosniff
x-download-options → noopen
x-frame-options → SAMEORIGIN
x-iam-trace-id → Z18d45ab-d674-4995-af3a-2d0255ba41b5
x-subject-token → MIYXQYJKoZIhvcNAQcCoIIYtjCCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjwMTktMDItMTNUMC
fj3KJs6YgKnPvNRbW2eZ5eb78SZOkqjACgkqO1wi4JIGzrpd18LGXK5bdfq4lqHCYb8P4NaY0NYejcAgz/VeFYtLWT1GSO0zxKZmiQHq82HBqHdglZO9fuEbL5dMhdavj+33wEI
xHRC9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXI1jipPEGA270g1FruooL6jgglFkNPQuFSOU8+uSsttVwRtnfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CM8nOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==
x-xss-protection → 1; mode=block;
```

响应消息体（可选）

响应消息体通常以结构化格式返回，与响应消息头中Content-type对应，传递除响应消息头之外的内容。

对于获取用户Token接口，返回如下消息体。为篇幅起见，这里只展示部分内容。

```
{
  "token": {
    "expires_at": "2019-02-13T06:52:13.855000Z",
```

```
"methods": [  
  "password"  
],  
"catalog": [  
  {  
    "endpoints": [  
      {  
        "region_id": "xxxxxxx",  
.....
```

当接口调用出错时，会返回错误码及错误信息说明，错误响应的Body体格式如下所示。

```
{  
  "error": {  
    "message": "The request you have made requires authentication.",  
    "title": "Unauthorized"  
  }  
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

3 API 概览

通过使用云证书管理服务提供的接口，您可以完整地使用云证书管理服务的所有功能。

管理 SSL 证书

API	说明
证书生命周期管理	管理SSL证书生命周期。包括导入证书、删除证书、导出证书等接口。
证书部署管理	证书部署管理，包含推送证书及部署证书等接口。

管理私有证书

API	说明
私有CA管理	私有CA管理接口，包括私有CA的创建，查询，删除等接口。
私有证书管理	私有证书管理接口，包括私有证书的申请，查询，删除等接口。
证书吊销处理	证书吊销处理管理接口，包括委托授权的创建、查询等接口。

4 API 说明

4.1 管理 SSL 证书

4.1.1 证书生命周期管理

4.1.1.1 查询证书列表

功能介绍

根据证书名称或绑定域名查询证书列表。

URI

GET /v3/scm/certificates

表 4-1 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	每页条目数量，取值如下： 10：每页显示10条证书信息。 20：每页显示20条证书信息。 50：每页显示50条证书信息。 最小值：10 最大值：50 缺省值：10

参数	是否必选	参数类型	描述
offset	否	Integer	偏移量。 最小值：0 最大值：100 缺省值：0
sort_dir	否	String	排序方式。根据排序参数 sort_key进行排序，取值如下： • ASC：升序。 • DESC：降序。 缺省值：DESC 最小长度：0 最大长度：32
sort_key	否	String	排序依据参数，取值如下： • certExpiredTime：证书到期时间。 • certStatus：证书状态。 • certUpdateTime：证书更新时间。 缺省值：certUpdateTime 最小长度：0 最大长度：64
status	否	String	证书状态，取值如下： • ALL：所有证书状态。 • EXPIRED：证书已过期。 • UPLOAD：证书托管中。 缺省值：ALL 最小长度：0 最大长度：64

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	企业多项目ID。用户未开通企业多项目时，不需要输入该字段。用户开通企业多项目时，查询资源可以输入该字段。若用户不输入该字段，默认查询租户所有有权限的企业多项目下的资源。此时“enterprise_project_id”取值为“all”。若用户输入该字段，取值满足以下任一条件。 - 取值为“all” - 取值为“0” - 满足正则匹配：“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$” 缺省值： all 最小长度： 0 最大长度： 64
deploy_support	否	Boolean	是否仅筛选支持部署的证书。 缺省值： false
expired_days_since	否	Integer	证书在有效期内及最多过期xx天。 最小值： 0 最大值： 1095 缺省值： 0

请求参数

表 4-2 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度： 32 最大长度： 2097152

响应参数

状态码：200

表 4-3 响应 Body 参数

参数	参数类型	描述
certificates	Array of CertificateDetail objects	证书列表，详情请参见CertificateDetail 字段数据结构说明。 数组长度： 0 - 1000
total_count	Integer	证书数量。 最小值： 0 最大值： 10000

表 4-4 CertificateDetail

参数	参数类型	描述
id	String	证书id。 最小长度： 16 最大长度： 16
name	String	证书名称。 最大值： 63 最小长度： 3
domain	String	证书绑定的域名。 最小长度： 1 最大长度： 255
sans	String	多域名证书绑定的附加域名。 最小长度： 1 最大长度： 4096
signature_algorithm	String	签名算法。 最小长度： 0 最大长度： 64
deploy_support	Boolean	是否支持部署。
type	String	证书类型。 最小长度： 1 最大长度： 128
brand	String	证书品牌。 最小长度： 1 最大长度： 255

参数	参数类型	描述
expire_time	String	证书过期时间。 最小长度：1 最大长度：32
domain_type	String	域名类型。 最小长度：1 最大长度：128
validity_period	Integer	证书有效期，按月为单位。 最小值：12 最大值：12
status	String	证书状态，取值如下： - EXPIRED：证书已过期。 - UPLOAD：证书托管中。 最小长度：0 最大长度：64
domain_count	Integer	证书可绑定域名个数。 最小值：1 最大值：100
wildcard_count	Integer	证书可绑定泛域名个数。 最小值：0 最大值：100
description	String	证书描述。 最小长度：0 最大长度：255
domain_id	String	账号ID。 最小长度：0 最大长度：100

状态码：401

表 4-5 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-6 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-7 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

无

响应示例

状态码：200

正常返回。

```
{  
  "certificates" : [ {
```

```
{
  "id": "scs1554192131150",
  "name": "test",
  "domain": "www.zx.com",
  "sans": "a.zx.com;b.zx.com",
  "type": "null",
  "deploy_support": true,
  "signature_algorithm": "SHA256WITHRSA",
  "brand": "null",
  "expire_time": "2021-05-27 16:46:25.0",
  "domain_type": "null",
  "validity_period": 12,
  "status": "UPLOAD",
  "domain_count": 2,
  "wildcard_count": 0,
  "description": null
},
{
  "total_count": 1
}
```

状态码：401

认证失败。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码：403

禁止访问。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码：500

请求未完成，服务器内部异常。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
200	正常返回。
401	认证失败。
403	禁止访问。
404	访问页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.1.1.2 导入证书

功能介绍

导入证书到CCM服务管理。

URI

POST /v3/scm/certificates/import

请求参数

表 4-8 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度： 32 最大长度： 2097152

表 4-9 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	证书名称。字符长度为3~63位, 请输入英文字符, 数字, 下划线, 中划线, 英文句点。 最小长度： 3 最大长度： 63
certificate	是	String	证书内容, 可包含中间证书及根证书。若certificate_chain字段传入证书链, 则该字段只取证书本身。回车换行需要使用转义字符\n或者\r\n替换。 最小长度： 0 最大长度： 4096
certificate_chain	否	String	证书链, 非必填, 可通过certificate字段传入。回车换行需要使用转义字符\n或者\r\n替换。 最小长度： 0 最大长度： 8192

参数	是否必选	参数类型	描述
private_key	是	String	证书私钥。 不能上传带有口令保护的私钥，回车换行需要使用转义字符\n或者\r\n替换。 最小长度：0 最大长度：4096
duplicate_check	否	Boolean	是否允许上传相同证书。 • true：同意上传相同证书。 • false：不同意上传相同证书。
enterprise_project_id	否	String	企业多项目ID。用户未开通企业多项目时，不需要输入该字段。用户开通企业多项目时，查询资源可以输入该字段。若用户不输入该字段，默认查询租户所有有权限的企业多项目下的资源。此时“enterprise_project_id”取值为“all”。若用户输入该字段，取值满足以下任一条件。 • 取值为“all” • 取值为“0” • 满足正则匹配：“^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$” 最小长度：0 最大长度：64

响应参数

状态码：200

表 4-10 响应 Body 参数

参数	参数类型	描述
certificate_id	String	证书id。 最小长度：16 最大长度：16

状态码：401

表 4-11 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-12 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-13 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

```
{
  "name" : "test_cert",
  "certificate" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----BEGIN CERTIFICATE-----
*****-----END CERTIFICATE-----",
}
```

```
{  "private_key": "-----BEGIN RSA PRIVATE KEY-----*****-----END RSA PRIVATE KEY-----"}
```

响应示例

状态码：200

正常返回。

```
{  "certificate_id": "scs1600313391074"}
```

状态码：401

认证失败。

```
{  "error_code": "SCM.XXX",  "error_msg": "XXX"}
```

状态码：403

禁止访问。

```
{  "error_code": "SCM.XXX",  "error_msg": "XXX"}
```

状态码：500

请求未完成，服务器内部异常。

```
{  "error_code": "SCM.XXX",  "error_msg": "XXX"}
```

状态码

状态码	描述
200	正常返回。
401	认证失败。
403	禁止访问。
404	访问页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.1.1.3 获取证书详情

功能介绍

查询某张证书的详细信息。

URI

GET /v3/scm/certificates/{certificate_id}

表 4-14 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	证书id。 最小长度：16 最大长度：16

请求参数

表 4-15 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：32 最大长度：2097152

响应参数

状态码：200

表 4-16 响应 Body 参数

参数	参数类型	描述
id	String	证书id。 最小长度：16 最大长度：16

参数	参数类型	描述
status	String	证书状态。取值如下： - PAID：证书已支付，待申请证书。 - ISSUED：证书已签发。 - CHECKING：证书申请审核中。 - CANCELCHECKING：取消证书申请审核中。 - UNPASSED：证书申请未通过。 - EXPIRED：证书已过期。 - REVOKING：证书吊销申请审核中。 - REVOKED：证书已吊销。 - UPLOAD：证书托管中。 - SUPPLEMENTCHECKING：多域名证书新增附加域名审核中。 - CANCELSUPPLEMENTING：取消新增附加域名审核中。 最小长度：0 最大长度：32
order_id	String	订单id。 最小长度：0 最大长度：63
name	String	证书名称。 最小长度：3 最大长度：63
type	String	证书类型。取值如下： DV_SSL_CERT、DV_SSL_CERT_BASIC、 EV_SSL_CERT、 EV_SSL_CERT_PRO、OV_SSL_CERT、 OV_SSL_CERT_PRO。 最小长度：0 最大长度：32
brand	String	证书品牌。取值如下： GLOBALSIGN、SYMANTEC、 GEOTRUST、CFCA。 最小长度：0 最大长度：32
push_support	String	证书是否支持推送。 最小长度：0 最大长度：32

参数	参数类型	描述
revoke_reason	String	证书吊销原因。 最小长度：0 最大长度：255
signature_algorithm	String	签名算法。 最小长度：0 最大长度：64
issue_time	String	证书签发时间，没有获取到有效值时为空。 最小长度：0 最大长度：32
not_before	String	证书生效时间，没有获取到有效值时为空。 最小长度：0 最大长度：32
not_after	String	证书失效时间，没有获取到有效值时为空。 最小长度：0 最大长度：32
validity_period	Integer	证书有效期，按月为单位。 最小值：12 最大值：12
validation_method	String	域名认证方式，取值如下：DNS、FILE、EMAIL。 最小长度：0 最大长度：32
domain_type	String	域名类型，取值如下： • SINGLE_DOMAIN：单域名 • WILDCARD：通配符 • MULTI_DOMAIN：多域名 最小长度：0 最大长度：32
multi_domain_type	String	多域名类型，取值如下： • primary_single：主单域名 • primary_wildcard：主泛域名 最小长度：0 最大长度：32

参数	参数类型	描述
domain	String	证书绑定域名。 最小长度：0 最大长度：255
sans	String	证书绑定的附加域名信息。 最小长度：0 最大长度：4096
domain_count	Integer	证书可绑定域名个数。 最小值：1 最大值：100
wildcard_count	Integer	证书可绑定附加域名个数。 最小值：0 最大值：99
fingerprint	String	证书的SHA-1指纹。 最小长度：40 最大长度：40
shared	Boolean	是否是共享资源。
application_info	application_info object	证书申请信息。
description	String	证书的描述。 最小长度：0 最大长度：255
authentication	Array of Authentication objects	域名所有权认证信息，详情请参见 Authentication 字段数据结构说明。 数组长度：0 - 100

表 4-17 application_info

参数	参数类型	描述
country	String	国家。 最小长度：0 最大长度：255
company_name	String	公司名称。 最小长度：0 最大长度：255

参数	参数类型	描述
company_province	String	公司省份。 最小长度：0 最大长度：255
company_city	String	公司所在城市。 最小长度：0 最大长度：255
applicant_name	String	申请人名称。 最小长度：0 最大长度：255
applicant_phone	String	申请人电话。 最小长度：0 最大长度：255
applicant_email	String	申请人邮箱。 最小长度：0 最大长度：255
contact_name	String	技术联系人名称。 最小长度：0 最大长度：255
contact_phone	String	技术联系人电话。 最小长度：0 最大长度：255
contact_email	String	技术联系人邮箱。 最小长度：0 最大长度：255

表 4-18 Authentication

参数	参数类型	描述
record_name	String	域名校验值名字。 最小长度：0 最大长度：255
record_type	String	域名校验值类型。 最小长度：0 最大长度：255

参数	参数类型	描述
record_value	String	域名校验值。 最小长度：0 最大长度：255
domain	String	校验值对应的域名。 最小长度：0 最大长度：255

