

拉卡拉在线支付 认证接口

文档编号：

文档类别：系统对外接口

密 级：机密

版本信息：V1.0

建立日期：

创 建 人：蒋志飞

审 核 者：

批 准 人：

批准日期：

更新记录

日期	作者	版本	变更内容
2016-12-20	蒋志飞	V1.0	创建

目录

更新记录.....	2
1. 引言.....	4
1.1 概述.....	4
1.2 适用范围.....	4
1.3 专用术语.....	4
1.4 成为开发者.....	4
2. 通信约定.....	4
2.1 环境说明.....	4
2.2 报文编码.....	5
2.2 HTTP 请求头	5
2.3 通信安全.....	5
2.3.1 请求方加密过程.....	5
2.3.2 响应方解密过程.....	6
2.4 数据类型说明.....	6
2.4.1 类型定义.....	6
2.4.2 长度定义.....	7
2.4.3 接口参数统一约定.....	7
2.4.4 接口报文参数约定.....	7
2.5 报文范例.....	8
2.5.1 交易报文.....	8
2.5.2 拉卡拉回调报文.....	9
3. 业务流程说明.....	10
3.1 认证	10
4. 接口说明.....	10
4.1 认证接口.....	10
4.1.1 请求参数.....	10
4.1.2 响应.....	11

1. 引言

1.1 概述

该文档定义了拉卡拉支付平台与商户系统之间的认证交易接口，主要是对消费处理流程、通信约定、通信接口的定义。商户通过这一规范可以实现与支付平台联通，实现用户通过支付平台支付。

1.2 适用范围

此文档适用于接入拉卡拉支付平台认证交易的商户

1.3 专用术语

商户：指在平台上直接或间接为用户提供商品或服务的支付平台协议方，也是本接口中的收款方之一。

用户：指在提交方网站平台进行购买商品和服务的企业代理或个人代理，也是本接口中的付款方。

1.4 成为开发者

商户欲接入拉卡拉跨境支付平台成为开发者需按如下步骤：

1. 提交材料至拉卡拉跨境支付平台运营人员进行注册
2. 一旦注册成功，拉卡拉跨境支付平台运营人员将下发商户编号、接口密钥（商户私钥、平台公钥）。

我方提供测试环境供开发者测试联调，当开发者需测试联调时需联系我方运营人员注册测试商户号以及相应密钥。

文档以及开发包见：<https://github.com/LklCBPay/>

2. 通信约定

2.1 环境说明

环境	HOST	SCHEME
测试	<i>testintl.lakala.com</i>	<i>http</i>

生产	<i>intl.lakala.com</i>	<i>https</i>
----	------------------------	--------------

2.2 报文编码

在 post 传输过程中用 UTF-8 编码；

2.2 HTTP 请求头

```
Content-Type:application/json;charset=utf-8;
Accept: :application/json;charset=utf-8;
```

2.3 通信安全

安全原理：采用非对称密钥结合对称密钥的方式，非对称密钥用来身份验证（签名/签），以及交换对称密钥（一次一密）；对称密钥用于加密业务参数；使用时间戳防重复。

2.3.1 请求方加密过程



2.3.2 响应方解密过程



关于MAC（数字签名）：

交易报文

1. 请求方 mac 拼接方式为：**商户号+版本号（3.0.0）+时间戳+encData;**
2. 响应方 mac 原文拼接为：**retCode+retMsg+merId+ver+ts+encData;**

通知报文

1. 请求方 mac 拼接方式为：**时间戳+reqType+encData**
2. 响应方 mac 拼接方式为：**retCode+retMsg+时间戳+reqType**

2.4 数据类型说明

2.4.1 类型定义

标识符	定义
A	字母
N	数字
AN	字母和/或数字
ANS	字母、数字和/或特殊符号
AS	字母和/或特殊符号
U	中文字符
O	无序集合键值对

2.4.2 长度定义

标识符	定义
A10	字母，定长，长度为定长 10 个字符
A. .10	字母，变长，长度为最长 10 个字符
AN. .32	字母和/或数字，变长，最长不超过 32 个字符
U. .99	中文字符，变长，最长不超过 99 个中文字符

