

裕福第三方支付平台 代扣接口文档

裕福支付平台项目组

文档版本：V1.0.0

2017 年 08 月 21 日

修订历史

当前版本	修订内容	作者	修订日期
1.0.0	初稿	鄧顺友	2017 年 08 月 21 日
1.0.0	1. 修改交易状态字段返回值 2. 修改响应码表 3. 新增代扣通知	鄧顺友	2018 年 03 月 09 日
1.0.0	新增接口业务响应码	鄧顺友	2018 年 04 月 02 日
1.0.0	移除代扣类型(type)字段	鄧顺友	2018 年 05 月 07 日
1.0.0	增加返回码 0090015,调整异步通知	张朝辉	2018 年 08 月 13 日

权利声明

本文档中的所有内容为裕福支付有限公司的机密和专属所有。未经裕福支付有限公司的明确书面许可，任何组织或个人不得以任何目的、任何形式及任何手段复制或传播本文档部分或全部内容。

目录

修订历史.....	2
权利声明.....	2
目录.....	3
一. 前言.....	5
1.1 目标.....	5
1.2 阅读对象.....	5
1.3 术语定义.....	5
二. 接入流程.....	5
2.1 接入准备.....	5
2.2 交易流程.....	6
2.2.1 代扣申请.....	6
2.2.2 代扣查询.....	6
2.3 上线流程.....	6
三. 通信安全.....	6
3.1 通信方案.....	6
3.2 报文形式.....	7
3.3 密文签名算法.....	7
3.3.1 加密加签公式.....	7
3.3.2 加密加签报文.....	8
3.3.3 解密验签公式.....	8
3.3.4 解密验签报文.....	9
3.4 明文签名算法.....	9
3.4.1 加签公式.....	9
3.4.2 加签报文.....	10
3.4.3 验签公式.....	10
3.4.4 验签报文.....	10
四. 接口说明.....	11
4.1 代扣申请.....	11
4.1.1 代扣请求报文.....	11
4.1.2 代扣应答报文.....	12
4.2 代扣查询.....	13
4.2.1 查询请求报文.....	13
4.2.2 查询应答报文.....	13
4.3 代扣通知.....	14
4.3.1 代付通知报文.....	14
五. 联调资源.....	14
5.1 接口地址.....	14
5.2 测试证书.....	15
5.3 软件开发包.....	15
六. 联系我们.....	15

6.1 公司相关信息.....15

6.2 客服联系方式.....15

七. 附录..... 15

7.1 响应码表.....15

7.2 省市码表.....17

7.3 银行码表.....17

7.4 异步通知.....17

7.5 规范说明.....17

一. 前言

1.1 目标

本文档对裕福支付第三方支付平台人民币批量代扣接口网关的使用进行详细说明,帮助外平台/合作方平台熟悉裕福支付人民币批量代扣接口网关的支付交易流程,达到方便外平台/合作方平台系统集成,快速接入代扣能力的目的。

1.2 阅读对象

本文档的阅读对象是裕福支付第三方支付平台接入方的应用开发人员、维护人员和管理人员。

1.3 术语定义

缩写/术语	解释
商户/商城	拥有自己的交易系统、具有外平台接入能力的、为社会公众提供电子商务功能的企业平台
商户/商城网站	商户/商城的电子商务平台
卖家	电子商务平台交易中出售商品、收取货款的一方
买家	电子商务平台交易中购买商品、支付货款的一方
付款方	商户在支付平台开通代扣接口功能并使用的一方
收款方	商户在支付平台使用代扣接口功能付款交易的收款一方
请求	通过约定的通信方式将报文发送给接收方的过程
通知	裕福支付平台的交易处理完成后将响应报文以前台或者后台的方式发送给商户网站的过程

二. 接入流程

2.1 接入准备

- 商户在裕福支付平台网站注册企业客户,并收取系统邮件进行激活。
- 商户以登录裕福支付平台,将营业执照等相关正面扫描件通过绑卡/实名认证功能上传系统,等待裕福运营审核。
- 审核通过后,商户可正常使用裕福支付平台客户相关功能。如需开通商户服务,则点击

系统的“我要开通商户服务”链接，并输入真实有效的商户申请信息，提交后等待裕福运营人员审核。

- 审核通过后，商户可登录裕福支付平台，在安全中心功能中设置通信安全所必须的内容（具体请参照本文档第三章<通信安全>）。
- 联系裕福支付平台技术支持（方式见本文档），进行接入联调。

2.2 交易流程

2.2.1 代扣申请

2.2.2 代扣查询

2.3 上线流程

- 商户接入裕福支付平台测试环境进行联调测试。
- 商户接入裕福支付平台正式环境进行联调测试。
- 正式上线运营。

三. 通信安全

3.1 通信方案

本文档接口的通信安全采用双向非对称的加解密、加解签组合的安全方案。按照本方案设计，裕福支付平台和商户平台需要拥有如下要素：

主体	要素	备注
裕福支付平台	安全的 RSA 私钥文件	可用的 RSA 公私钥对
	经合法第三方 CA 签发的 RSA 公钥证书	
商户平台	安全的 RSA 私钥文件	可用的 RSA 公私钥对
	经合法第三方 CA 签发的 RSA 公钥证书	