状态码：401

表 4-19 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-20 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-21 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

无

响应示例

状态码：200

正常返回。

```
{
  "id" : "scs1590053258704",
  "order_id" : null,
  "name" : "scm-testing",
  "type" : null,
  "brand" : null,
  "push_support" : "OFF",
  "revoke_reason" : null,
  "status" : "UPLOAD",
  "signature_algorithm" : null,
  "issue_time" : null,
  "not_before" : null,
  "not_after" : null,
  "validity_period" : 12,
  "validation_method" : null,
  "domain_type" : null,
  "multi_domain_type" : null,
  "domain" : "hosting-*****.test.cn",
  "sans" : null,
  "domain_count" : 1,
  "wildcard_count" : 0,
  "fingerprint" : "185d687de3f44f2249d0e0f084efccb56b7c2cbe",
  "enterprise_project_id" : "0"
}
```

状态码：401

认证失败。

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

禁止访问。

```
{
  "error_code" : "SCM.XXX",
}
```

```
{  
  "error_msg": "XXX"  
}
```

状态码：500

请求未完成，服务器内部异常。

```
{  
  "error_code": "SCM.XXX",  
  "error_msg": "XXX"  
}
```

状态码

状态码	描述
200	正常返回。
401	认证失败。
403	禁止访问。
404	请求页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.1.1.4 删除证书

功能介绍

删除证书实例，即将证书资源从系统中删除。

URI

DELETE /v3/scm/certificates/{certificate_id}

表 4-22 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	证书id。 最小长度：16 最大长度：16

请求参数

表 4-23 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：32 最大长度：2097152

响应参数

状态码：204

正常返回。

状态码：401

表 4-24 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-25 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-26 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

无

响应示例

状态码：401

认证失败。

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

禁止访问。

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

请求未完成，服务器内部异常。

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
204	正常返回。
401	认证失败。
403	禁止访问。

状态码	描述
404	请求页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.1.1.5 导出证书

功能介绍

导出证书。

URI

POST /v3/scm/certificates/{certificate_id}/export

表 4-27 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	证书id。 最小长度：16 最大长度：16

请求参数

表 4-28 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：32 最大长度：2097152

响应参数

状态码：200

表 4-29 响应 Body 参数

参数	参数类型	描述
entire_certificate	String	证书及证书链。 最小长度：1 最大长度：12288
certificate	String	证书内容，不包含证书链。 最小长度：1 最大长度：4096
certificate_chain	String	证书链。 最小长度：1 最大长度：8192
private_key	String	证书私钥。 最小长度：1 最大长度：4096

状态码：401

表 4-30 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-31 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-32 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

无

响应示例

状态码：200

正常返回。

```
{
  "entire_certificate" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----BEGIN CERTIFICATE-----
*****-----END CERTIFICATE-----",
  "certificate" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----",
  "certificate_chain" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----",
  "private_key" : "-----BEGIN RSA PRIVATE KEY-----*****-----END RSA PRIVATE KEY-----"
}
```

状态码：401

认证失败。

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

禁止访问。

```
{
  "error_code" : "SCM.XXX",
}
```

```
"error_msg": "XXX"
}
```

状态码：500

请求未完成，服务器内部异常。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
200	正常返回。
401	认证失败。
403	禁止访问。
404	访问页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.1.2 证书部署管理

4.1.2.1 推送证书

功能介绍

推送SSL证书到弹性负载均衡（Elastic Load Balance，简称ELB）、Web应用防火墙（Web Application Firewall，WAF）等其它云产品中。

URI

POST /v3/scm/certificates/{certificate_id}/push

表 4-33 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	证书id。 最小长度： 16 最大长度： 16

请求参数

表 4-34 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：32 最大长度：2097152

表 4-35 请求 Body 参数

参数	是否必选	参数类型	描述
target_project	是	String	推送到的目标服务所在的区域。 最小长度：1 最大长度：255
target_service	是	String	证书推送的目标服务，当前仅支持：CDN、WAF、ELB。 最小长度：1 最大长度：64

响应参数

状态码：204

正常返回。

状态码：401

表 4-36 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-37 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-38 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

```
{
  "target_service": "waf",
  "target_project": "cn-north-7"
}
```

响应示例

状态码：401

认证失败。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码：403

禁止访问。

```
{
  "error_code": "SCM.XXX",
}
```

```
{
  "error_msg": "XXX"
}
```

状态码：500

请求未完成，服务器内部异常。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
204	正常返回。
401	认证失败。
403	禁止访问。
404	访问页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.1.2.2 批量推送证书

功能介绍

批量推送SSL证书到弹性负载均衡（Elastic Load Balance，简称ELB）、Web应用防火墙（Web Application Firewall，WAF）等其它云产品中。

URI

POST /v3/scm/certificates/{certificate_id}/batch-push

表 4-39 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	证书id。 最小长度： 16 最大长度： 16

请求参数

表 4-40 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：32 最大长度：2097152

表 4-41 请求 Body 参数

参数	是否必选	参数类型	描述
target_projects	是	Array of strings	推送到的目标服务所在的区域，CDN、ELB、WAF。 最小长度：1 最大长度：32 数组长度：1 - 10
target_service	是	String	证书推送的目标服务，当前仅支持：CDN、WAF、ELB。 最小长度：1 最大长度：64

响应参数

状态码：200

表 4-42 响应 Body 参数

参数	参数类型	描述
results	Array of results objects	部署结果。 数组长度：1 - 10

表 4-43 results

参数	参数类型	描述
project_name	String	推送区域名称，如cn-north-7。 最小长度：0 最大长度：63
cert_id	String	目标证书ID。 最小长度：0 最大长度：255
message	String	推送结果。 最小长度：0 最大长度：255

状态码：401

表 4-44 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-45 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-46 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

```
{
  "target_service": "waf",
  "target_projects": [ "my-kualalumpur-1" ]
}
```

响应示例

状态码：200

正常返回。

```
{
  "results": [ {
    "project_name": "cn-north-7",
    "cert_id": "scs16751254852691",
    "message": "success"
  } ]
}
```

状态码：401

认证失败。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码：403

禁止访问。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码：500

请求未完成，服务器内部异常。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
200	正常返回。
401	认证失败。
403	禁止访问。
404	访问页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.1.2.3 部署证书

功能介绍

部署SSL证书到弹性负载均衡（Elastic Load Balance，简称ELB）、Web应用防火墙（Web Application Firewall，WAF）等其它云产品中。

接口约束

- 上传证书，部署其他云产品中，部署费用30元/域名。

URI

POST /v3/scm/certificates/{certificate_id}/deploy

表 4-47 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	证书id。 最小长度：16 最大长度：16

请求参数

表 4-48 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：32 最大长度：2097152

表 4-49 请求 Body 参数

参数	是否必选	参数类型	描述
project_name	否	String	部署的资源所在的项目名称，若在主项目下，则该值为region id。 最小长度：1 最大长度：255
service_name	是	String	证书推送的目标服务，当前仅支持：WAF、ELB。 最小长度：1 最大长度：64
resources	是	Array of DeployedResource objects	所要部署的资源列表。 数组长度：1 - 20

表 4-50 DeployedResource

参数	是否必选	参数类型	描述
id	否	String	资源Id，部署WAF与ELB时，必传此字段。 最小长度：0 最大长度：63
type	否	String	资源类型，当前仅部署WAF资源时需传入，即独享模式（premium）与云模式（cloud）。 最小长度：0 最大长度：63

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	需部署的资源所属的企业项目ID，当前仅部署WAF资源时，需传入。 最小长度：0 最大长度：63

响应参数

状态码：200

表 4-51 响应 Body 参数

参数	参数类型	描述
failure_list	Array of FaiureResource objects	部署失败的资源列表。 数组长度：1 - 20

表 4-52 FaiureResource

参数	参数类型	描述
resource	String	部署失败的资源信息，部署WAF与ELB时，此字段为资源ID，部署CDN时，本字段为加速域名。 最小长度：0 最大长度：63
failure_info	String	失败原因，一般为目标服务返回的错误码信息。 最小长度：0 最大长度：255

状态码：401

表 4-53 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：403

表 4-54 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

状态码：500

表 4-55 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。 最小长度：3 最大长度：36
error_msg	String	错误请求返回的错误信息。 最小长度：0 最大长度：1024

请求示例

```
{
  "service_name": "ELB",
  "project_name": "cn-north-7",
  "resources": [ {
    "id": "982b8a6a6ebc43809d82a46ca99aaeb7"
  } ]
}
```

响应示例

状态码：200

正常返回。

```
{
  "failure_list": [ {
    "resource": "982b8a6a6ebc43809d82a46ca99aaeb7",
    "failure_info": "ELB.8904:certificate 982b8a6a6ebc43809d82a46ca99aaeb7 does not exist"
  } ]
}
```

状态码：401

认证失败。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码：403

禁止访问。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码：500

请求未完成，服务器内部异常。

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
200	正常返回。
401	认证失败。
403	禁止访问。
404	访问页面未找到。
500	请求未完成，服务器内部异常。

错误码

请参见[错误码](#)。

4.2 管理私有证书

4.2.1 私有 CA 管理

4.2.1.1 查询 CA 列表

功能介绍

查询CA列表。

URI

GET /v1/private-certificate-authorities

表 4-56 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	指定查询返回记录条数，默认值 10。
name	否	String	CA证书名称（CN）过滤值，用于获取名称中带有特定值的CA证书集合。
offset	否	Integer	索引位置，从offset指定的下一条数据开始查询。默认值为0。
status	否	String	CA证书状态，通过状态过滤证书集合： ● PENDING：待激活，此状态下，不可用于签发证书； ● ACTIVED：已激活，此状态下，可用于签发证书； ● DISABLED：已禁用，此状态下，不可用于签发证书； ● DELETED：计划删除，此状态下，不可用于签发证书； ● EXPIRED：已过期，此状态下，不可用于签发证书。
type	否	String	CA证书类型： ● ROOT：根CA证书 ● SUBORDINATE：从属CA证书
sort_key	否	String	排序属性，目前支持以下属性： ● create_time：证书创建时间（默认） ● common_name：证书名称 ● ca_type：CA证书类型 ● not_after：证书到期时间

参数	是否必选	参数类型	描述
sort_dir	否	String	排序方向，支持以下值： • DESC：降序（默认） • ASC：升序

请求参数

表 4-57 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-58 响应 Body 参数

参数	参数类型	描述
total	Integer	CA证书总数。
certificate_authorities	Array of CertificateAuthorities objects	CA列表，详情请参见 CertificateAuthorities 字段数据结构说明。

表 4-59 CertificateAuthorities

参数	参数类型	描述
ca_id	String	CA证书ID。
type	String	CA类型： • ROOT: 根CA • SUBORDINATE: 从属CA

参数	参数类型	描述
status	String	CA证书状态： ● PENDING：待激活，此状态下，不可用于签发证书； ● ACTIVED：已激活，此状态下，可用于签发证书； ● DISABLED：已禁用，此状态下，不可用于签发证书； ● DELETED：计划删除，此状态下，不可用于签发证书； ● EXPIRED：已过期，此状态下，不可用于签发证书。
path_length	Integer	CA路径长度。 说明 注：生成的根CA证书，其路径长度不做限制，但本字段在数据库中统一置为7。从属CA的路径长度在创建时由用户指定，缺省值为0。
issuer_id	String	父CA证书ID，即签发此证书的CA证书ID。根CA中，此参数为 null 。
issuer_name	String	父CA证书名称。根CA中，此参数为 null 。
key_algorithm	String	密钥算法。
signature_algorithm	String	签名哈希算法。
freeze_flag	Integer	冻结标识： ● 0：非冻结状态； ● 其它值：冻结状态，当前预留。
gen_mode	String	证书生成方式： ● GENERATE：PCA系统生成； ● IMPORT：外部导入； ● CSR：外部提供CSR，内部CA进行签发，即私钥不在PCA进行托管。
serial_number	String	证书序列号。
create_time	Long	证书创建时间，格式为时间戳（毫秒级）。
delete_time	Long	证书删除时间，格式为时间戳（毫秒级）。
not_before	Long	证书创建时间，格式为时间戳（毫秒级）。

参数	参数类型	描述
not_after	Long	证书到期时间，格式为时间戳（毫秒级）。
distinguished_name	DistinguishedName object	证书名称配置，详情请参见 DistinguishedName 字段数据结构说明。
crl_configuration	ListCrlConfiguration object	证书CRL配置，详情请参见 ListCrlConfiguration 字段数据结构说明。

表 4-60 DistinguishedName

参数	参数类型	描述
common_name	String	证书通用名称（CN）。
country	String	国家编码，需符合正则" [A-Za-z]{2} "。
state	String	省市名称。
locality	String	地区名称。
organization	String	组织名称。
organizational_unit	String	组织单元名称。

表 4-61 ListCrlConfiguration

参数	参数类型	描述
enabled	Boolean	是否启用CRL发布功能。 • true • false
crl_name	String	吊销列表文件名称。 说明 若用户不指定，系统将默认采用当前证书的父CA ID。
obs_bucket_name	String	OBS桶名称。
valid_days	Integer	CRL更新周期，单位为"天"。当启用CRL发布功能，为必填项。

参数	参数类型	描述
crl_dis_point	String	吊销列表分发地址，即对应的OBS桶中的CRL文件地址。 说明 本参数由程序根据crl_name、obs_bucket_name以及OBS地址进行拼接而成。

状态码：400

表 4-62 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-63 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-64 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-65 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-66 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查询CA证书列表，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities

