沃通电子认证服务有限公司

PDF 数字证书申请 API 接口说明书

文档版本　V1.0.6

发布日期　2021 年 09 月 22 日

目 录

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本	发布日期	说明
V1.0	2020/05/13	文档首次发布。
V1.01	2020/05/22	添加 Order Status 名词解释， 添加 pendingRevoke 状态 证书月份添加 13，25 两个值，保证客户续期不减少月份
V1.02	2020/05/25	删除创建单位，删除根据单位 ID 创建订单 创建订单的接口参数名称修改，保持 一词一义 SN => Hosts Csr => Csr_Sign ProductType => ProductID BindRSAProductType => BindRSAProductID 此 csr 改动目的: csr 是什么类型，就对应相应的参数 增加 RSA 证书域名验证查询 API RSA 域名验证增加 delayQuery 延迟查询参数，详细请参考其解释
V1.03	2020/06/02	RSA Order 状态添加 pendingSubmitOrderToCA pendingDCV pendingCAIssued RSA OVSSL,RSA EVSSL 正常流程如下: 1.调用下单接口后 status=pendingSubmitOrderToCA 2.沃通法务审核通过后 status=pendingDCV 3.调用 RSADCV 验证通过后 status=pendingCAIssued 》这里 comodo 会电话客户，进行验证单位身份 4.调用取证书接口，如果可以取到证书 status=issued

版权所有 © 沃通电子认证服务有限公司

文档版本	发布日期	说明
		RSA DV SSL: 1.调用下单接口后 status=pendingSubmitOrderToCA >后台程序自动提交 status =pendingDCV 2.调用 RSADCV 验证通过后 status=pendingCAIssued 3.调用取证书接口，如果可以取到证书 status=issued
V1.04	2020/06/11	重新颁发后，老订单的状态做了补充 推送添加了签名，可进行验证是否由我们系统发出的推送请求
V1.05	2020/09/11	吊销推送 重新颁发可传入一个 idempotenceID 保持一致，方便对账 每次请求可带上一个 header “RequestID:xxxxxxx”，方便日志定位
V1.06	2021/09/22	增加 RSA 查询域名验证值接口 详见 第 5 节 RSA 获取验证域名验证值 接口
V1.07	2021/10/18	Sectigo 证书的域名验证值中 以前的 comodoca.com 更换为 sectigo.com
V1.08	2021/11/2	增加通知用户证书已签发接口 详见 接口 15
V1.09	2022/11/1	增加单位文档签名证书和个人文档签名证书产品

版权所有 © 沃通电子认证服务有限公司

1. 概述

1.1 API 的作用

WoTrus API 接口主要适用于代理商合作伙伴申请 SSL 证书和管理 SSL 证书订单，代理商的业务系统或应用程序中集成 WoTrus API，无需登录沃通官网，即可实现 SSL 证书下单、证书注销、证书查询等操作。

代理商对接 WoTrus API，可以实现代理商合作伙伴的系统自动下单到我司系统，从而保证两个系统之间的订单信息一致，同时也提高代理商下单效率。

1.2 申请条件

1. 用户需在沃通官网完成注册方可调用(https://buy.wosign.com)，后台客服会将您的账号设置为代理商。
2. 请求 API 之前必须先获取 API token，配置身份认证结果推送。
   登录 https://partner.wosign.com，单击“API 配置”页面设置。
3. 发起 https 请求时须带上一个 header: WoTrusToken: your api token，如果不带该请求头或该请求头错误，将返回一个 401 http 错误状态码.

1.3 接口目标

接口功能达到以下目标：

1. 接口简单便于操作，并能够兼容接口以后扩充。
2. 提供对外开放性，能够具备认证功能，保证系统的安全性。
3. 接口标准对外可靠高效。
4. 提供解决故障手段和流程机制，快速高效定位故障和解决方法。