时区示例：GMT+8 表示东 8 区

2.4.3 接口参数统一约定

注：所有接口参数列表中具有*标志的为必填项。

所有参数名采用驼峰命名法。

2.4.4 接口报文参数约定

本节对第 4 章节中的业务接口的参数作如下约定：

1. 响应报文

1.1 接口响应报文结构 公用响应字段+业务参数。业务数据加密后设置为 key=“encData” 的 value，业务参数见各业务接口说明。

1.2 公用响应字段

公用响应字段			
字段名	属性	名称	说明
retCode*	N4	响应码	无论接口处理是否成功，都需返回此参数
retMsg*	U. .99	响应释义	无论接口处理是否成功，都需返回此参数

2. 请求报文

2.1 报文结构：公用请求字段+业务参数。业务数据加密后设置为 key=“encData” 对应的 value，业务参数见业务接口说明。

2.2 公用请求字段

公用响应字段			
字段名	属性	名称	说明
merId	AN12	商户号	注册成为拉卡拉跨境支付商户后，拉卡拉跨境支付下发的商户号
ver	N3	协议版本号	3.0.0
ts	N20	时间戳	yyyyMMddHHmmss+6 位不重复随机数或序列，不能重复

2.5 报文范例

2.5.1 交易报文

- 商户请求报文

```
{  
  
  "encData": "70C38CB4A37EB899FBD8B98FD40EBF26E3F882F06652183EB21E30619DA0896BC077956703  
5BC7F3D62EC28A020383F5671CD6CE6DCB63FC2107881A3103C6B83F520FC8BAC3A5F23825FF38FE563  
6E68C6EB70F41D27DB0D3EB2989AC4002FC75735ABD24602A62B599E21B35769457D481B9579F6AB53  
398A1A4F9AE3FD53B356ED9AC595B4EE774FD113BA73D",  
  
  "encKey": "A0F678AF8435E6341D59B8D177A58609CA307BBC14E07373BBB597022CB3DB0D86E45380E  
D3CC7DBB504F86C4F2BF382AA0AE02A45DECC357BDCBB27C96384A7DEF0697616DCC9CAC85D5A41D  
58E9D9EAFEE183F3C923514D94001A8750FC4B0B2D0857C1C1F8E9CC74E8C3B99F420A137F9E243AF11  
CFBA48BABE2DB5AD4",  
  
  "mac": "90B66B56A19E88FF415F8AD801E45B2973E6287391202E390937DB8574B80BB5F20794643D7  
B562A5BA934B84E01D0581040F212885877D6884F4804A2E7D2EEEC0F892B3FFAD204D54973A9F7A97  
59B",  
  "merId": "DOPCHN000258",  
  "ts": "20161031160900000026",  
  "ver": "3.0.0"  
}
```

- 拉卡拉响应报文

```
{  
  "merId": "DOPCHN000258",  
  "ver": "3.0.0",  
  "ts": "20161031162800000046",  
  "encData": "9DACB6F666F63BD76977BC528AB70A15915E691BED1A13E479C383D0F81AC93414190B8249CB613  
7344A08270E4669C16675965526BA6E71FC50016DF1505680AB291E2A98F6C73210FA7B49C802C6B24E1DC78D  
F3CE5749C8C9094B12497E",  
  "mac": "8FBB78D1C43AE7AE9E3977410019EED9F9DF9544CB10142D884EC64D7385002DA407D24EB564261B69  
509CE45EC486111EAA5DEEFE7AF019C03BE30D7983D81A5BB8AC1ACC02AD896890E5A7C94B9F389320E865356  
9422C65CFC04B44C4D021BA75E72795F319E67A41DB410E151EB1D215D1AB79D66AB9B0C4F25EE393CD",  
  "retCode": "0000",  
  "retMsg": "成功"  
}
```