响应示例

状态码：200

请求已成功

```
{
  "total": 2,
  "certificate_authorities": [ {
    "signature_algorithm": "SHA384",
    "issuer_id": null,
    "issuer_name": null,
    "not_after": 1678159435000,
    "not_before": 1646623375000,
    "status": "ACTIVED",
    "freeze_flag": 0,
    "gen_mode": "GENERATE",
    "serial_number": "202203070322544291829058",
    "distinguished_name": {
      "country": "cn",
      "state": "shanghai",
      "locality": "shanghai",
      "organization": "shanghai",
      "organizational_unit": "shanghai",
      "common_name": "CSR_123"
    },
    "key_algorithm": "EC384",
    "create_time": 1646623375000,
    "delete_time": null,
    "ca_id": "a6bbf0be-79f3-4f66-858a-0fdc96dfcbe",
    "type": "ROOT",
    "path_length": 7,
    "crl_configuration": {
      "enabled": false,
      "obs_bucket_name": null,
      "valid_days": null,
      "crl_name": null,
      "crl_dis_point": null
    }
  }
]
```

```
}
}, {
  "signature_algorithm": "SHA256",
  "issuer_id": null,
  "issuer_name": null,
  "not_after": 1727492412000,
  "not_before": 1632797952000,
  "status": "ACTIVED",
  "freeze_flag": 0,
  "gen_mode": "GENERATE",
  "serial_number": "202109280259122080649087",
  "distinguished_name": {
    "country": "CN",
    "state": "Sichuan",
    "locality": "Chengdu",
    "organization": "Huawei",
    "organizational_unit": "CloudBU",
    "common_name": "pca-ca"
  },
  "key_algorithm": "RSA2048",
  "create_time": 1632797953000,
  "delete_time": null,
  "ca_id": "fb7bd6a6-6a11-4a58-8710-a3c0a620aedc",
  "type": "ROOT",
  "path_length": 7,
  "crl_configuration": {
    "enabled": false,
    "obs_bucket_name": null,
    "valid_days": null,
    "crl_name": null,
    "crl_dis_point": null
  }
}
}]
}
```

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.2 创建 CA

功能介绍

创建CA，分以下三种情况：

- 创建根CA，根据参数介绍中，填写必选值；
- 创建从属CA，并需要直接激活该证书，根据参数介绍中，填写必选值；
- 创建从属CA，不需要直接激活该证书，请求body中只需要缺少此三个参数之一即可：issuer_id、signature_algorithm、validity。

URI

POST /v1/private-certificate-authorities

请求参数

表 4-67 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

表 4-68 请求 Body 参数

参数	是否必选	参数类型	描述
type	是	String	创建的CA类型。 ● ROOT : 根CA ● SUBORDINATE : 从属CA
distinguished_name	是	DistinguishedName object	证书名称配置, 详情请参见 DistinguishedName 字段数据结构说明。
key_algorithm	是	String	密钥算法, 可选值如下: ● RSA2048 : RSA算法, 密钥长度2048位; ● RSA4096 : RSA算法, 密钥长度4096位; ● EC256 : 椭圆曲线算法 (Elliptic Curve Digital Signature Algorithm (ECDSA)), 密钥长度256位; ● EC384 : 椭圆曲线算法 (Elliptic Curve Digital Signature Algorithm (ECDSA)), 密钥长度384位。
validity	否	Validity object	证书有效期, 分以下三种情况: ● 创建根CA, 为必填值; ● 创建从属CA, 并需要直接激活该证书, 为必填值; ● 创建从属CA, 不需要直接激活该证书, 本参数值将被忽略, 激活证书时需要再次传入。 说明 详情请参见 Validity 字段数据结构说明。

参数	是否必选	参数类型	描述
issuer_id	否	String	父CA证书ID，分以下三种情况： • 创建根CA，根CA为自签名证书，无父CA，将忽略该参数； • 创建从属CA，并需要直接激活该证书，为必填值； • 创建从属CA，不需要直接激活该证书，本参数值将被忽略，激活证书时需要再次传入。
path_length	否	Integer	CA证书路径长度，分以下三种情况： • 创建根CA，为便于后期对证书层级的扩展，根CA默认不对路径长度做限制，故将忽略该参数。证书层级规划可由从属CA做限制； • 创建从属CA，并需要直接激活该证书，用户可自定义。缺省值为0； • 创建从属CA，不需要直接激活该证书，本参数值将被忽略。激活证书时若要自定义，需要再次传入；
signature_algorithm	否	String	签名哈希算法。 • 分以下三种情况： - 创建根CA，为必填值； - 创建从属CA，并需要直接激活该证书，为必填值； - 创建从属CA，不需要直接激活该证书，本参数值将被忽略，激活证书时需要再次传入。 • 可选值如下： - SHA256 - SHA384 - SHA512

参数	是否必选	参数类型	描述
key_usages	否	Array of strings	密钥用法，具体标准参见RFC 5280中:4.2.1.3节。 • digitalSignature : 数字签名; • nonRepudiation : 不可抵赖; • keyEncipherment : 密钥用于加密密钥数据; • dataEncipherment : 用于加密数据; • keyAgreement : 密钥协商; • keyCertSign : 签发证书; • cRLSign : 签发吊销列表; • encipherOnly : 仅用于加密; • decipherOnly : 仅用于解密。 说明 缺省值如下: • 根CA证书: 默认为**[digitalSignature,keyCertSign,cRLSign]**, 忽略用户传入值; • 从属CA证书: 默认为**[digitalSignature,keyCertSign,cRLSign]**, 支持用户自定义。
crl_configuration	否	CrlConfiguration object	证书CRL配置, 详情请参见 CrlConfiguration 字段数据结构说明。

表 4-69 DistinguishedName

参数	是否必选	参数类型	描述
common_name	是	String	证书通用名称 (CN) 。
country	是	String	国家编码, 需符合正则"[A-Za-z]{2}"。
state	是	String	省市名称。
locality	是	String	地区名称。

参数	是否必选	参数类型	描述
organization	是	String	组织名称。
organizational_unit	是	String	组织单元名称。

表 4-70 Validity

参数	是否必选	参数类型	描述
type	是	String	有效期类型，为必填值： • YEAR：年（12个月） • MONTH：月（统一按31天） • DAY：日 • HOURL：小时
value	是	Integer	证书有效期值，与type对应的类型值，换算成年需满足以下规则： • 根CA，有效期小于等于30年； • 从属CA与私有证书，有效期小于等于20年。
start_from	否	Integer	起始时间，为可选值： • 格式为时间戳（毫秒级），如1645146939688代表2022-02-18 09:15:39； • 不早于当前时间5分钟，即 $start_from > (current_time - 5min)$。

表 4-71 CrlConfiguration

参数	是否必选	参数类型	描述
enabled	是	Boolean	是否启用CRL发布功能。 • true • false
crl_name	否	String	吊销列表文件名称。 说明 若用户不指定，系统将默认采用当前证书的父CA ID。

参数	是否必选	参数类型	描述
obs_bucket_name	否	String	OBS桶名称。 说明 当需要启用CRL发布功能： - 此参数为必填项，且用户必须已创建委托授权，授予PCA服务对OBS的相关权限，具体参见本文档：证书吊销处理>查看是否具有委托权限、证书吊销处理>创建委托； - 指定的OBS桶必须存在，否则将报错。
valid_days	否	Integer	CRL更新周期，单位为"天"。当启用CRL发布功能，为必填项。

响应参数

状态码：200

表 4-72 响应 Body 参数

参数	参数类型	描述
ca_id	String	当前签发的CA证书ID。

状态码：400

表 4-73 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-74 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-75 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404**表 4-76 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500**表 4-77 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

创建CA证书，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities

```
{
  "type": "ROOT",
  "key_algorithm": "RSA4096",
  "signature_algorithm": "SHA512",
  "distinguished_name": {
    "common_name": "demoRootRSA",
    "country": "CN",
    "locality": "chengdu",
    "organization": "HW",
    "organization_unit": "dew",
    "state": "sichuan"
  },
  "validity": {
    "type": "YEAR",
    "value": 3
  },
  "crl_configuration": {
```

```
"enabled" : false,
"obs_bucket_name" : "demoBucket",
"valid_days" : 8
}
}
```

响应示例

状态码：200

请求已成功

```
{
  "ca_id" : "66504812-fedc-414a-9b7c-4c1836398524"
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.3 查询 CA 配额

功能介绍

查询CA证书配额。

URI

GET /v1/private-certificate-authorities/quotas

请求参数

表 4-78 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-79 响应 Body 参数

参数	参数类型	描述
quotas	Quotas object	证书配额，详情请参见 Quotas 字段数据结构说明。

表 4-80 Quotas

参数	参数类型	描述
resources	Array of Resources objects	资源配额列表，详情请参见 Resources 字段数据结构说明。

表 4-81 Resources

参数	参数类型	描述
type	String	证书类型: • CERTIFICATE_AUTHORITY: CA证书; • CERTIFICATE: 私有证书。
used	Integer	已使用配额数。
quota	Integer	配额总数: • CERTIFICATE_AUTHORITY: 当前系统指定100; • CERTIFICATE: 当前系统指定100000。

状态码：400

表 4-82 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-83 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-84 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-85 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-86 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查询CA证书配额，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/quotas

响应示例

状态码：200

请求已成功

```
{
  "quotas": {
    "resources": [ {
      "type": "CERTIFICATE_AUTHORITY",
      "used": 25,
      "quota": 100
    } ]
  }
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.4 查询 CA 详情

功能介绍

查询CA详情。

URI

GET /v1/private-certificate-authorities/{ca_id}

表 4-87 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	CA证书ID。

请求参数

表 4-88 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-89 响应 Body 参数

参数	参数类型	描述
ca_id	String	CA证书ID。
type	String	CA类型: • ROOT: 根CA • SUBORDINATE: 从属CA

参数	参数类型	描述
status	String	CA证书状态： ● PENDING：待激活，此状态下，不可用于签发证书； ● ACTIVED：已激活，此状态下，可用于签发证书； ● DISABLED：已禁用，此状态下，不可用于签发证书； ● DELETED：计划删除，此状态下，不可用于签发证书； ● EXPIRED：已过期，此状态下，不可用于签发证书。
path_length	Integer	CA路径长度。 说明 注：生成的根CA证书，其路径长度不做限制，但本字段在数据库中统一置为7。从属CA的路径长度在创建时由用户指定，缺省值为0。
issuer_id	String	父CA证书ID，即签发此证书的CA证书ID。根CA中，此参数为 null 。
issuer_name	String	父CA证书名称。根CA中，此参数为 null 。
key_algorithm	String	密钥算法。
signature_algorithm	String	签名哈希算法。
freeze_flag	Integer	冻结标识： ● 0：非冻结状态； ● 其它值：冻结状态，当前预留。
gen_mode	String	证书生成方式： ● GENERATE：PCA系统生成； ● IMPORT：外部导入； ● CSR：外部提供CSR，内部CA进行签发，即私钥不在PCA进行托管。
serial_number	String	证书序列号。
create_time	Long	证书创建时间，格式为时间戳（毫秒级）。
delete_time	Long	证书删除时间，格式为时间戳（毫秒级）。
not_before	Long	证书创建时间，格式为时间戳（毫秒级）。

参数	参数类型	描述
not_after	Long	证书到期时间，格式为时间戳（毫秒级）。
distinguished_name	DistinguishedName object	证书名称配置，详情请参见 DistinguishedName 字段数据结构说明。
crl_configuration	ListCrlConfiguration object	证书CRL配置，详情请参见 ListCrlConfiguration 字段数据结构说明。

表 4-90 DistinguishedName

参数	参数类型	描述
common_name	String	证书通用名称（CN）。
country	String	国家编码，需符合正则" [A-Za-z]{2} "。
state	String	省市名称。
locality	String	地区名称。
organization	String	组织名称。
organizational_unit	String	组织单元名称。

表 4-91 ListCrlConfiguration

参数	参数类型	描述
enabled	Boolean	是否启用CRL发布功能。 • true • false
crl_name	String	吊销列表文件名称。 说明 若用户不指定，系统将默认采用当前证书的父CA ID。
obs_bucket_name	String	OBS桶名称。
valid_days	Integer	CRL更新周期，单位为"天"。当启用CRL发布功能，为必填项。

参数	参数类型	描述
crl_dis_point	String	吊销列表分发地址，即对应的OBS桶中的CRL文件地址。 说明 本参数由程序根据crl_name、obs_bucket_name以及OBS地址进行拼接而成。

状态码：400

表 4-92 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-93 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-94 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-95 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-96 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查询CA详情，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7

响应示例

状态码：200

请求已成功

```
{
  "signature_algorithm": "SHA384",
  "issuer_id": "928bd666-e879-448a-ab54-82f6ae3d81e0",
  "issuer_name": "Huawei IT Root CA",
  "not_after": 1647567892000,
  "not_before": 1645148632000,
  "status": "ACTIVED",
  "freeze_flag": 0,
  "gen_mode": "CSR",
  "serial_number": "202202180143522338893611",
  "distinguished_name": {
    "country": "CN",
    "state": "guangdong",
    "locality": "shenzhen",
    "organization": "Huawei",
    "organizational_unit": "IT",
    "common_name": "Huawei IT Root CA"
  },
  "key_algorithm": "RSA",
  "create_time": 1645148633000,
  "delete_time": null,
  "ca_id": "4c0e772e-a30c-4029-b929-b7acb04143f7",
  "type": "SUBORDINATE",
  "path_length": 0,
  "crl_configuration": {
    "enabled": false,
    "obs_bucket_name": null,
    "valid_days": null,
    "crl_name": null,
    "crl_dis_point": null
  }
}
```

```
}  
}
```