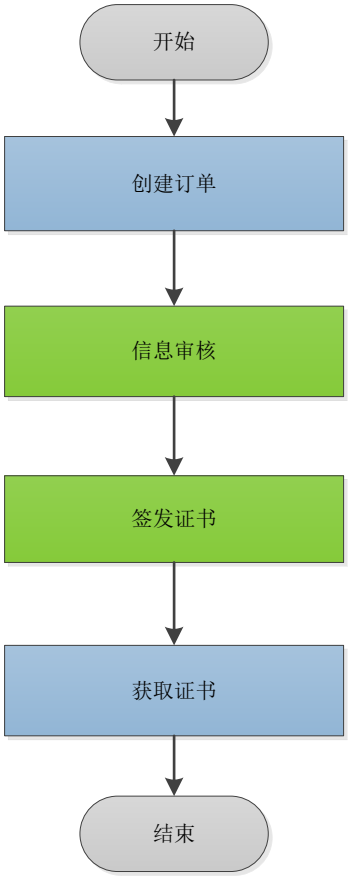
1.4 数据交互

此接口只支持 HTTPS 数据传输请求，调用 API 使用 Post 方式传递数据，“content-type”的格式为：“application/json”。

版权所有 © 沃通电子认证服务有限公司

1.5 接口流程

云厂商通过 API 证书下单的流程如下图所示。



流程说明：

1. 云厂商调用 API 下单，申请证书
2. **WoTrus** 团队对厂商身份、用户信息、域名验证、身份审核等操作，并完成后签发证书。
3. 云厂商调用取证书 API，下载证书。

1.6 注意事项

1. 接口地址：https://restapi.wosign.com
2. 接口认证 添加一个 header WoTrusToken tk_xxxxx?????
3. POST 接口需要添加另一个 header Content-Type application/json

版权所有 © 沃通电子认证服务有限公司

2. 创建订单

功能描述

创建订单接口支持 sm2 下单,rsa 下单，和证书续期

请求方式

POST 请求

环境地址

https://restapi.wosign.com/v1/Order/Create

请求参数

OrderInfo

参数标识	参数名称	说明
productID	产品类型	**必选参数。 Pdf 证书固定值如下** 76ECE651-B59E-48F2-A47B-135614AADAD9 PDF 签名和加密证书 2C17C336-A772-42F8-B3DD-4F2591A5B116 单位文档签名证书 D4D30B75-68D5-471C-B66A-21299F1DFAA5 个人文档签名证书
commonName	证书主题 CN 字段	**必选参数。** **一般填单位名字**
csr_RSA	RSA 证书的 CSR	RSA 证书的 CSR，ECC 证书的 CSR
uKeyPassword	PDF 证书的 UKey 密码	可选参数。
uKeyShipAddress	PDF 证书的 Ukey 邮寄地址	可选参数。
month	月份	必选参数。取值范围： 12：表示申请证书的有效期是 12 个月。 24：表示申请证书的有效期是 24 个月。

版权所有 © 沃通电子认证服务有限公司

参数标识	参数名称	说明
		13：表示申请证书的有效期是 13 个月。常用于续期 补客户老证书的剩余时间 25：表示申请证书的有效期是 25 个月。常用于续期 补客户老证书的剩余时间
idempotenceID	幂等值	幂等值保证两边系统订单数量一致，一般传调用者数据库的 ID。

OrgInfo

参数标识	参数名称	说明
orgName	单位名称	**必选参数**。
businessCategory	单位类型	可选参数。 取值范围：(取英文字符串) ● Business Entity：个体 ● Private Organization：企业 ● Government Entity：政府事业单位 ● Non-Commercial Entity：非商业机构/协会
orgPhone	单位电话	可选参数。
orgEmail	单位邮箱地址	可选参数。
userFirstName	申请人名	可选参数。
userLastName	申请人姓	可选参数。
userEmail	申请人邮箱地址	可选参数。
userMobile	申请人手机号	可选参数。
idCardNO	申请人身份证号码	可选参数。
countryCode	国家代码	两个字符的英文，如:CN,US,JP,RU… 中国:CN 美国:US 日本:JP

版权所有 © 沃通电子认证服务有限公司

参数标识	参数名称	说明
		…
state	单位所在省份	可选参数。
city	单位所在城市	可选参数。
street	单位所在地址	可选参数。
zip	单位地址对应的邮编	可选参数。
businessLicense	统一社会信用代码	可选参数。
otherName	公司其他名字	可选参数。

参数标识	参数名称	说明
documentType	材料类型	1. 授权书 2. 营业执照 3. 身份证
fileType	文档的后缀名	.jpg .gif .pdf
fileContent	文档的 base64 编码	

