

文档版本	1.0
保密级别	

## 发卡属地查询 V1.0 接口定义

---

2024/3/20

## 目录

发卡属地查询 V1.0 接口定义 .....	1
1. 文档说明 .....	3
1.1 功能描述 .....	3
1.2 阅读对象 .....	3
1.3 业务术语 .....	3
1.4 技术服务 .....	4
1.5 商户号 .....	4
1.6 开发密钥(key) .....	4
2. 接口定义 .....	4
2.1 调用方式 .....	4
2.2 报文格式 .....	4
2.2.1 报文头 .....	4
2.2.2 报文内容 .....	5
2.3 发起查询 .....	5
2.3.1 请求参数 .....	5
2.3.2 返回参数 .....	6
2.4 报文示例 .....	7
2.4.1 请求报文示例 .....	7
2.4.2 返回报文示例 .....	7
2.5 body 加密验证规则说明示例 .....	7
2.6 签名串示例 .....	9

3. 安全签名机制 .....	10
3.1 MD5 安全签名机制说明 .....	10
3.2 需要参与签名的参数 .....	10
4. 返回代码 status .....	10
5. 域名地址 .....	11
6. Demo .....	11

## 使用授权声明

本文档中所包含的信息属于商业机密信息，应严格控制使用范围。如无浙江大数据交易中心有限公司的书面许可，任何人员不得以任何介质方式持有或使用本文档的部分或全部内容。

文档修订记录

序号	日期	版本号	修订说明	修订人	审核人
1	2024-03-20	1.0	新建		

# 1. 文档说明

## 1.1 功能描述

查询并返回发卡属地数据。

## 1.2 阅读对象

开发人员以及相关项目管理人员。

## 1.3 业务术语

术语	解释
请求	商户服务端或商户客户端以字符串形式把需要传输的数据发送给交易中心开放平台系统的接口服务接收方的过程
返回	交易中心开放平台系统以字符串形式直接把处理结果数据返回给商户请求系统

## 1.4 技术服务

在开发或使用 API 接口时，产生疑问或出现问题，可通过 qq、Email、手机联系相关技术人员，交易中心技术支持人员会及时处理。

## 1.5 商户号

由浙江大数据交易中心运营人员，在通过协议审核之后，在交易中心开放平台系统创建商户，并通过邮件方式通知到商户相应联系人员。

## 1.6 开发密钥(key)

同商户号一致，由浙江大数据交易中心运营人员，在通过协议审核之后，在交易中心开放平台系统创建商户，并通过邮件方式通知到商户相应联系人员。

# 2. 接口定义

## 2.1 调用方式

接口通过 HTTPS 协议，使用 POST 方式进行接口的调用。

## 2.2 报文格式

### 2.2.1 报文头

Content-Type: text/plain;charset=UTF-8;

## 2.2.2 报文内容

加密后数据流的格式上传

## 2.3 发起查询

### 2.3.1 请求参数

Y:必传 N:可传可不传;

请求地址请与相关对接人员沟通明确。

字段说明	字段名	是否必传	类型	描述
请求地址: <a href="https://{域名}/dm-api/api/v2/verify/colony">https://{域名}/dm-api/api/v2/verify/colony</a>				
请求方式:	<b>POST</b>			
请求格式:	<b>text/plain</b>			
header:请求头				
sign:签名				
签名	<a href="#">sign</a>	Y	String	加密签名串; 详见签名安全机制
merchantCode:商户号				
商户号	<a href="#">merchantId</a>	Y	String	商户号, 由交易中心提供
requestTime:请求时间戳				
请求时间	<a href="#">requestTime</a>	Y	Long	请求时间戳 (精确到毫秒)
requestTime:接口开始时间				
接口开始时间	<a href="#">startTime</a>	Y	Long	接口开始时间 (精确到毫秒)
body:请求体, 内容转 json 字符串采用 AES 加密规则加密				
用户号	<a href="#">userNo</a>	N	String	用户编号。总/分公司对接平台非终端类用户使用银杏盾验证服务时必须通过该字段随报文同步上传真实使用方唯一标识符 (该符号由各接入平台自由分配)
银行卡号	<a href="#">cardNo</a>	Y	String	银行卡号

## 2.3.2 返回参数

Y:必传 N:可传可不传

字段说明	字段名	是否必传	类型	描述
报文格式:	<b>JSON</b>			
响应编码	status	Y	Integer	返回编码, 具体详见章节 4.
收费状态码	chargeCode	Y	String	0:查询成功-计费 其他为失败
响应描述	errorMsg	N	String	描述
响应状态码	code	Y	String	0:查询成功-计费 其他为失败
接口请求编号	transNo	Y	String	唯一编号
响应内容	data	N	JsonObject	响应报文数据

响应内容(data)

字段说明	字段名	是否必传	类型	描述
银行卡号	cardNo	Y	String	
卡 bin	cardBin	Y	String	
发卡机构名称	issurName	Y	String	
是否银联品牌卡	cupLogoFlag	Y	String	0: 非银联品牌卡 1: 银联品牌卡(9 字头卡或银联标准卡)
卡种	dcFlag	Y	String	1: 借记卡 2: 贷记卡 3: 准贷记卡 4: 预付卡
	cityInfo	Y	数组	