状态码：400

请求参数有误。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：401

被请求的页面需要鉴权。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：403

认证失败。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：404

资源不存在或资源未找到。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：500

服务内部错误。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.5 删除 CA

功能介绍

计划删除CA。计划多少天后删除CA证书，可设置7天~30天内删除。

说明

只有当证书状态为”待激活“或”已禁用“状态时，才可删除。”待激活“状态下，将会立即删除证书，不支持延迟删除。

URI

DELETE /v1/private-certificate-authorities/{ca_id}

表 4-97 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	所要计划删除的CA证书ID。

表 4-98 Query 参数

参数	是否必选	参数类型	描述
pending_days	是	String	延迟删除时间，单位为”天“。

请求参数

表 4-99 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：204

请求已成功，无响应body

状态码：400

表 4-100 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-101 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-102 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-103 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-104 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

计划删除CA，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

```
DELETE https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7?pending_days=7
```

响应示例

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
204	请求已成功，无响应body
400	请求参数有误。
401	被请求的页面需要鉴权。

状态码	描述
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.6 导出 CA 的证书签名请求（CSR）

功能介绍

导出CA的证书签名请求。

 说明

只有当CA处于"待激活"状态时，可导出证书签名请求。

URI

GET /v1/private-certificate-authorities/{ca_id}/csr

表 4-105 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	未激活的从属CA证书ID。

请求参数

表 4-106 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-107 响应 Body 参数

参数	参数类型	描述
csr	String	证书签名请求内容，有以下两种情况： - 通过API请求本接口，证书签名请求中换行符已使用"\r\n"代替； - 通过console端导出证书签名请求，将得到标准的PEM格式的证书签名请求文件。

状态码：400

表 4-108 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-109 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-110 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-111 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-112 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

导出CA的证书签名请求，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

```
GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/csr
```

响应示例

状态码：200

请求已成功

```
{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\r
\nMIIIBUDCB2AIBADBZMRAwDgYDVQQDDAdDU1IsMTIzMQswCQYDVQQGEWJjbjERMA8G\r
\nA1UECAwlc2hhbmdoYWxkETAPBgNVBACmCHNoYW5naGFpMRIwEAYDVQQKDAlzaGFu\r
\nZyxoYWkwZjAQBgcqhkiOPQIBBgUrgQQAlGNiAAQl9M7bK+vys5x9mnfG3783aPRh\r\nP/\r
\nxqLPKVsRsqniC3vPZvlz9E7SasMfZLrXVK37QWhtAEtGNG7NrQnwiOye0/8VZL\r
\nVX7ildM6CZY4SUYSa6TBUxYgJjOs514fjxbuT6gADAKBggqhkiOPQQDAgNnADBk\r\nr\nAjbBQIPXU7TDDDwxrh\r
\n+JfZEYgmr61clQdE5GMozPDYime30zcuMnVrb9i3o/2BW+\r
\n0IECMG0QWbAYh0LoqnmAYqlgTKK8nKsxm0xFuTrfyxynWi8BpCvAGx803Qpa8EJV\r\nr\nJTJcw==\r\n-----\r
\nEND CERTIFICATE REQUEST-----"
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
}
```

```
"error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.7 禁用 CA

功能介绍

禁用CA。

 说明

只有当证书处于"已激活"或"已过期"状态时，可进行禁用操作。

URI

POST /v1/private-certificate-authorities/{ca_id}/disable

表 4-113 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	所要禁用CA证书ID。

请求参数

表 4-114 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：204

请求已成功，无响应body

状态码：400

表 4-115 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-116 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-117 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-118 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-119 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

禁用CA，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/disable

响应示例

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
```

```
"error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
204	请求已成功，无响应body
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.8 启用 CA

功能介绍

启用CA。

说明

注：只有当证书处于“已禁用”状态时，可进行启用操作。

URI

POST /v1/private-certificate-authorities/{ca_id}/enable

表 4-120 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	所要启用的CA证书ID。

请求参数

表 4-121 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：204

请求已成功，无响应body

状态码：400

表 4-122 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-123 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-124 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-125 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-126 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

启用CA，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/enable

响应示例

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

```
"error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
204	请求已成功，无响应body
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.9 导出 CA 证书

功能介绍

导出CA证书。

说明

注：只有当证书处于“已激活”或“已过期”时，可进行导出操作。

URI

POST /v1/private-certificate-authorities/{ca_id}/export

表 4-127 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	所要导出的CA证书ID。

请求参数

表 4-128 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-129 响应 Body 参数

参数	参数类型	描述
certificate	String	证书内容。 说明 - 通过API请求本接口，证书内容中换行符已使用"\r\n"代替； - 通过console端导出证书，将得到标准的PEM格式的证书文件。
certificate_chain	String	证书链内容，证书链中排列顺序（从上至下）：中间证书>...>根证书。 说明 - 通过API请求本接口，证书链内容中换行符已使用"\r\n"代替； - 通过console端导出证书链，将得到标准的PEM格式的证书链文件。

状态码：400

表 4-130 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-131 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-132 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-133 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-134 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。


```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.10 导入 CA 证书

功能介绍

导入CA证书，使用本接口需要满足以下条件：

- （1）证书为“待激活”状态的从属CA；

- （2）导入的证书体必须满足以下条件：
 - a、该证书被签发时的证书签名请求必须是从PCA系统中导出；
 - b、其证书链虽然允许不上传，但后期若想要导出完整的证书链，应导入完整的证书链；
 - c、证书体与证书链必须为PEM编码。

URI

POST /v1/private-certificate-authorities/{ca_id}/import

表 4-135 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	所要导入的CA证书ID。

请求参数

表 4-136 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

表 4-137 请求 Body 参数

参数	是否必选	参数类型	描述
certificate	是	String	证书内容。
certificate_chain	否	String	证书链内容。

响应参数

状态码：204

请求已成功，无响应body

状态码：400

表 4-138 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：401**表 4-139** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-140** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404**表 4-141** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500**表 4-142** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

导入CA证书，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

```
POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/import
{
  "certificate": "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----",
  "certificate_chain": "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----"
}
```

响应示例

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
204	请求已成功，无响应body

状态码	描述
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.11 恢复 CA

功能介绍

恢复CA，将处于“计划删除”状态的CA证书，重新恢复为“已禁用”状态。

说明

注：只有处于“计划删除”状态的CA证书，才可进行恢复操作。

URI

POST /v1/private-certificate-authorities/{ca_id}/restore

表 4-143 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	所需要恢复的CA证书ID。

请求参数

表 4-144 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见： IAM token获取方法 。

响应参数

状态码：204

请求已成功，无响应body

状态码：400**表 4-145** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401**表 4-146** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-147** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404**表 4-148** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500**表 4-149** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

请求示例

恢复CA，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/restore

响应示例

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
204	请求已成功，无响应body
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.1.12 吊销 CA

功能介绍

吊销子CA。

说明

注：当不想填写吊销理由时，请求body请置为 "{}"，否则将会报错。

URI

POST /v1/private-certificate-authorities/{ca_id}/revoke

表 4-150 路径参数

参数	是否必选	参数类型	描述
ca_id	是	String	所要吊销的子CA ID。

请求参数

表 4-151 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见： IAM token获取方法 。

表 4-152 请求 Body 参数

参数	是否必选	参数类型	描述
reason	否	String	吊销理由，支持以下选项： • UNSPECIFIED：吊销时未指定吊销原因，为默认值； • KEY_COMPROMISE：证书密钥材料泄露； • CERTIFICATE_AUTHORITY_COMPROMISE：颁发路径上，可能存在CA密钥材料泄露； • AFFILIATION_CHANGED：证书中的主体或其他信息已经被改变； • SUPERSEDED：此证书已被取代； • CESSATION_OF_OPERATION：此证书或颁发路径中的实体已停止运营； • CERTIFICATE_HOLD：该证书当前不应被视为有效，预计将来可能会生效； • PRIVILEGE_WITHDRAWN：此证书不再具备其声明的属性的权限； • ATTRIBUTE_AUTHORITY_COMPROMISE：担保此证书属性的机构可能已受到损害。 说明 当不想填写吊销理由时，请求body体请置为 "{}"，否则将会报异常，默认值为UNSPECIFIED。

响应参数

状态码：204
请求已成功，无响应body

状态码：400

表 4-153 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：401**表 4-154 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-155 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404**表 4-156 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500**表 4-157 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

吊销子CA，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

```
POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/  
6434f74f-2d13-4e6a-89eb-93ee313f1a43/revoke  
  
{  
  "reason": "KEY_COMPROMISE"  
}
```

响应示例

状态码：400

请求参数有误。

```
{  
  "error_code": "PCA.XXX",  
  "error_msg": "XXX"  
}
```

状态码：401

被请求的页面需要鉴权。

```
{  
  "error_code": "PCA.XXX",  
  "error_msg": "XXX"  
}
```

状态码：403

认证失败。

```
{  
  "error_code": "PCA.XXX",  
  "error_msg": "XXX"  
}
```

状态码：404

资源不存在或资源未找到。

```
{  
  "error_code": "PCA.XXX",  
  "error_msg": "XXX"  
}
```

状态码：500

服务内部错误。

```
{  
  "error_code": "PCA.XXX",  
  "error_msg": "XXX"  
}
```

状态码

状态码	描述
204	请求已成功，无响应body

状态码	描述
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2 私有证书管理

4.2.2.1 查询私有证书列表

功能介绍

查询私有证书列表。

URI

GET /v1/private-certificates

表 4-158 Query 参数

参数	是否必选	参数类型	描述
limit	否	Integer	指定查询返回记录条数，默认值 10。
name	否	String	私有证书名称，返回名称带有 name字段的证书集合。
offset	否	Integer	索引位置，从offset指定的下一条数据开始查询。
status	否	String	私有证书状态，通过状态过滤证书集合。 ● ISSUED：已签发； ● REVOKED：已吊销； ● EXPIRED：已过期。

参数	是否必选	参数类型	描述
sort_key	否	String	排序属性，目前支持以下属性： • create_time：证书创建时间（默认） • common_name：证书名称 • issuer_name：签发CA名称 • not_after：证书到期时间
sort_dir	否	String	排序方向，支持以下值： • DESC：降序（默认） • ASC：升序

请求参数

表 4-159 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见 IAM token获取方法 。

响应参数

状态码：200

表 4-160 响应 Body 参数

参数	参数类型	描述
total	Integer	私有证书总数。
certificates	Array of Certificates objects	证书列表，详情请参见 Certificates 字段数据结构说明。

表 4-161 Certificates

参数	参数类型	描述
certificate_id	String	私有证书ID。

参数	参数类型	描述
status	String	证书状态： • ISSUED : 已签发； • EXPIRED : 已过期； • REVOKED : 已吊销。
issuer_id	String	父CA证书ID。
issuer_name	String	父CA证书名称。
key_algorithm	String	密钥算法。
signature_algorithm	String	签名算法。
freeze_flag	Integer	冻结标识： • 0 : 非冻结状态； • 其它值 : 冻结状态，当前预留。
gen_mode	String	证书生成方式： • GENERATE : PCA系统生成； • IMPORT : 外部导入； • CSR : 外部提供CSR，内部CA进行签发，即私钥不在PCA进行托管。
serial_number	String	序列号。
create_time	Long	证书创建时间，格式为时间戳（毫秒级）。
delete_time	Long	证书删除时间，格式为时间戳（毫秒级）。
not_before	Long	证书创建时间，格式为时间戳（毫秒级）。
not_after	Long	证书到期时间，格式为时间戳（毫秒级）。
distinguished_name	DistinguishedName object	证书名称配置，详情请参见 DistinguishedName 字段数据结构说明。

表 4-162 DistinguishedName

参数	参数类型	描述
common_name	String	证书通用名称（CN）。
country	String	国家编码，需符合正则" [A-Za-z]{2} "。

参数	参数类型	描述
state	String	省市名称。
locality	String	地区名称。
organization	String	组织名称。
organizational_unit	String	组织单元名称。

状态码：400**表 4-163** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401**表 4-164** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-165** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-166 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-167 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查询私有证书列表，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates

响应示例

状态码：200

请求已成功

```
{
  "total": 2,
  "certificates": [ {
    "signature_algorithm": "SHA256",
    "issuer_id": "ef5d84d1-4f52-47d2-b1c8-a91a672487a0",
    "issuer_name": "12",
    "not_after": 1665539214000,
    "not_before": 1634295475000,
    "status": "ISSUED",
    "freeze_flag": 0,
    "gen_mode": "GENERATE",
    "serial_number": "202110151057541266081861",
    "distinguished_name": {
      "country": "cn",
      "state": "guizhou",
      "locality": "guiyang",
      "organization": "hw",
      "organizational_unit": "IT",
      "common_name": "test.huawei.com"
    },
    "key_algorithm": "RSA4096",
    "create_time": 1634295475000,
    "delete_time": null,
    "certificate_id": "6434f74f-2d13-4e6a-89eb-93ee313f1a43"
  }, {
    "signature_algorithm": "SHA256",
    "issuer_id": "ef5d84d1-4f52-47d2-b1c8-a91a672487a0",
    "issuer_name": "12",
```

```
"not_after" : 1665539214000,
"not_before" : 1634110315000,
"status" : "ISSUED",
"freeze_flag" : 0,
"gen_mode" : "GENERATE",
"serial_number" : "202110130731541908887138",
"distinguished_name" : {
  "country" : "cn",
  "state" : "sichuan",
  "locality" : "chengdu",
  "organization" : "hw",
  "organizational_unit" : "HR",
  "common_name" : "hr.huawei.com"
},
"key_algorithm" : "RSA4096",
"create_time" : 1634110316000,
"delete_time" : null,
"certificate_id" : "1cbb5a52-806b-469c-b182-7446e1851a1c"
}]
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.2 申请证书