请求示例


```
{
  "orderinfoPost": {
    "productID": "76ECE651-B59E-48F2-A47B-135614AADAD9",
    "commonName": "沃通电子认证服务有限公司",
    "csR_RSA": "-----BEGIN CERTIFICATE REQUEST-----
MIIDhzCCAm8CAQAwJzEJMAcGA1UECgwAMRowGAYDVQQDDBFmeXQuYW1hemluZ2Jv
eS5jbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMCEbQtd7P/FfzxA
Qs/kunglD8yVMN1cib56KyKOmjdAobHZrpRH4EnpS0wNahwX/+LeyAqydAmVp7+0
/4xf9AHN3GAA44EBu29QX6BdXw5UkLi37Ov0HOC+/2TS736eOgFOcsf90V4QA9b6
pZjFlGEhNjxqOznN7uaIIrOonAaSYuqCqTkB0gpu6pV/b314TBj4GuEyKcoFm8KM
Qu88Hm1gGff8B5GmG9kR4BKoGPi/FBazmbkUmXPbfu0uljGLDg5zpcQpOuAjzXKY
```


版权所有 © 沃通电子认证服务有限公司

```
eYLLVWSHnYB4xiiUnzGuuMaF5d67BaFyT7EwNADgLD9SOr6hjmqyVZjtYyk6b7Dm
DMrt+CECAwEAAaCCARkwGgYKKwYBBAGCNw0CAzEMFgo2LjIuOTIwMC4yMD4GCSqG
SIb3DQEJDjExMC8wHQYDVR0OBBYEFBnGOl3vNU7DVTwoAS6rtZszrF8oMA4GA1Ud
DwEB/wQEAwIFIDBFBgkrBgEEAYI3FRQxODA2AgEFDBtERVNLVE9QLVpXSi5jb3Jw
Lndvc2lnbi5jb20MCUNPUlBcY21zNgwJdG9vbHMuZXhlMHQGCisGAQQBgjcNAgIx
ZjBkAgEBHlwATQBpAGMAcgBvAHMAbwBmAHQAIABFAG4AaABhAG4AYwBlAGQAIABD
AHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByACAAdgAx
AC4AMAMBADANBgkqhkiG9w0BAQUFAAOCAQEAtNCFnM54Bes/SWhhADJFqKhsK6ld
ubP2IUaA0czGKBu8Z8hut/Oe5I0WYnuH/dbz1hGvqghDYFiYpq7G1dJCseUa0h97
jvMTEC6XCTOSjw+rnh9FUu/KEnJ1YTwuwD/SeevrqQJnOlqkMlSEpFzvmmyFFuEc
d95SaFq2o52NZ3cXvGjCzgvFCJUfs/OLzCQToJcr2TjDnnkXjefbuC21c+pTJ/YR
/AP2Ez2g1tVqK3UcYFzbrsAtNKRkfN3xVuLjO2tsy9vCjiCASffEMegoH3qLCZZf
0eayPh7fv5daQQWcF6RxH3FXfIT9d0RhTXUeStwyOtL86UWGJ/09eHYBtQ==
-----END CERTIFICATE REQUEST-----",
    "month": 12,
    "idempotenceID": ""
  },
  "organizationPost":{
    "OrgName":"刘大强",
    "BusinessCategory":"",
    "OrgPhone":"18610077459",
    "OrgEmail":"ldq@wotrus.com",
    "UserFirstName":"大强",
    "UserLastName":"刘",
    "UserEmail":"ldq@wotrus.com ",
    "UserMobile":"18610077459",
    "IDCardNO":"",
    "countryCode": "CN",
    "state": "",
    "city": "",
    "street": "",
    "zip": "",
    "businessLicense": "",
    "OtherName":null
},
  "documentsPost": [

  ]
```


 版权所有 © 沃通电子认证服务有限公司

```
}
```

响应参数

参数标识	参数名称	说明
isSuccess	结果标识	取值范围： ● true：请求成功。 ● false：请求失败。
errorMsg	创建失败描述	仅当创建订单失败时，该参数返回值不为空。
successMsg	创建成功描述	仅当创建订单成功时，该参数返回值不为空。
orderID	SM2 证书订单 ID	SM2 证书的订单 ID。
orderID_RSA	RSA 证书订单 ID	SM2 搭配的 RSA 证书订单 ID。
page	统计参数	统计参数。

响应示例

```
{
    "isSuccess": true,
    "errorMsg": "string",
    "successMsg": "string",
    "data": {
        "orderID": "644A3E60-F1AA-4E25-821A-ACFBC462BC37",
        "orderID_RSA": "89CB4BF6-3E53-4B49-9AB9-92D578144260"
    },
    "page": {
        "total": 0,
        "limit": 0,
        "skip": 0
    }
}
```