响应数据(cityInfo)

字段说明	字段名	是否必传	类型	描述
省	province	Y	String	
市	city	Y	String	
地区代码	areaCode	Y	String	
占比	perc	Y	String	银行卡号段地域消费占比

## 2.4 报文示例

### 2.4.1 请求报文示例

#### Request Headers

```
sign: 6764a6055f4ea240d8831f75f1509c32
merchantCode: M100000001
requestTime:1620386822
startTime:1620386822
```

#### Request Payload

```
{"userNo":"xxx","cardNo":"xxx"}
```

Key: 97D41DF5EE586F1F (生成规则参考2.6)

#### AES加密后

```
6wFefe92uJ+F0NO1106ioMFvqvkLevsOkFH4ZPYC7K8mOfYcEX7y+/ANIZwdtgL2jwtCe0b8ZIM
GP0+dEt135R6ml+BwyRVUN3QVS9Dr9B29VD8FCJ2F2ISr5FAeEFclJDgiHAr8lqsOzCUhew+armV
Ld7+p1NPZH654jwb1YyZlpgk/SRhC91XYtgODY1
```

### 2.4.2 返回报文示例

正常

```
{
```

```
"chargeCode": "0",
"code": "20000000",
"data": {
  "dcFlag": "1",
  "cardBin": "622848",
  "cupLogoFlag": "1",
  "issuerName": "农业银行",
  "userNo": "1111",
  "cityInfo": [{
    "areaCode": "370400",
    "perc": "",
    "province": "山东省",
    "city": "枣庄市"
  }, {}, {}],
  "cardNo": "6228481316061302369"
},
"errorMsg": "成功",
"status": 0,
"transNo": "44d9790702133e115fefbbbed469fa2ec"
}
```

#### 平台请求异常

```
{
  "status":1002,
  "des":"签名错误"
}
```

## 2.5 body 加密验证规则说明示例

1.加密规则采用 AES/ECB/PKCS5Padding 来加密, 秘钥使用商户的秘钥进行 16 位的 MD5 转大写获取, 通过 AES 加密转 base64 位串传输, 详情可参考 demo, 下图说明

秘钥获取如图:



# MD5在线加密

要加密的字符串: 1234

加密

字符串	1234
	<div style="background-color: red; width: 100px; height: 15px;"></div>
16位 大写	52D04DC20036DBD8

参考的加密、解密如图所示:

AES加密模式: ECB 填充: pkcs5padding 数据块: 128位 密码: 52D04DC20036 偏移量: iv偏移量, ecb模 输出: base64 字符集: utf8编码 (unicode编码)

待加密、解密的文本: hello

↑ 将你电脑文件直接拖入试试^-^

AES加密 AES解密

AES加密、解密转换结果(base64了): ZwlT/tVtMHYS76HrYz9AkG==

AES加密模式: ECB 填充: pkcs5padding 密钥长度: 128位 密钥: 97D41DF5EE536F1F 输出: base64

("idCard": "371d8701f81009dfdf0d0909ce682d5a", "mobile": "0b0f88cd7d99a03ce5149f58cb9d4121", "name": "e7aa5b47c74c8eeaca6b409d8ac40076")

AES加密 AES解密 复制结果 清空所有

6wFefea92uJ+F0N01106ioMFvqvKLevs0kFH4ZPYC7K8m0fYcEX7y+/ANIZwdtGL2jwCtCe0b8ZIMGP0+dEt135R6m1+BwyRVUN3QVS9Dr9B29VD8FCJ2F2ISr5FAeEfc1JDgiHAr8lqs0zCUhew+armVLd7+p1NP2H654jwb1VyZ1pkpg/SRhc91XYtg0DY1

## 2.6 签名串示例

签名串 MD5(MD5(时间戳+商户秘钥))

参考如下:

时间戳: 1621478294646

商户秘钥: D8BF74ADB86F4CDD81D0484F9D514AEE

第一次MD5: 1ea73ca458dbb473cfe056f0fceeacc0

第二次MD5: 5368e24930689a0ca5211739647a550e

→ Sign: 5368e24930689a0ca5211739647a550e

## 3. 安全签名机制

### 3.1 MD5 安全签名机制说明

MD5 安全签名机制是商户和交易中心约定一个签名 key，由交易中心生成，再调用交易中心提供的 api 接口的时候直接把参数和此 key 带入进行加密即可。

### 3.2 需要参与签名的参数

请求头参数 requestTime

商户秘钥 key

## 4. 返回代码

### 4.1 status

status	des	解决方案
0	请求成功	-
-1	服务器繁忙,请重试	未知错误, 具体咨询技术人员
-101	请求参数错误	按照 des 进行处理
1001	商户不存在	确认商户号是否正确
1002	签名错误	参照 3
1003	商户可用余额不足	确认账户余额是否足够
1004	商户未开通产品	确认产品是否正常开通
1005	商户产品未启用	联系商务人员
2001	订单号重复	调整订单号, 重新发起交易
2002	订单号不存在	确认订单号, 重新发起查询
3001	交易异常, 具体咨询技术人员	咨询技术人员

## 5. 域名地址

环境	地址
正式	<a href="https://dmapi.zjdex.com">https://dmapi.zjdex.com</a>

## 6. Demo