裕福支付平台接口安全算法支持密文签名算法和明文签名算法两种接入方式。密文签名

算法首先对报文进行加密，然后签名后通过公共网络传输，此算法能保证在非安全网络（如 HTTPS 接口、存在代理网关的网络）环境下保证通信安全。明文签名算法将直接对报文明文签名后通过公共网络传输，此算法仅能保证报文正确性，不能保护报文在网络传输过程中被第三方嗅探。

3.2 报文形式

发送方通信报文参数如下表：

参数名称	参数值	参数说明
商户代码	merchantId	商户唯一标识代码，必填
报文密文	data	被加密的业务报文
报文加密密码密文	enc	被加密的业务报文加密密码
报文加密密码密文签名	sign	加密密码密文的签名

接收方若验签/解密失败，返回参数如下：

参数名称	参数值	参数说明
商户代码	merchantId	商户唯一标识代码，必填
通信响应码	respCode	安全通信响应码（见附录）
通信响应描述	respDesc	安全通信响应描述（见附录）

3.3 密文签名算法

加密算法采用标准、公开的 AES 对称加密解密算法和 RSA 非对称加密解密算法组合。报文计算过程中，均使用 UTF-8 编码。AES 加密密码在每次报文通信过程中，由发送方随机生成（一次一密）。

3.3.1 加密加签公式

业务报文（P）首先应转换为标准的 JSON 字符串格式，转换公式如下：

$$JP = \text{JSON.Encrypt}(P);$$

发送方随机生成 16 位的 AES 加密密码 K，使用 AES 算法对业务报文 JP 进行 AES 算法加密，加密结果按照标准的 Base64 算法做格式转换，得到 Base64 格式的业务报文，即业务报文密文（BEJP）。转换公式如下：

$$\text{BEJP} = \text{Base64.Encrypt}(\text{AES.Encrypt}(JP, K)); \quad K = \text{Random}(16)。$$

随机生成的 AES 加密密码 K 需要加密传输给接收方，因此将使用 RSA 算法，对 K 进行非对称加密，得到加密后的 AES 加密密码密文 EK，然后按照 Base64 算法做格式转换，得到 Base64

格式的 AES 加密密码密文 BEK。转换公式如下：

$BEK = \text{Base64.Encrypt}(\text{RSA.Encrypt}(K, \text{pubKey}))$; pubKey 为接收方的公钥。

为保证发送方、接收方的双向认证，发送方需要对自己发送的报文进行签名，为优化签名效率，签名将仅对 AES 加密密码密文 BEK 进行签名，得到签名结果 S，然后使用 Base64 做格式转换，得到 Base64 格式的签名字符串 BS。转换公式如下：

$BS = \text{Base64.Encrypt}(\text{RSA.Signature}(EK, \text{priKey}))$; priKey 为发送方的私钥。

3.3.2 加密加签报文

参数名称	参数值	参数说明
商户代码	merchantId	商户唯一标识代码，必填
报文密文	data	BEJP
报文加密密码密文	enc	BEK
报文签名	sign	BS

3.3.3 解密验签公式

接收方在接收到报文后，首先需要验证签名，得到验签结果 Rt（成功）或者 Rf（失败）。公式如下：

$R(t,f) = \text{RSA.VerifySignature}(\text{Base64.Decrypt}(BS), \text{pubKey})$; pubKey 为发送方的公钥。

如果验签成功，则需要对 AES 加密密码密文（BEK）进行解密，得到 AES 加密密码（K）。公式如下：

$K = \text{RSA.Decrypt}(\text{Base64.Decrypt}(BEK), \text{priKey})$; priKey 为接收方的私钥。

得到 AES 加密密码 K 后，就可以对业务报文 BEJP 进行解密，并得到 JSON 格式的业务报文（JP）。公式如下：

$JP = \text{AES.Decrypt}(\text{Base64.Decrypt}(BEJP), K)$;

对 JSON 格式的业务报文（JP）做格式转换，得到最终的业务报文明文。公式如下：

$P = \text{JSON.Decrypt}(JP)$;

3.3.4 解密验签报文

参数名称	参数值	参数说明
商户代码	merchantId	商户唯一标识代码，必填
报文密文	data	BEJP
报文加密密码密文	enc	BEK
报文签名	sign	BS

3.4 明文签名算法

加密算法采用标准、公开的 MD5 算法和 RSA 非对称签名验签算法组合。报文计算过程中，均使用 UTF-8 编码。报文计算过程中使用报文构建时间作为计算签名的一部分。接收方在验证签名通过的同时，也需要计算报文构建时间与报文收到时间的的时间差，该时间差值的大小与该报文的安全性成反比。