版权所有 © 沃通电子认证服务有限公司

3. 查询订单

功能描述

通过订单 ID 查询订单的信息。订单 ID 在创建订单成功后由接口返回给调用方。

请求方式

GET 请求。

环境地址

https://restapi.wosign.com/v1/Order/{订单 id}

请求参数

以订单 id 作为查询条件。

请求示例

无。

响应参数

查询订单的响应参数大部分为创建订单的请求参数，这里不再重复列举，详细参数请参见响应示例。响应参数中的关键参数说明如下表所示。

参数标识	参数名称	说明
id	订单 ID	订单 ID 由创建订单成功后，接口返回给接口调用方。
Status	订单状态	取值范围： ● pendingAutoIssue; 不需要人工审核完成域名验证，自动签发 ● closed; 订单已关闭 ● revoked; 订单已吊销 ● rejected; 订单已被拒绝 ● pending; 等待人工审核 ● pendingRevoke 等待人工审核吊销 ● issued; 订单已签发 ● unknown; 未知的情况 ● pendingSubmitOrderToCA 订单在沃通审核 ● pendingDCV 订单等待做域名验证

版权所有 © 沃通电子认证服务有限公司

参数标识	参数名称	说明
		● pendingCAIssued 订单等待 CA 签发
isPay	支付状态	取值范围： ● 0：未支付 ● 1：已支付 ● 2：先签发后支付，但还未支付
pendingLink	待操作链接	该链接用于提供用户直接在沃通系统上进行域名验证、上传证明材料、递交 CSR 等操作。API 对接方，无须关心证书中间繁琐的流程步骤，无须集成域名验证接口，类似于 SaaS。

响应示例


```
{
    "isSuccess": true,
    "errorMsg": null,
    "successMsg": "success",
    "data": {
        "id": "a4a78326-0546-4602-9586-8ee3c05e8068",
        "productName": "超快 SSL V1",
        "productID": "30B3F256-9D2D-43C5-ABCB-017AA9D3CB6D",
        "cn": "fyt.amazingboy.cn",
        "sn": "fyt.amazingboy.cn",
        "org": {
            "id": "31cd6419-0fc2-4273-8f7f-5193d4900423",
            "orgName": "xxxx 有限公司",
            "orgPhone": "",
            "orgEmail": "",
            "userFirstName": null,
            "userLastName": null,
            "userEmail": null,
            "userMobile": null,
            "idCardNumber": null,
            "isUpload": false,
            "status": "pending"
        },
```


 版权所有 © 沃通电子认证服务有限公司

```
        "orderNumber": "200331142742552",
        "duration": 12,
        "durationType": 0,
        "createTime": "2020-03-31T14:27:42.286+08:00",
        "serverCount": 1,
        "includeRSA": true,
        "isUploadedPic": true,
        "isSNVerified": false,
        "isCSRSubmited": true,
        "isCustomerInfoFilled": true,
        "status": "pendingAutoIssue",
        "isPay": 1,
        "pendingLink":
"https://buy.wosign.com/ProductV4/OrderSuccess/4798ED51DBOE5M79BBAC5F86A7A122B18
B59D8ECDF6E8F063C9245F413611759B4BE76CCEAF11390A10A43F.html"
    },
    "page": null
}
```

4. 获取证书

功能描述

证书签发后，调用此接口将返回证书文件。

请求方式

GET 请求。

环境地址

https://restapi.wosign.com/v1/Certificate/RetrievePem

请求参数

以订单 id（orderID）作为查询条件。

请求示例

```
https://restapi.wosign.com/v1/Certificate/RetrievePem?orderID=644A3E60-F1AA-4E25-821A-ACFBC462BC37
```

响应参数

参数标识	参数名称	说明
isSuccess	结果标识	取值范围： true：请求成功。 false：请求失败。
errorMsg	失败描述	仅当请求失败时，该参数返回值不为空。
successMsg	成功描述	仅当请求成功时，该参数返回值不为空。
pem_RSA pem_Sign pem_Encrypt	证书公钥	对应类型证书的公钥
chains_RSA chains_Sign chains_Encrypt	根公钥	Chains 数组中的第一项为顶级根，最后一项为中级根。
result	结果标识	结果标识。取值范围： true：成功 false：失败