功能介绍

申请证书。

URI

POST /v1/private-certificates

请求参数

表 4-168 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

表 4-169 请求 Body 参数

参数	是否必选	参数类型	描述
issuer_id	是	String	父CA证书ID。

参数	是否必选	参数类型	描述
key_algorithm	是	String	密钥算法，可选值如下： ● RSA2048：RSA算法，密钥长度2048位； ● RSA4096：RSA算法，密钥长度4096位； ● EC256：椭圆曲线算法（Elliptic Curve Digital Signature Algorithm (ECDSA)），密钥长度256位； ● EC384：椭圆曲线算法（Elliptic Curve Digital Signature Algorithm (ECDSA)），密钥长度384位。
signature_algorithm	是	String	签名哈希算法，可选值如下： ● SHA256 ● SHA384 ● SHA512
distinguished_name	是	CertDistinguishedName object	证书名称配置，详情请参见 CertDistinguishedName 字段数据结构说明。
validity	是	Validity object	证书有效期，详情请参见 Validity 字段数据结构说明。
key_usages	否	Array of strings	密钥用法，具体标准参见RFC 5280中 4.2.1.3节 。 ● digitalSignature：数字签名； ● nonRepudiation：不可抵赖； ● keyEncipherment：密钥用于加密密钥数据； ● dataEncipherment：用于加密数据； ● keyAgreement：密钥协商； ● keyCertSign：签发证书； ● cRLSign：签发吊销列表； ● encipherOnly：仅用于加密； ● decipherOnly：仅用于解密。

参数	是否必选	参数类型	描述
subject_alternative_names	否	Array of SubjectAlternativeName objects	主体备用名称，详情请参见 SubjectAlternativeName 字段数据结构说明。 array大小：[0,20]。
extended_key_usage	否	ExtendedKeyUsage object	增强型密钥用法，详情请参见 ExtendedKeyUsage 字段数据结构说明。
customized_extension	否	CustomizedExtension object	自定义扩展信息，详情请参见 CustomizedExtension 字段数据结构说明。

表 4-170 CertDistinguishedName

参数	是否必选	参数类型	描述
common_name	是	String	证书通用名称（CN）。
country	否	String	国家编码，需符合正则" [A-Za-z]{2} "。若不传入，则默认继承父CA对应的值。
state	否	String	省市名称。若不传入，则默认继承父CA对应的值。
locality	否	String	地区名称。若不传入，则默认继承父CA对应的值。
organization	否	String	组织名称。若不传入，则默认继承父CA对应的值。
organizational_unit	否	String	组织单元名称。若不传入，则默认继承父CA对应的值。

表 4-171 Validity

参数	是否必选	参数类型	描述
type	是	String	有效期类型，为必填值： YEAR：年（12个月） MONTH：月（统一按31天） DAY：日 HOURL：小时

参数	是否必选	参数类型	描述
value	是	Integer	证书有效期值，与type对应的类型值，换算成年需满足以下规则： - 根CA，有效期小于等于30年； - 从属CA与私有证书，有效期小于等于20年。
start_from	否	Integer	起始时间，为可选值： - 格式为时间戳（毫秒级），如1645146939688代表2022-02-18 09:15:39； - 不早于当前时间5分钟，即start_from > (current_time - 5min)。

表 4-172 SubjectAlternativeName

参数	是否必选	参数类型	描述
type	是	String	备用名称类型，当前仅支持DNS、IP、EMAIL、URI。 DNS IP EMAIL URI
value	是	String	对应备用名称类型的值。 - DNS类型，长度为不超过253； - IP类型，长度不超过39，支持IPV4、IPV6； - EMAIL类型，长度不超过256； - URI类型，长度不超过253。

表 4-173 ExtendedKeyUsage

参数	是否必选	参数类型	描述
server_auth	否	Boolean	服务器身份验证，OID为：1.3.6.1.5.5.7.3.1。 • true • false 说明 服务器证书请启用本增强型密钥用法，默认为false。
client_auth	否	Boolean	客户端身份验证，OID为：1.3.6.1.5.5.7.3.2。 • true • false 说明 客户端证书请启用本增强型密钥用法，默认为false。
code_signing	否	Boolean	代码签名，OID为：1.3.6.1.5.5.7.3.3。 • true • false 说明 签署可下载的可执行代码客户端认证，默认为false。
email_protection	否	Boolean	安全电子邮件，OID为：1.3.6.1.5.5.7.3.4。 • true • false 说明 电子邮件保护，默认为false。
time_stamping	否	Boolean	时间戳，OID为：1.3.6.1.5.5.7.3.8。 • true • false 说明 将一个对象的哈希绑定到一个时间，默认为false。

表 4-174 CustomizedExtension

参数	是否必选	参数类型	描述
object_identifier	否	String	对象标识符。 说明 本参数需要满足ASN1规范的点分十进制符号格式的字符串，如1.3.6.1.4.1.2011.4.99。
value	否	String	自定义属性内容。

响应参数

状态码：200

表 4-175 响应 Body 参数

参数	参数类型	描述
certificate_id	String	当前签发的证书ID。

状态码：400

表 4-176 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-177 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-178 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-179 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-180 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

申请证书，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates

```
{
  "key_algorithm": "RSA2048",
  "distinguished_name": {
    "country": "CN",
    "state": "Sichuan",
    "locality": "Chengdu",
    "organization": "Huawei",
    "organizational_unit": "CloudBU",
    "common_name": "TestCert"
  },
  "subject_alternative_names": [ {
    "type": "IP",
    "value": "156.127.116.38"
  } ],
  "signature_algorithm": "SHA256",
  "validity": {
    "type": "YEAR",
    "value": 3
  },
  "issuer_id": "2cb2878b-6cd1-460d-bd25-afe655159bdc",
}
```

```
"key_usages" : [ "digitalSignature", "nonRepudiation" ]
}
```

响应示例

状态码：200

请求已成功

```
{
  "certificate_id" : "ae9a326a-b61e-4446-854d-cda30ffe31f5"
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。

状态码	描述
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.3 通过 CSR 签发证书

功能介绍

通过CSR签发证书。功能约束如下：

- 1、当前默认参数如下：
 - CA 默认参数：
 - keyUsage**: digitalSignature, keyCertSign, cRLSign, 优先采用CSR中的参数；
 - SignatureHashAlgorithm**: SHA384；
 - PathLength**: 0（可自定义）。
 - 私有证书：
 - keyUsage**: digitalSignature keyAgreement, 优先采用CSR中的参数；
 - SignatureHashAlgorithm**: SHA384；
- 2、当传入的type为INTERMEDIATE_CA时，创建出的从属CA证书，有以下限制：
 - 不占用CA配额。在查询CA列表时，不会返回该证书；
 - 只支持通过以下两个接口获取其信息：
 - GET /v1/private-certificate-authorities/{ca_id} 获取证书详情
 - POST /v1/private-certificate-authorities/{ca_id}/export 导出证书
 - 本接口返回的**certificate_id**即代表从属CA的**ca_id**；
 - 无法用于签发证书，密钥在用户侧。
- 3、当type为ENTITY_CERT时，创建出的私有证书，有以下特点：
 - 占用私有证书配额。在查询私有证书列表时，会返回该证书；
 - 除了导出时不包含密钥信息（密钥在用户端），其余用法与其它私有证书一致。

 说明

注：需要使用“\r\n”或“\n”代替换行符，将CSR转换成一串字符，可参考示例请求。注：目前，证书的组织信息、公钥算法以及公钥内容均来自CSR文件，暂不支持API传入。

URI

POST /v1/private-certificates/csr

请求参数

表 4-181 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

表 4-182 请求 Body 参数

参数	是否必选	参数类型	描述
issuer_id	是	String	父CA证书ID。
csr	是	String	证书签名请求。请使用“\r\n”或“\n”替代证书签名请求中的换行符，若通过console端请求此接口，则无需做符号转换。
validity	是	Validity object	证书有效期，详情请参见 Validity 字段数据结构说明。
type	否	String	证书类型，用于区分从属CA与私有证书。 • ENTITY_CERT：签发私有证书，为缺省值； • INTERMEDIATE_CA：签发从属CA。
path_length	否	Integer	路径长度，仅当签发从属CA时有效。
subject_alternative_names	否	Array of SubjectAlternativeName objects	主体备用名称(本接口预留参数，当前在后端被忽略)，详情请参见 SubjectAlternativeName 字段数据结构说明。

表 4-183 Validity

参数	是否必选	参数类型	描述
type	是	String	有效期类型，为必填值： • YEAR：年（12个月） • MONTH：月（统一按31天） • DAY：日 • HOURL：小时
value	是	Integer	证书有效期值，与type对应的类型值，换算成年需满足以下规则： • 根CA，有效期小于等于30年； • 从属CA与私有证书，有效期小于等于20年。
start_from	否	Integer	起始时间，为可选值： • 格式为时间戳（毫秒级），如1645146939688代表2022-02-18 09:15:39； • 不早于当前时间5分钟，即 $start_from > (current_time - 5min)$。

表 4-184 SubjectAlternativeName

参数	是否必选	参数类型	描述
type	是	String	备用名称类型，当前仅支持DNS、IP、EMAIL、URI。 • DNS • IP • EMAIL • URI
value	是	String	对应备用名称类型的值。 • DNS类型，长度为不超过253； • IP类型，长度不超过39，支持IPV4、IPV6； • EMAIL类型，长度不超过256； • URI类型，长度不超过253。

响应参数

状态码：200

表 4-185 响应 Body 参数

参数	参数类型	描述
certificate_id	String	当前签发的证书ID。

状态码：400

表 4-186 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-187 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-188 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-189 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-190 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

通过CSR签发证书，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

```
POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates/csr
```

```
{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\nMIICyTCCAbECAQAwXjELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB3NpY2hhbW4xEDAO\nBgNVBACTB2NoZW5nZHUxCzAJBgNVBAoTAkhXMQswCQYDVQQLLEwJJVDERMA8GA1UE\nAxAkMldGVzdC5jb20wgGgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCZ4q5z\nFC9x2jESeUW5GB6zS5rVxT0WLTCTv9d1LtWBLsRIinATYTYiP1pNo4/pBq\nHIM3IiUDkc896CJerYINzOljTaV4GjCZvPrxSHU5toJvIdfBsY+gnzbT1ol/y0r\nZNRb+0CY30hrXMDrWjp5dtLGTlr5EFYxIKNOPCkR\n+6BGyJnC9PWSuqwsykFbgMRkcBaNAxa59dRhMF50pvx2Vs929vFrMi+ofDELUOqz\nn1vyjaEA3pn3AGJGXZgrGNbSfz12ixgLEs4cQD21GCIWgnBQ7b1ru2V8lmUfyh0\n+257AgMBAAAgJjAkBgkqhkiG9w0BCQ4xFzAVMBMGA1UdEQQMMAQC\nCHRLc3QuY29tMA0GCSqGSIb3DQEBwUAA4IBAQBKfjZuYsz4s0wb1POIWn41eiAB\nnp53qb63QKWILN9z8dLktcdSL3IPfcfPZpXv++QPtn3LR9rJKBawusk6SPXbvOGgS\n+6eM8kVW2O3gHFgoaMcPYVtiO7ekG6o25qx6+Rj84wbFdmPoiCc8AwrLEBwzYV\nnp1zaprWQu6PxBulkYPa3FLcntDdi7B67r0YtpxVvo1K7vHYFboDvpz7xG57QIFIM\nnwGd1OegariMT3N8gBOzLZc+jqLpxgo4xoNqBHM06DEmKLdWdzU4ljpuGK9had99K\nQra3v1uq2lOm/G92b0uA9Y1t2bMHobTAnuXL0HmY9XcLdzpC3f8h8\n-----END CERTIFICATE REQUEST-----",
  "validity" : {
    "type" : "YEAR",
    "value" : 3
  },
  "issuer_id" : "2cb2878b-6cd1-460d-bd25-afe655159bdc"
}
```

响应示例

状态码：200

请求已成功

```
{
  "certificate_id" : "e3e10fc6-5dff-4a70-9cb5-320d258a6215"
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.4 解析 CSR

功能介绍

解析CSR。

URI

POST /v1/private-certificates/csr/parse

请求参数

表 4-191 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

表 4-192 请求 Body 参数

参数	是否必选	参数类型	描述
csr	是	String	证书签名请求。请使用“\r\n”或“\n”替代证书签名请求中的换行符，若通过console端请求此接口，则无需做符号转换。

响应参数

状态码：200

表 4-193 响应 Body 参数

参数	参数类型	描述
key_algorithm	String	密钥算法。
key_algorithm_length	String	密钥算法长度，单位为bit。
signature_algorithm	String	签名算法，带具体的签名与哈希算法，如"SHA256withRSA"。

参数	参数类型	描述
public_key	String	公钥内容。 说明 其中，换行符已被“\r\n”替代；
distinguished_name	DistinguishedName object	证书名称配置，详情请参见 DistinguishedName 字段数据结构说明。

表 4-194 DistinguishedName

参数	参数类型	描述
common_name	String	证书通用名称（CN）。
country	String	国家编码，需符合正则"[A-Za-z]{2}"。
state	String	省市名称。
locality	String	地区名称。
organization	String	组织名称。
organizational_unit	String	组织单元名称。

状态码：400

表 4-195 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-196 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-197 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-198 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-199 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