2.5.2 拉卡拉回调报文

● 拉卡拉通知报文

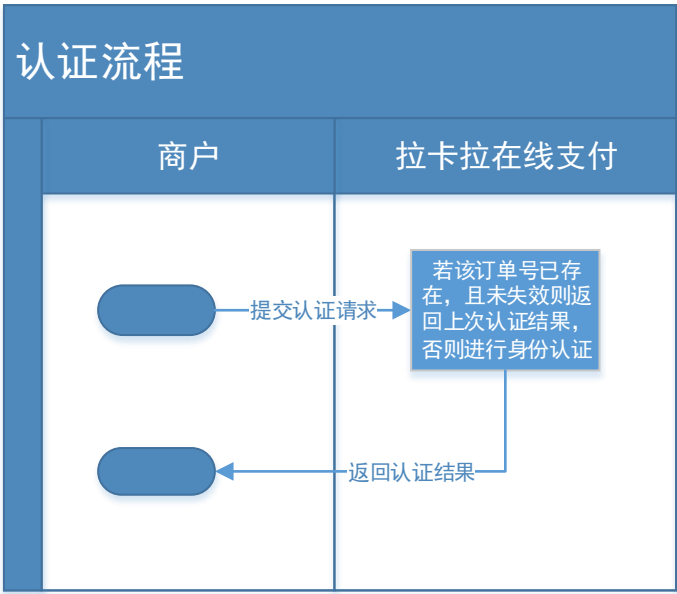
```
{
  "encData": "0F66CFCB535D44E25A24D1DC2231874BA38E7BF17D8407842D0A64CC58C0",
  "ts": "20161031164400000052",
  "encKey": "0E4E992A692678194B6CBA7044C5812D5971E7D8E4BA08F18A85B556BDF63368EB809B5CD90DEC9D
E11E70176FBEFFC064009E92F99F77A9F7F34371825A31DAD486B88E50E423ABE4A8CAF24B2B65262043E91018
E25C31E28EFD09FCD7D9D66E48ECCB1F9F5CD79877E4CD2A7945381E3882AE214DE1C7EBDD451D5DA",
  "reqType": "B0005",
  "merId": "DOPCHN000455",
  "mac": "6C0A21E79A0F7019A7B73E22A18FB2941A472B007ED96F9819383DB31640B7253980EFFEE9388232402
DA61BD6C1647886EB5DB15B244B26BFD407C04BE8F5B183EB41EDE31F63AED79BA7694AE4A5F402920AE43D8
8774684CFBB514483BDE49268377C6F655DAA4561F971375D2BD4181DC594C3ADC4F46D71A6E0DE",
  "ver": "3.0.0"
}
```

● 商户响应报文

```
{
  "retCode": "0000",           //响应码，见附录
  "retMsg": "成功",           //响应消息
  "ts": "201641417949161767", //时间戳，yyyyMMddHHmmss+6 位不重复随机数或序列
  "merId": "DOPCHN000339",     //商户号
  "mac": "6E87502D96871C50BB644B389A98744403BCCBB779E85AB65E7550C5C421074170EEF076BCFD0E99862
3AB91479308BDF5E9D96E75124236D748C49ABE2259684C95B227633043A514A9A61BFC216F", //MAC
  "ver": "3.0.0",             //协议版本号
  "encData": "0F66CFCB535D44E25A24D1DC2231874BA38E7BF17D8407842D0A64CC58C0"
}
```

3.业务流程说明

3.1 认证



4. 接口说明

4.1 认证接口

URL: {domain}:{port}/gate/auth

METHOD: POST

请求方：商户

响应方：拉卡拉支付平台

协议版本：V3.0.0

【功能描述】：

商户申请批量交易令牌，并凭此上传批量文件

4.1.1 请求参数

业务参数			
字段名	属性	名称	说明

orderNo*	AN50	商户订单号	商户需保持其不可重复性
bizType*	N2	认证类型	00：身份认证 01：银行卡三要素认证 02：银行卡四要素认证
name*	A10	姓名	
certNo*	AN20	证件号	
certType*	N2	证件类型	00：身份证
bankCardNo	N20	银行卡号	当bizType为01和02时必填
bankMobile	N15	银行预留手机号	当bizType为02时必填

4.1.2 响应

业务参数			
字段名	属性	名称	说明
orderNo	AN50	商户订单号	商户需保持其不可重复性
bizType	N2	认证类型	00：身份认证 01：银行卡三要素认证 02：银行卡四要素认证
name	A10	姓名	
certNo	AN20	证件号	
certType	N2	证件类型	00：身份证
bankCardNo	N20	银行卡号	当bizType为01和02时必填
bankMobile	N15	银行预留手机号	当bizType为02时必填
retCode*	N4	0000-认证成功 9001-认证失败-信息不符 9002-认证失败-内部系统异常 9003-认证失败-请求信息与已存在订单信息不符 9004-认证订单重复 9005-认证订单失效 9006-商户未配置该认证类型 9007-多次查询不一致，稍后再试 9999-系统异常	
retMsg*	U..99		