版权所有 © 沃通电子认证服务有限公司

参数标识	参数名称	说明
page	统计参数	统计参数。

响应示例

```
{
    "isSuccess": true,
    "errorMsg": "",
    "successMsg": "",
    "data": {
        "pem_RSA": "---begin xxxxx ---end---",
        "chains_RSA": ["root 公钥", "cross 公钥", "中级根公钥"],
        "pem_Sign": "---begin xxxxx ---end---",
        "chains_Sign": ["root 公钥", "cross 公钥", "中级根公钥"],
        "pem_Encrypt": "---begin xxxxx ---end---",
        "chains_Encrypt": ["root 公钥", "cross 公钥", "中级根公钥"]
    },
    "page": {
        "total": 0,
        "limit": 0,
        "skip": 0
    }
}
```


版权所有 © 沃通电子认证服务有限公司

5. 取消订单

功能描述

该接口用于取消证书订单。如果证书已签发或吊销，则不能进行取消订单操作。

请求方式

POST 请求

环境地址

https://restapi.wosign.com/v1/Order/Cancel

请求参数

参数标识	参数名称	说明
orderID	订单 ID	需要取消订单的 ID。
reason	取消原因	用于描述取消订单的原因。

请求示例

```
{
    "orderID": "A30B3F256-9D2D-43C5-ABCB-017AA9D3CB6D ",
    "reason": "域名填写错误"
}
```

响应参数

参数标识	参数名称	说明
isSuccess	结果标识	取值范围： true：请求成功。 false：请求失败。
errorMsg	请求失败描述	接口请求失败的描述。
successMsg	请求成功描述	接口请求成功的描述。
cancelResult	取消结果	取值范围： ● true：表示取消订单成功

版权所有 © 沃通电子认证服务有限公司

参数标识	参数名称	说明
		● false：表示取消订单失败
cancelFailedReason	失败原因描述	仅当参数“cancelResult”为“false”时，该参数取值不为空。

响应示例

```
{
    "isSuccess": true,
    "errorMsg": "",
    "successMsg": "",
    "data": {
        "cancelResult": false,
        "cancelFailedReason": "证书已签发"
    }
}
```


版权所有 © 沃通电子认证服务有限公司

6. 吊销证书

功能描述

该接口用于吊销用户证书，吊销证书需提供单位吊销证明材料，沃通会提供专门的吊销证明材料模板。

请求方式

POST 请求

环境地址

https://restapi.wosign.com/v1/Certificate/RevokeRequest

请求参数

参数标识	参数名称	说明
orderID	订单 ID	必选参数。 证书对应的订单号。
reason	吊销原因	必选参数。 吊销证书的原因。
fileType	材料格式	必选参数。 吊销证明文件的格式类型。
fileContent	材料二进制 base64	必选参数。 吊销证明文件的二进制的 base64。

请求示例

```
{
    "orderID": "644A3E60-F1AA-4E25-821A-ACFBC462BC37",
    "reason": "私钥泄露",
    "fileType": ".jpg",
    "fileContent": "AZIDFSLDFDDFKKDF"
}
```

响应参数

参数标识	参数名称	说明

版权所有 © 沃通电子认证服务有限公司

参数标识	参数名称	说明
isSuccess	结果标识	取值范围： true：请求成功。 false：请求失败。
errorMsg	请求失败描述	接口请求失败的描述。
successMsg	请求成功描述	接口请求成功的描述。
revokeStatus	吊销状态	吊销状态
revoked	吊销标识	吊销标识
page	统计参数	统计参数

响应示例

```
{
    "isSuccess": true,
    "errorMsg": "",
    "successMsg": "申请吊销成功",
    "data": {
        "revokeStatus": "pendingAudit",
        "revoked": false
    },
    "page": {
        "total": 0,
        "limit": 0,
        "skip": 0
    }
}
```


版权所有 © 沃通电子认证服务有限公司

7. 重新颁发

功能描述

该接口用于重新为用户颁发证书，新证书在签发后将吊销原有证书。重新颁发证书需要根据沃通的模板要求，提供单位吊销证书证明材料。

注意：如果不是 SM2 和 Sectigo 产品,在重新颁发后，我们系统不会主动发起吊销，需要用户按自己需求申请吊销，如下场景：如果用户重新颁发多张后又不想用了，应该把每一张都进行吊销操作。