解析CSR，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates/csr/parse

```
{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\n
MIICyTCCABECAQAwXjELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB3NpY2hhbW4xEDAO\n
BgNVBACTB2NoZW5nZHUxCzAJBgNVBAoTAkhXMQswCQYDVQQLLEwJJVDERMA8GA1UE\n
AxMldGVzdC5jb20wggiEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIABQCCz4q5z\n
FC9x2jESeUW5GB6zS5rVxT0WLTCTv9d1LtWBLsRiinATYTYiP1pNo4/pBq\n
/nHlM3liUDkc896CJerYINzOljTaV4GjCZvPrxSHU5toJvDfLBSY+gnzbT1ol/y0r\n
ZNRb+0CY30hrXMDrWjp5dtLTlR5EFYxlKNOPCkR\n
+6BGylNc9PWSuqwsykFbgMRkcBaNAxa59dRhMF50pvx2Vs929vFrMi+ofDELUOqz\n
\n1vyjaEA3pn3AGJGXZgrGNbSfz12ixgGLes4cQD21GCIAGnBQ7b1ru2V8ImUfyh0\n
+257AgMBAAGgJjAkBgqhkiG9w0BCQ4xFzAVMBMGAlUEEQMMMAQC\n
\nCHRlc3QuY29tMA0GCSqGSIb3DQEBCwUAA4IBAQBKfjZuYsz4s0wb1POIWn41eiAB\n
\np53qb63QKWILN9z8dLktcdSL3lPfcfPZpXv++QPtN3LR9rjKBawusk6SPXbvOGgS\n
+6eM8kVW2O3gHFgoaMcPYvtiO7ekG6o25qx6+Rj84wbFdmPoiCc8AwrLEBwzYV\n
\np1zapRWQu6PxBulkYPa3FLcntDdi7B67r0YtpxVvo1K7vHYFboDvPz7xG57QIFIM\n
\nnwGd1OegariMT3N8gBOzLZc+jqLpxgo4xoNqBHM06DEmKLDWdzU4lpuGK9had99k\n
Qra3v1uq2lOm/G92b0uA9Y1t2bMHobTAnuXL0HmY9XcldzpC3f8h8\n
-----END CERTIFICATE REQUEST-----"
```

响应示例

状态码：200

请求已成功

```
{
  "distinguished_name": {
    "country": "CN",
    "state": "sichuan",
    "locality": "chengdu",
    "organization": "HW",
    "organizational_unit": "IT",
    "common_name": "test.com"
  },
  "public_key": "-----BEGIN PUBLIC KEY-----\r
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx1EX1JfOXquoFDjVi67T\r
\npF4kFwetNnLwC0ZQtOK3fftX4/rkHwdGdsYAalzLz2ltlgbtLJHeKaNnjlqTL8bn\r
\n0DVIxww6ZP6VaxpfKXaj76GxDdvb5kp8yRFUAK8N2YQ0UIcsFoXn2CAx1dOtAaNF\r
\nO+HwooRnp6GekZaRSYS2bk4olkQ83/2WkkTGC+tAmjSFG7AIY8jaO5RgX40YGANh\r
\nU9UGOo8xCxux8k2dsXRnY+fxRiLWphiT2ij4CYURagETbKuRl9WOI+HFVkmIU/Op\r
\nn3FWqB0RdrRTEcAC+S5fmW75E85rAMh9f65wa/6eWcM6vlnby4Bbm1mcJdR3olgKJ\r
\nnUQIDAQAAB\r
\n-----END PUBLIC KEY-----\r
\n",
  "key_algorithm": "RSA",
  "key_algorithm_length": 2048,
  "signature_algorithm": "SHA256withRSA"
}
```

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

```
"error_msg": "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.5 查询私有证书配额

功能介绍

查询私有证书配额。

URI

GET /v1/private-certificates/quotas

请求参数

表 4-200 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-201 响应 Body 参数

参数	参数类型	描述
quotas	Quotas object	证书配额，详情请参见 Quotas 字段数据结构说明。

表 4-202 Quotas

参数	参数类型	描述
resources	Array of Resources objects	资源配额列表，详情请参见 Resources 字段数据结构说明。

表 4-203 Resources

参数	参数类型	描述
type	String	证书类型: • CERTIFICATE_AUTHORITY: CA证书; • CERTIFICATE: 私有证书。
used	Integer	已使用配额数。
quota	Integer	配额总数: • CERTIFICATE_AUTHORITY: 当前系统指定100; • CERTIFICATE: 当前系统指定100000。

状态码：400

表 4-204 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-205 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-206 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-207 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-208 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查询私有证书配额，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

```
GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates/quotas
```

响应示例

状态码：200

请求已成功

```
{
  "quotas": {
    "resources": [ {
      "type": "CERTIFICATE",
      "used": 25,
      "quota": 100000
    } ]
  }
}
```

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。

状态码	描述
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.6 查询证书详情

功能介绍

查询证书详情。

URI

GET /v1/private-certificates/{certificate_id}

表 4-209 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	需要查询的私有证书ID。

请求参数

表 4-210 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-211 响应 Body 参数

参数	参数类型	描述
certificate_id	String	私有证书ID。

参数	参数类型	描述
status	String	证书状态： ● ISSUED : 已签发； ● EXPIRED : 已过期； ● REVOKED : 已吊销。
issuer_id	String	父CA证书ID。
issuer_name	String	父CA证书名称。
key_algorithm	String	密钥算法。
signature_algorithm	String	签名算法。
freeze_flag	Integer	冻结标识： ● 0 : 非冻结状态； ● 其它值 : 冻结状态，当前预留。
gen_mode	String	证书生成方式： ● GENERATE : PCA系统生成； ● IMPORT : 外部导入； ● CSR : 外部提供CSR，内部CA进行签发，即私钥不在PCA进行托管。
serial_number	String	序列号。
create_time	Long	证书创建时间，格式为时间戳（毫秒级）。
delete_time	Long	证书删除时间，格式为时间戳（毫秒级）。
not_before	Long	证书创建时间，格式为时间戳（毫秒级）。
not_after	Long	证书到期时间，格式为时间戳（毫秒级）。
distinguished_name	DistinguishedName object	证书名称配置，详情请参见 DistinguishedName 字段数据结构说明。

表 4-212 DistinguishedName

参数	参数类型	描述
common_name	String	证书通用名称（CN）。
country	String	国家编码，需符合正则" [A-Za-z]{2} "。

参数	参数类型	描述
state	String	省市名称。
locality	String	地区名称。
organization	String	组织名称。
organizational_unit	String	组织单元名称。

状态码：400**表 4-213** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401**表 4-214** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-215** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-216 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-217 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查询证书详情，请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限。

```
GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates/6434f74f-2d13-4e6a-89eb-93ee313f1a43
```

响应示例

状态码：200

请求已成功

```
{
  "signature_algorithm": "SHA256",
  "issuer_id": "ef5d84d1-4f52-47d2-b1c8-a91a672487a0",
  "issuer_name": "HW CA",
  "not_after": 1665539214000,
  "not_before": 1634295475000,
  "status": "ISSUED",
  "freeze_flag": 0,
  "gen_mode": "GENERATE",
  "serial_number": "202110151057541266081861",
  "distinguished_name": {
    "country": "cn",
    "state": "guizhou",
    "locality": "guiyang",
    "organization": "hw",
    "organizational_unit": "IT",
    "common_name": "test.huawei.com"
  },
  "key_algorithm": "RSA4096",
  "create_time": 1634295475000,
  "delete_time": null,
  "certificate_id": "6434f74f-2d13-4e6a-89eb-93ee313f1a43"
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.7 删除证书

功能介绍

删除证书。

URI

DELETE /v1/private-certificates/{certificate_id}

表 4-218 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	所要删除的私有证书ID。

请求参数

表 4-219 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：204

请求已成功，无响应body

状态码：400

表 4-220 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-221 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-222 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-223 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-224 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

删除证书，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

```
DELETE https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates/  
6434f74f-2d13-4e6a-89eb-93ee313f1a43
```

响应示例

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
204	请求已成功，无响应body
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.8 导出证书

功能介绍

导出证书。

- 选择是否压缩时，分以下两种情况：
 - is_compressed为true时，返回文件压缩包，命名为：证书名称_type字段小写字母.zip，如“test_apache.zip”。
 - type = "APACHE"时，压缩包中包含三个文件：**server.key**（密钥文件，内容为PEM格式）、**chain.crt**（证书链，内容为PEM格式）、**server.crt**（证书，内容为PEM格式）；
 - type = "IIS"时，压缩包中包含两个文件：**keystorePass.txt**（keystore口令）、**server.pfx**（PFX证书，证书与证书链包含在同一个文件）；
 - type = "NGINX"时，压缩包中包含两个文件：**server.key**（密钥文件，内容为PEM格式）、**server.crt**（内容为PEM格式，证书与证书链包含在同一个文件）；
 - type = "TOMCAT"时，压缩包中包含两个文件：**keystorePass.txt**（keystore口令）、**server.jks**（JKX证书，证书与证书链包含在同一个文件）；
 - type = "OTHER"时，压缩包中包含三个文件：**server.key**（密钥文件，内容为PEM格式）、**chain.pem**（证书链）、**server.pem**（证书）。
 - is_compressed为false时，返回json格式，返回的具体参数如下：
 - type = "APACHE"或"NGINX"或"OTHER"时，返回参数如下：
 - **certificate**（证书内容，PEM格式）；
 - **certificate_chain**（证书链，PEM格式）；
 - **private_key**（证书私钥，PEM格式）；
 - type = "IIS"或"TOMCAT"时，暂时未定义。

说明

只有当证书状态为“已签发”时，可进行导出操作。

URI

POST /v1/private-certificates/{certificate_id}/export

表 4-225 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	所要导出的私有证书ID。

请求参数

表 4-226 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

表 4-227 请求 Body 参数

参数	是否必选	参数类型	描述
is_compressed	是	String	是否压缩。 • true • false
type	是	String	根据服务器类型选择下载证书的形式，支持以下五种类型： • APACHE：apache服务器推荐使用此参数； • NGINX：nginx服务器推荐使用此参数； • IIS：windows服务器推荐使用此参数； • TOMCAT：tomcat服务器推荐使用此参数； • OTHER：下载PEM格式证书，推荐使用此参数。

响应参数

状态码：200

表 4-228 响应 Body 参数

参数	参数类型	描述
private_key	String	私钥内容。
certificate	String	证书内容。
certificate_chain	String	证书链内容。

状态码：400

表 4-229 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-230 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-231 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-232 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-233 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

导出证书，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

```
POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates/  
6434f74f-2d13-4e6a-89eb-93ee313f1a43/export
```

```
{  
  "type" : "other",  
  "is_compressed" : false  
}
```

响应示例

状态码：200

请求已成功

```
{  
  "certificate" : "-----BEGIN CERTIFICATE-----\r\n*****\r\n-----END CERTIFICATE-----",  
  "certificate_chain" : "-----BEGIN CERTIFICATE-----\r\n*****\r\n-----END CERTIFICATE-----\r\n-----BEGIN  
CERTIFICATE-----\r\n*****\r\n-----END CERTIFICATE-----",  
  "private_key" : "-----BEGIN RSA PRIVATE KEY-----\r\n*****\r\n-----END RSA PRIVATE KEY-----\r\n"  
}
```

状态码：400

请求参数有误。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：401

被请求的页面需要鉴权。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：403

认证失败。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：404

资源不存在或资源未找到。

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

状态码：500

服务内部错误。

```
{  
  "error_code" : "PCA.XXX",  
}
```

```
"error_msg": "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.2.9 吊销证书

功能介绍

吊销证书。

 说明

注：当不想填写吊销理由时，请求body体请置为"**{}**"，否则将会报错。

URI

POST /v1/private-certificates/{certificate_id}/revoke

表 4-234 路径参数

参数	是否必选	参数类型	描述
certificate_id	是	String	所要吊销的私有证书ID。

请求参数

表 4-235 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

表 4-236 请求 Body 参数

参数	是否必选	参数类型	描述
reason	否	String	吊销理由，支持以下选项： • UNSPECIFIED：吊销时未指定吊销原因，为默认值； • KEY_COMPROMISE：证书密钥材料泄露； • CERTIFICATE_AUTHORITY_COMPROMISE：颁发路径上，可能存在CA密钥材料泄露； • AFFILIATION_CHANGED：证书中的主体或其他信息已经被改变； • SUPERSEDED：此证书已被取代； • CESSATION_OF_OPERATION：此证书或颁发路径中的实体已停止运营； • CERTIFICATE_HOLD：该证书当前不应被视为有效，预计将来可能会生效； • PRIVILEGE_WITHDRAWN：此证书不再具备其声明的属性的权限； • ATTRIBUTE_AUTHORITY_COMPROMISE：担保此证书属性的机构可能已受到损害。 说明 当不想填写吊销理由时，请求body体请置为 "{}"，否则将会报异常，默认值为UNSPECIFIED。

响应参数

状态码：204
请求已成功，无响应body

状态码：400

表 4-237 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：401**表 4-238** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-239** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404**表 4-240** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500**表 4-241** 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

吊销证书，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

```
POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificates/6434f74f-2d13-4e6a-89eb-93ee313f1a43/revoke
{
  "reason": "KEY_COMPROMISE"
}
```

响应示例

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码

状态码	描述
204	请求已成功，无响应body

状态码	描述
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.3 证书吊销处理

4.2.3.1 查看是否具有委托权限

功能介绍

查看是否具有委托权限。

 说明

用户所使用账号token需要具备安全管理员（secu_admin）权限。

URI

GET /v1/private-certificate-authorities/obs/agencies

请求参数

表 4-242 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-243 响应 Body 参数

参数	参数类型	描述
agency_granted	String	OBS当前的授权结果。 • true • false

状态码：400

表 4-244 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-245 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-246 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-247 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-248 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查看PCA是否具有用户的OBS委托权限（用于访问OBS桶，更新吊销列表），请求头中的X-Auth-Token字段需要填写token，且该token需要具有本API的访问权限与安全管理员（secu_admin）权限。

GET https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/obs/agencies

响应示例

状态码：200

请求已成功

```
{
  "agency_granted": "true"
}
```

状态码：400

请求参数有误。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.3.2 创建委托

功能介绍

用户给PCA创建OBS委托授权，用于访问OBS桶，更新吊销列表。

 说明

用户所使用账号token需要具备安全管理员（secu_admin）权限。

URI

POST /v1/private-certificate-authorities/obs/agencies

请求参数

表 4-249 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-250 响应 Body 参数

参数	参数类型	描述
agency_id	String	创建OBS委托，由IAM返回的授权ID。

状态码：400

表 4-251 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401

表 4-252 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403

表 4-253 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。

参数	参数类型	描述
error_msg	String	错误请求返回的错误信息。

状态码：404

表 4-254 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500

表 4-255 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

用户给PCA创建OBS委托授权（用于访问OBS桶，更新吊销列表），请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限与安全管理员（secu_admin）权限。

POST https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/obs/agencies

响应示例

状态码：200

请求已成功

```
{
  "agency_id" : "078ade0fc20010004f8fc0034fad529d"
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

4.2.3.3 查询 OBS 桶列表

功能介绍

查询OBS桶列表。

 说明

只有用户创建了委托授权，方可使用此接口。创建委托授权参见本文档：[证书吊销处理>创建委托](#)。

URI

GET /v1/private-certificate-authorities/obs/buckets

请求参数

表 4-256 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户token，参见: IAM token获取方法 。

响应参数

状态码：200

表 4-257 响应 Body 参数

参数	参数类型	描述
total	Integer	OBS桶总数。
obs_buckets	Array of ObsBuckets objects	OBS桶列表，详情请参见 ObsBuckets 字段数据结构说明。

表 4-258 ObsBuckets

参数	参数类型	描述
bucket_name	String	桶名称。
create_time	Long	创建时间,格式为时间戳（毫秒级）。

状态码：400

表 4-259 响应 Body 参数

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：401**表 4-260 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：403**表 4-261 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：404**表 4-262 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

状态码：500**表 4-263 响应 Body 参数**

参数	参数类型	描述
error_code	String	错误请求返回的错误码。
error_msg	String	错误请求返回的错误信息。

请求示例

查询用户OBS桶列表，请求头中的**X-Auth-Token**字段需要填写token，且该token需要具有本API的访问权限。

GET <https://ccm.ru-moscow-1.hc.sbercloud.ru/v1/private-certificate-authorities/obs/buckets>

响应示例

状态码：200

请求已成功

```
{
  "total" : 2,
  "obs_buckets" : [ {
    "create_time" : 1554867690718,
    "bucket_name" : "admin1"
  }, {
    "create_time" : 1554949519646,
    "bucket_name" : "admin3"
  } ]
}
```

状态码：400

请求参数有误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：401

被请求的页面需要鉴权。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：403

认证失败。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：404

资源不存在或资源未找到。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码：500

服务内部错误。

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

状态码

状态码	描述
200	请求已成功
400	请求参数有误。
401	被请求的页面需要鉴权。
403	认证失败。
404	资源不存在或资源未找到。
500	服务内部错误。

错误码

请参见[错误码](#)。

5 权限和授权项

5.1 权限及授权项说明

如果您需要对您所拥有的云证书管理服务（Cloud Certificate Manager，CCM）进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CCM的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略以API接口为粒度进行权限拆分，授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

说明

如果您要允许或是禁止某个接口的操作权限，请使用策略。

账号具备所有接口的调用权限，如果使用账号下的IAM用户发起API请求时，该IAM用户必须具备调用该接口所需的权限，否则，API请求将调用失败。每个接口所需要的权限，与各个接口所对应的授权项相对应，只有发起请求的用户被授予授权项所对应的策略，该用户才能成功调用该接口。例如，用户要调用接口来查询云服务器列表，那么这个IAM用户被授予的策略中必须包含允许“ecs:servers:list”的授权项，该接口才能调用成功。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。
- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。

 说明

“√”表示支持，“x”表示暂不支持。

5.2 SSL 证书管理

v3 接口的授权信息

权限	对应API接口	授权项（Action）	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）
查询证书列表	GET /v3/scm/certificates	scm:cert:list	-	√	x
获取证书详情	GET /v3/scm/certificates/{certificate_id}	scm:cert:get	-	√	x
删除证书	DELETE /v3/scm/certificates/{certificate_id}	scm:cert:delete	-	√	x
推送证书	POST /v3/scm/certificates/{certificate_id}/push	scm:cert:push	-	√	x
导入证书	POST /v3/scm/certificates/import	scm:cert:upload	-	√	x
导出证书	POST /v3/scm/certificates/{certificate_id}/export	scm:cert:download	-	√	x

5.3 私有证书管理

私有 CA 相关接口的授权信息

权限	对应API接口	授权项（Action）
创建CA	POST /v1/private-certificate-authorities	pca:ca:create

权限	对应API接口	授权项 (Action)
取消计划删除CA	POST /v1/private-certificate-authorities/{ca_id}/restore	pca:ca:restore
查询私有CA详情	GET /v1/private-certificate-authorities/{ca_id}	pca:ca:get
查询私有CA CSR	GET /v1/private-certificate-authorities/{ca_id}/csr	pca:ca:getCsr
查询私有CA配额	GET /v1/private-certificate-authorities/quotas	pca:ca:quota
导出私有CA	POST /v1/private-certificate-authorities/{ca_id}/export	pca:ca:export
删除私有CA	DELETE /v1/private-certificate-authorities/{ca_id}	pca:ca:delete
禁用私有CA	POST /v1/private-certificate-authorities/{ca_id}/disable	pca:ca:disable
启用私有CA	POST /v1/private-certificate-authorities/{ca_id}/enable	pca:ca:enable
激活私有CA	POST /v1/private-certificate-authorities/{ca_id}/activate	pca:ca:active
导入 CA	POST /v1/private-certificate-authorities/{ca_id}/import	pca:ca:import
查询私有CA列表	GET /v1/private-certificate-authorities	pca:ca:list

私有证书相关接口的授权信息

权限	对应API接口	授权项 (Action)
查询私有证书详情	GET /v1/private-certificates/{certificate_id}	pca:cert:get
解析私有证书CSR	POST /v1/private-certificates/csr/parse	pca:cert:parseCsr
导出私有证书	POST /v1/private-certificates/{certificate_id}/export	pca:cert:export
查询私有证书配额	GET /v1/private-certificates/quotas	pca:cert:quota
创建私有证书	POST /v1/private-certificates	pca:ca:issueCert

权限	对应API接口	授权项（ Action ）
删除私有证书	DELETE /v1/private-certificates/{certificate_id}	pca:cert:delete
吊销私有证书	POST /v1/private-certificates/{certificate_id}/revoke	pca:cert:revoke
使用CSR创建私有证书	POST /v1/private-certificates/csr	pca:ca:issueCertThroughCSR
查询私有证书列表	GET /v1/private-certificates	pca:cert:list

A 附录

A.1 状态码

私有证书管理状态码

状态码	编码	状态说明
200	OK	请求已成功。
201	Created	创建类的请求完全成功。
204	NO Content	执行成功，无响应消息体。
400	Bad Request	请求参数有误。
401	Unauthorized	服务端指出客户端所提供的认证信息不正确或非法。
403	Forbidden	服务器已经理解请求，但是拒绝执行它。
404	Not Found	资源不存在，资源未找到。
500	Internal Server Error	服务内部错误。

A.2 错误码

A.2.1 SSL 证书管理错误码

状态码	错误码	错误信息	描述	处理措施
400	SCM.0003	Tenant has no privilege.	租户无法操作不属于自己的证书	请操作自己的证书

状态码	错误码	错误信息	描述	处理措施
400	SCM.0005	Incorrect request parameter.	请求参数错误	请填写正确的请求参数
400	SCM.0006	The uploaded certificate failed to be resolved. Ensure that the uploaded certificate has been issued.	上传证书解析不正确	请上传已签发的证书
400	SCM.0008	Abnormal certificate ID	证书编号异常	请填写正确的证书编号
400	SCM.0009	Failed to upload the certificate because no domain name is bound to the certificate.	证书未绑定域名，上传失败	请传递已绑定域名的证书
400	SCM.0010	This operation is not allowed by the current certificate type or status.	证书类型或当前状态不支持此操作	请传递证书的证书类型或者选择证书状态的证书进行此操作
400	SCM.0011	The max number of free certificates for the current user has been reached, and you cannot continue to purchase free certificates.	当前用户证书数量已经达到最大值,不能继续添加	请不要继续添加证书
400	SCM.0012	The uploaded private key failed to be resolved. Ensure that the certificate has been issued.	上传私钥解析不正确，请确保填写已签发证书	请填写正确的证书私钥

状态码	错误码	错误信息	描述	处理措施
400	SCM.0014	The uploaded certificate does not match the private key.	上传证书和私钥不匹配	请传递正确的证书和私钥
400	SCM.0020	Incorrect certificate ID.	证书ID错误	请传递正确的证书编号
400	SCM.0023	Modify key format error.	修改键错误	请输入不为空的键
400	SCM.0024	Modify value format error.	修改内容错误	请输入不为空的值
400	SCM.0028	Push cert error	证书推送异常	请联系技术支持
400	SCM.0030	Certificates cannot be pushed to this service.	暂不支持的推送服务类型	请填写正确的推送服务
400	SCM.0031	Certificate parsing error.	证书解析异常	请上传正确的证书
400	SCM.0032	Incorrect certificate name.	证书名称错误	请填写正确的证书名称
400	SCM.0039	The updated quota value must be greater than the currently used quota.	更新的配额数值必须大于当前已使用的配额数量	请输入正确的配额数值
400	SCM.0042	Cert has expired.	证书已过期	请不要上传已过期的证书
400	SCM.0044	Permission denied, please obtain {0} permission.	权限不足, 请先获取{0}权限	请先获取权限
400	SCM.0052	Cert effective time error.	证书有效期异常	请输入正确的证书
400	SCM.0059	The certificate private key is empty.	证书私钥为空	请联系客服处理

状态码	错误码	错误信息	描述	处理措施
400	SCM.0061	Region parameter error.	region参数异常	请输入正确的region
400	SCM.0063	Duplicate domain error.	域名重复	请输入不重复的域名
400	SCM.0065	File size exceeds limit.	文件大小超过限制	请输入正确大小的文件
400	SCM.0066	Current domain type not allowed to operate.	证书域名类型不支持当前操作	请联系客服处理
400	SCM.0067	Sans changed.	已有附加域名被修改	请输入正确的附加域名
400	SCM.0068	Unsupported region.	暂不支持推送到该Region	请联系技术支持
400	SCM.0070	Incorrect format of the domain bound to the certificate to be uploaded.	上传证书域名格式错误	请传递正确证书
400	SCM.0072	SCM does not support this status.	SCM暂不支持的操作类型	请联系技术支持
400	SCM.0075	Invalid region id.	无效的region id	请输入合法的region id
400	SCM.0080	Required param cert_info is null or empty.	必填请求参数cert_info为空	请输入非空的证书信息
400	SCM.0081	Required param cert_info is null or empty.	必填请求参数cert_info为空	请输入非空的证书信息
400	SCM.0082	Invalid validity_period, should be 12.	无效参数validity_period, 必须为12	请输入合法的属性
400	SCM.0083	Required param first_name is null or empty.	必填请求参数first_name为空	请输入不为空的属性

状态码	错误码	错误信息	描述	处理措施
400	SCM.0085	Required param phone is null or empty.	必填请求参数 phone 为空	请输入不为空的属性
400	SCM.0086	Required param email is null or empty.	必填请求参数 email 为空	请输入不为空的属性
400	SCM.0095	Run RmsApiController failed.	请求有误，调用接口时报	请联系技术支持
400	SCM.0103	This resource is not exist.	资源不存在	请不要操作不存在的资源
400	SCM.0104	This region is not support.	不支持的 region	请不要操作不支持的 region
400	SCM.0106	The resource domain is not equals the cert.	资源域名与证书域名不匹配	请输入正确的域名
400	SCM.0108	Domain format is invalid.	域名格式非法	请输入正确的域名
400	SCM.0109	Cert chain length must be more than 1.	证书链长度必须大于1	请联系技术支持
400	SCM.0201	Failed to push to ELB.	推送失败，ELB error message:	请联系客服处理
400	SCM.0202	Insufficient ELB permissions	ELB 权限不足	请配置 ELB 权限
400	SCM.0204	ELB does not support this region.	ELB 暂不支持此 region	请选择其他支持的 region
400	SCM.0221	Failed to push to WAF.	推送失败，WAF error message:	请联系客服处理
400	SCM.0222	Insufficient WAF permissions	WAF 权限不足	请配置 WAF 权限