请求方式

POST 请求

环境地址

https://restapi.wosign.com/v1/Certificate/ReissueRequest

请求参数

参数标识	参数名称	说明
orderID	订单 ID	必选参数。
csr	证书 CSR	必选参数。 SM2 签名证书的 CSR 或普通 SSL 的 CSR。
csR_Encrypt	SM2 加密证书的 CSR	如果重新颁发的是 SM2 证书，则该参数取值不为空。
reason	重新颁发的原因	必选参数。
idempotenceID	幂等值	可选参数 幂等值保证两边系统订单数量一致，一般传调用者数据库的 ID。 同时方便两边系统对账
fileType	材料格式	如果不是 SM2 和 Sectigo 产品 可不传，其它则必须传吊销证明文件的格式类型。
fileContent	材料二进制 base64	如果不是 SM2 和 Sectigo 产品 可不传，其它则必须传吊销证明文件的二进制的 base64。

版权所有 © 沃通电子认证服务有限公司

请求示例

```
{
    "orderID": "644A3E60-F1AA-4E25-821A-ACFBC462BC37",
    "csr": "--- begin ---xxx xxx ---end---",
    "csR_Encrypt": "--- begin ---xxx xxx ---end---",
    "reason": "私钥泄露",
    "fileType": ".jpg",
    "fileContent": "AZIDFSLDFDDFKKDF"
}
```

响应参数

参数标识	参数名称	说明
isSuccess	结果标识	取值范围： true：请求成功。 false：请求失败。
errorMsg	请求失败描述	接口请求失败的描述。
successMsg	请求成功描述	接口请求成功的描述。
newOrderID	新的订单 ID	重新生成新的订单 ID。
page	统计参数	统计参数

响应示例

```
{
    "isSuccess": true,
    "errorMsg": "",
    "successMsg": "申请重新颁发成功",
    "data": {
        "newOrderID": "644A3E60-F1AA-4E25-821A-ACFBC462BC37"
    },
    "page": {
        "total": 0,
        "limit": 0,
        "skip": 0
```


版权所有 © 沃通电子认证服务有限公司

```
    }
}
```


版权所有 © 沃通电子认证服务有限公司

8. 推送状态

推送状态接口包括推送单位状态和推送订单状态两种类型，用于推送消息通知接口对接方进行后续的业务操作。每条推送记录最多推送 3 次，如果推送获取的响应码为 200 OK，则不继续推送。

8.1 推送订单状态

功能描述

用于推送订单状态，提醒对接方下载证书。

参数说明

参数标识	参数名称	说明
dataAction	状态类型标识	订单状态消息标识为“order”。
orderID	订单 ID	“错误!未找到引用源。 错误!未找到引用源。”或“2 创建订单”接口返回订单 ID 的取值。
isIssued	是否已签发	取值范围： ● true：已签发 ● false：未签发
isRevoked	是否已吊销	取值范围： ● true：已吊销 ● false：未吊销

示例

```
{
    "dataAction": "order",
    "orderID": "30B3F256-9D2D-43C5-ABCB-017AA9D3CB6D",
    "isIssued": true,
    "isRevoked": false
}
```


版权所有 © 沃通电子认证服务有限公司

9. 通知接口

功能描述

该接口用于邮件通知用户订单已签发操作。

请求方式

POST 请求

环境地址

https://restapi.wosign.com/v1/Notification/email

请求参数

参数标识	参数名称	说明
orderID	订单 ID	需要取消订单的 ID。
collectUrl	下载证书网址	

请求示例

```
{
    "orderID": "A30B3F256-9D2D-43C5-ABCB-017AA9D3CB6D ",
    "collectUrl": "https://console.aliyun.com/ssl/order/exiud34"
}
```

响应参数

参数标识	参数名称	说明
isSuccess	结果标识	取值范围： true：请求成功。 false：请求失败。
errorMsg	请求失败描述	接口请求失败的描述。
successMsg	请求成功描述	接口请求成功的描述。
sentResult	取消结果	取值范围： ● true：表示发送通知结果成功

版权所有 © 沃通电子认证服务有限公司

参数标识	参数名称	说明
		● false：表示发送通知结果失败

响应示例

```
{
    "isSuccess": true,
    "errorMsg": "",
    "successMsg": "",
    "data": {
        "sentResult": false
    }
}
```


版权所有 © 沃通电子认证服务有限公司