状态码	错误码	错误信息	描述	处理措施
400	SCM.0224	WAF does not support this region.	WAF暂不支持此region	请选择其他支持的region
400	SCM.0225	Insufficient WAF quota.	WAF配额不足	请联系客服处理
400	SCM.0301	Tag is not found.	标签未找到	请联系客服处理
400	SCM.0302	Tag quota is upper limit.	标签配额达到上限	请不要添加标签
400	SCM.0303	Match tag invalid.	标签匹配错误	请添加合法标签
400	SCM.0304	Field action is error.	action字段有误	请联系客服处理
400	SCM.0305	Tag value is invalid.	标签值非法	请输入合法的标签值
400	SCM.0306	Tag key is invalid.	标签键非法	请输入合法的标签键
400	SCM.0309	Tag value length is invalid.	标签值长度非法	请输入长度合法的标签值
400	SCM.0310	Tag key length is invalid.	标签键长度非法	请输入长度合法的标签键
400	SCM.0311	Tag key list is invalid.	标签键列表非法	请输入合法的标签键列表
400	SCM.0312	Tag value list is invalid.	标签值列表非法	请输入合法的标签值列表
400	SCM.0313	Tag list is invalid.	标签列表非法	请输入合法的标签列表
400	SCM.0314	Match resourceId invalid.	匹配错误	请联系客服处理
400	SCM.0318	Tag limit invalid.	标签查询limit参数非法	请输入合法的参数
400	SCM.0319	Tag offset invalid.	标签查询offset参数非法	请输入合法的参数
400	SCM.0321	Invalid param sys_tags.	参数sys_tags错误	请输入合法的参数

状态码	错误码	错误信息	描述	处理措施
400	SCM.0323	Invalid tag parameter.	不合法的标签参数	请输入合法的参数
400	SCM.0501	The parameter cannot be null or the parameter is wrong. Currently only supports:	参数不可为空或者参数错误，目前仅支持：	目前仅支持 WAF/ELB
400	SCM.0502	The certificate ID list cannot be empty.	证书ID列表不可为空	请输入不为空的证书id列表
400	SCM.0505	Parameter error, parameter is null or its list size is out of range, additional info:{0}	参数错误，参数为null或其列表大小超出范围	请输入长度大于0小于51的列表参数
400	SCM.0506	There is no corresponding certificate ID under the tenant, and the set of certificate IDs that cannot be found:{0}	该租户下不存在对应证书ID	请联系技术支持
400	SCM.0507	The list parameter cannot have duplicate elements	该列表参数不可存在重复元素	请输入不重复的参数
400	SCM.0508	Parameter error, the following certificates do not support querying deployed resources:{0}	参数错误，以下证书不支持查询已部署资源	请输入合法的证书
401	SCM.0092	Decrypt jwt token failed.	解密JWT token失败	请联系技术支持

状态码	错误码	错误信息	描述	处理措施
401	SCM.1000	The token of the request fails to be authenticated	请求所带的Token没有经过认证或者认证失败	请填写正确token
401	SCM.1004	Failed to apply for OBT.	用户未申请服务公测，请先申请公测	请申请公测
401	SCM.1009	Your account is restricted.	账户受限	请联系管理员解冻
401	SCM.1010	Your account is frozen.	账户冻结	请联系管理员解冻
401	SCM.4002	You do not have permission to perform this operation.	您的权限不足。缺少策略	请联系管理员添加策略
403	SCM.0001	Service is not open.	服务未开放	请联系技术支持
403	SCM.0002	Incorrect tenant ID.	租户ID错误	请传递正确与X-Auth-Token匹配的projectId
403	SCM.0040	The max number of free certificates for the current user has been reached, and you cannot continue to purchase free certificates.	当前用户免费证书数量已经达到最大值，不能继续购买免费证书	请停止购买免费证书
403	SCM.0322	Invalid user token, user role don't contain op_service.	用户token非法，未包含op_service角色	请联系客服处理
404	SCM.0069	No projects found.	项目不存在	请选择存在的项目
404	SCM.0094	Resource not found.	未找到资源	请联系技术支持

状态码	错误码	错误信息	描述	处理措施
500	SCM.0007	Failed to download the certificate.	证书下载失败	请联系客服处理
500	SCM.0013	The uploaded certificate chain failed to be resolved. Ensure that the certificate has been issued.	上传证书链解析不正确，请确保填写已签发证书	请填写正确的证书链
500	SCM.0017	product wrong.	产品错误	请联系技术支持
500	SCM.0019	CSB response error.	CSB连接失败	请联系技术支持
500	SCM.0037	Failed to encrypt the certificate.	证书加密失败	请联系客服处理
500	SCM.0038	Cert decrypt fail.	证书解密失败	请联系技术支持
500	SCM.0071	SCM does not support this resourceType.	SCM不支持的资源类型	请联系技术支持
500	SCM.0087	Request cert failed.	申请证书失败	请联系技术支持
500	SCM.0091	Connect jwt server failed.	连接到JWT服务器失败	请联系技术支持
500	SCM.0093	Invalid jwt token.	无效的JWT token	请联系技术支持
500	SCM.0097	Encode next token failed.	加密next token失败	请联系技术支持
500	SCM.0098	Decode next token failed.	解密next token失败	请联系技术支持
500	SCM.0099	Invalid domain id.	无效的domain id	请输入合法的domain id
500	SCM.0100	UnKnown error.	未知错误	请联系技术支持
500	SCM.0203	Failed to push to ELB.	ELB推送失败	请联系客服处理

状态码	错误码	错误信息	描述	处理措施
500	SCM.0223	Failed to push to WAF.	WAF推送失败	请联系客服处理
500	SCM.0324	Calculate digest failure.	计算签名失败	请联系技术支持
500	SCM.0402	Encrypt cert content or private key is null.	加密证书内容或私钥为空	请联系技术支持
500	SCM.0504	Service internal error, please contact technical support.	服务内部错误, 请联系技术支持	请联系技术支持
500	SCM.4001	An error occurred when accessing the PDP API.	获取细粒度授权结果失败	请联系客服处理

A.2.2 私有证书管理错误码

状态码	错误码	错误信息	描述	处理措施
400	PCA.00020001	Incorrect parameter.	参数无效。	请确认输入参数是否正确。
400	PCA.00020101	Incorrect certificate distinguished name.	证书唯一性标志名称无效。	请确认参数 distinguished_name 中所有字段是否符合要求。
400	PCA.00020102	Invalid key algorithm. Only RSA2048, RSA4096, EC256, and EC384 are supported.	密钥算法无效, 目前支持 RSA2048、RSA4096、EC256 及 EC384。	请确认密钥算法输入是否正确。

状态码	错误码	错误信息	描述	处理措施
400	PCA.00020103	Invalid signature hash algorithm. Only SHA256, SHA384, and SHA512 are supported.	签名哈希算法无效，目前支持SHA256、SHA384及SHA512。	请确认输入的签名哈希算法是否正确。
400	PCA.00020109	Invalid validity period type or value. Only year, month, or day supported.	有效期类型或范围无效，目前支持类型为年、月、日。	请确认输入的有效期类型及取值是否正确。
400	PCA.00020110	Incorrect domain name.	域名无效。	请确认输入的域名长度在[1,64]范围内，并且符合域名规则。
400	PCA.00020111	Invalid IP. Enter an IPv4 address.	IP无效，目前支持符合IPv4规则的IP。	请确认IP地址符合IPv4规则。
400	PCA.00020112	Invalid alternative name type of the certificate subject. Enter an IP or DNS.	证书主题备用名称的类型无效，目前支持IP及DNS类型。	请确认类型取值为IP或DNS。
400	PCA.00020201	Invalid CA ID. Valid CA IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx format.	CA编号无效，取值需满足正则表达式： [0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}。	请输入正确的CA编号。
400	PCA.00020202	Invalid CA type. Only root CA and subordinate CA are supported.	CA类型无效，取值必须为ROOT或者SUBORDINATE。	请确认输入的CA类型是否正确，CA类型取值必须为ROOT或者SUBORDINATE。

状态码	错误码	错误信息	描述	处理措施
400	PCA.00020203	Invalid CA path length. The value range is [0, 6].	CA路径长度无效，取值范围[0,6]。	请确认输入的CA路径是否正确，CA路径取值范围[0,6]。
400	PCA.00020204	Invalid CRL configuration.	证书吊销列表配置无效。	请检查输入的证书吊销列表配置是否正确，包括OBS桶名称、CRL文件名称及更新周期取值范围[7,30]。
400	PCA.00020301	Invalid certificate ID. Valid certificate IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx format.	证书编号无效，取值需满足正则表达式：[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}。	请输入的正确的证书编号。
400	PCA.00020401	Incorrect certificate signature request.	证书签名请求无效。	请检查证书签名请求是否正确。
400	PCA.00020402	Incorrect certificate. Please contact technical support.	证书无效，请联系技术支持。	请联系技术支持。
400	PCA.00020403	Incorrect certificate chain.	证书链无效。	请确认输入的证书链符合要求： 1、格式要正确，通过API请求时，需要使用“ ”或“\r ”代替换行符； 2、证书链要完整，不能缺少一些中间CA证书，排列顺序为：中间CA>...>根CA。

状态码	错误码	错误信息	描述	处理措施
400	PCA.00020404	Invalid status. The status can only be Pending activation, Activated, Disabled, Pending deletion, or Expired.	状态无效，当前支持状态为待激活、已激活、已禁用、已删除及已过期。	请输入有效的状态值，当前支持的状态值为：待激活（PENDING）、已激活（ACTIVED）、已禁用（DISABLED）、已删除（DELETED）、已过期（EXPIRED）。
401	PCA.00000101	Access Denied. No permissions granted for this OBT.	没有公测权限。	请申请公测权限。
401	PCA.00010001	Incorrect X-Auth-Token in the request header.	请求Header中的X-Auth-Token无效。	请检查： 1、是否按照统一身份认证服务（IAM）提供的接口，获取的token； 2、token是否已过期。 若检查以上条件后仍未解决问题，请联系技术支持。
401	PCA.00010002	Account frozen. Please contact technical support.	账号已被冻结。	请联系技术支持。
401	PCA.00010003	Access denied. Real-name authentication failed or account in arrears.	账号受限，可能原因为账号未认证或者欠费。	请确认账号是否进行实名认证、是否欠费，若仍未解决请联系技术支持。
401	PCA.00010004	Insufficient permissions. Contact administrator.	账号权限不足。	请找账号管理员确认账号权限，若仍未解决请联系技术支持。

状态码	错误码	错误信息	描述	处理措施
403	PCA.00000006	Obtaining OBS buckets failed. Please contact technical support.	服务内部获取对象存储桶错误。	请联系技术支持。
403	PCA.00030001	CA or certificate quantity exceeds quota.	CA或证书数量超出配额限制。	请检查已创建的CA或已申请的证书数量是否达到最大值。如果需要提高额度，请联系技术支持。

状态码	错误码	错误信息	描述	处理措施
403	PCA.00030201	Operation not allowed in the current status.	当前状态不允许执行本操作。	CA或证书在不同状态下所允许执行的操作有限制，请检查操作的条件： 1、禁用CA：CA状态需处于”已激活“或”已过期“状态； 2、启用CA：CA状态需处于”已禁用“状态； 3、删除CA：CA状态需处于“待激活“或”已禁用“状态； 4、恢复CA：CA状态需要处于“已删除”状态； 5、导出CA的CSR：CA状态需要处于”待激活“状态； 6、导出CA证书：CA状态需要处于”已激活“或”已过期“状态； 7、激活CA：CA状态需要处于“待激活”状态； 8、申请证书：签发CA状态需要处于“已激活”状态； 9、导出证书：证书状态需要处于“已签发”状态； 若检查操作条件后仍未解决问题，请联系技术支持。
403	PCA.00030202	CA or certificate frozen. Contact administrator.	对象已被冻结，除了查看外不允许其他操作。	请联系技术支持。

状态码	错误码	错误信息	描述	处理措施
403	PCA.00030301	Certificate public key and private key does not match.	证书的公钥与私钥不匹配。	如果导入CA证书时出现本错误提示，请检查生成证书的CSR是否是从该CA导出的CSR。
404	PCA.00030102	CA or certificate is not found.	CA或证书不存在。	请确认CA或证书已经存在。
404	PCA.00030103	Issuer CA is not found	签发CA不存在，无法签发证书。	请确认指定的签发CA已经创建并且状态为“已激活”状态。
500	PCA.00000001	Unknown error. Please contact technical support.	服务内部当前未识别的错误。	请联系技术支持。
500	PCA.00000002	Parameter processing failed. Please contact technical support.	服务内部参数处理错误。	请联系技术支持。
500	PCA.00000003	Certificate processing failed. Please contact technical support.	服务内部证书处理错误。	请联系技术支持。
500	PCA.00000004	Key processing failed. Please contact technical support.	服务内部密钥处理错误。	请联系技术支持。
500	PCA.00000005	Authentication failed. Please contact technical support.	服务内部鉴权处理错误。	请联系技术支持。

A.3 获取项目 ID

调用 API 获取项目 ID

项目ID可以通过调用IAM服务的“查询指定条件下的项目信息”API获取。

获取项目ID的接口为“GET https://{Endpoint}/v3/projects”，其中{Endpoint}为IAM的终端节点，可以从[地区和终端节点](#)获取。接口的认证鉴权请参见[认证鉴权](#)。

响应示例如下，其中projects下的“id”即为项目ID。

```
{
  "projects": [
    {
      "domain_id": "65382450e8f64ac0870cd180d14e684b",
      "is_domain": false,
      "parent_id": "65382450e8f64ac0870cd180d14e684b",
      "name": "xxxxxxx",
      "description": "",
      "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
      },
      "id": "a4a5d4098fb4474fa22cd05f897d6b99",
      "enabled": true
    }
  ],
  "links": {
    "next": null,
    "previous": null,
    "self": "https://www.example.com/v3/projects"
  }
}
```

从控制台获取项目 ID

在调用接口的时候，部分URL中需要填入项目编号，所以需要获取到项目编号。项目编号获取步骤如下：

1. 登录管理控制台。
2. 单击用户名，在下拉列表中单击“我的凭证”。
在“我的凭证”页面的项目列表中查看项目ID。

B 修订记录

发布日期	修改说明
2025-10-30	第一次正式发布。