注意：裕福支付平台将自动丢弃时间差超过 60 秒的报文。

3.4.1 加签公式

业务报文（P）首先应转换为标准的 JSON 字符串格式，转换公式如下：

$JP = \text{JSON.Encrypt}(P);$

转换结果 JP 按照标准的 Base64 算法做格式转换，得到 Base64 格式的业务报文，即业务报文（BEJP）。转换公式如下：

$BJP = \text{Base64.Encrypt}(JP)。$

对业务报文（P）的所有报文参数名按照 ASCII 升序排序，按照排序后的报文参数名顺序遍历，将所有报文参数的非空参数值拼接为字符串 PVS，对 PVS 计算 MD5 值 MS。转换公式如下：

$MS = \text{MD5.doMD5}(PVS); PVS = \text{Connect}(\text{NotEmpty}(\text{Sorted}(P.\text{key}, \text{ASCII.ascend}).\text{value}))。$

获取当前时间的毫秒形式，得到字符串 T，将 MS 和 T 使用英文符号“|”拼接得到新字符串“MS|T”。

为保证发送方、接收方的双向认证，发送方需要对自己发送的报文进行签名，为优化签名效率，签名将仅对上述得到的字符串“MS|T”进行签名，得到签名结果 S，然后使用 Base64 做格式转换，得到 Base64 格式的签名字符串 BS。转换公式如下：

$BS = \text{Base64.Encrypt}(\text{RSA.Signature}(\text{"MS|T"}, \text{priKey}));$ priKey 为发送方的私钥。

3.4.2 加签报文

参数名称	参数值	参数说明
商户代码	merchantId	商户唯一标识代码，必填
报文密文	data	BJP
报文加密密码密文	enc	T
报文签名	sign	BS

3.4.3 验签公式

接收方在接收到报文后，对业务报文 BJP 进行计算，并得到 JSON 格式的业务报文（JP）。公式如下：

$$JP = \text{Base64.Decrypt}(BJP);$$

对 JSON 格式的业务报文（JP）做格式转换，得到最终的业务报文明文。公式如下：

$$P = \text{JSON.Decrypt}(JP);$$

对业务报文（P）的所有报文参数名按照 ASCII 升序排序，按照排序后的报文参数名顺序遍历，将所有报文参数的非空参数值拼接为字符串 PVS，对 PVS 计算 MD5 值 MS。转换公式如下：

$$MS = \text{MD5.doMD5}(PVS); PVS = \text{Connect}(\text{NotEmpty}(\text{Sorted}(P.\text{key}, \text{ASCII.ascend}).\text{value})).$$

将 MS 和 T 使用英文符号“|”拼接得到新字符串“MS|T”后，开始签证签名，得到验签结果 Rt（成功）或者 Rf（失败）。公式如下：

$$R(t,f) = \text{RSA.VerifySignature}(\text{"MS|T"}, \text{pubKey}); \text{ pubKey 为发送方的公钥。}$$

如果验签成功，则获取当前时间 CT，同上送报文的时间 T 进行差值计算得到差值 PT：

$$PT = CT - T; PT \text{ 单位为毫秒。}$$

如果 PT 值大于 60000，则丢弃报文，验证报文失败，否则，验证成功。

商户可以根据自己安全定义，自行调整 PT 的差值，提高或降低报文验证的成功率。

3.4.4 验签报文

参数名称	参数值	参数说明
------	-----	------

商户代码	merchantId	商户唯一标识代码，必填
报文密文	data	BJP
报文加密密码密文	enc	T
报文签名	sign	BS

四. 接口说明

4.1 代扣申请

API 提交申请，发起对私银行账户扣款。

4.1.1 代扣请求报文

名称	KEY	数据类型	必填	说明
接口版本号	version	String	是	固定值：1.0.0
商户订单号	merchantOrderId	String	是	商户订单号
商户订单时间	merchantOrderTime	String	是	商户订单时间格式为 ：yyyyMMddHHmmss
商户代码	merchantId	String	是	商户代码必须为整数，且长度须在1-24之间
用户信息	userInfo	String	是	单笔代扣必填-见下方注释
备注	remark	String	是	备注信息，长度38个字符内
后台通知地址	backUrl	String	是	后台通知地址
商户保留域	msgExt	String	否	
自定义保留域	misc	String	否	

注释：userInfo 为单笔代扣用户的相关信息。

如：

名称	KEY	数据类型	说明
银行编号	bankNo	String	是

银行名称	bankName	String	是
银行卡号	cardNo	String	是
卡类型	cardType	String	P1-借记卡 P2-贷记卡 P5-福卡
姓名	certName	String	是
证件类型	certType	String	是 01 身份证
身份证号	certNo	String	是
银行预留手机号	mobile	String	是
金额	amt	String	是
信用卡有效期	expired	String	是
CVN2 码	cvn2	String	是
银行账号属性	pblFlag	String	是 01 对公 02 对私

4.2.2 代扣应答报文

名称	KEY	数据类型	说明
接口版本号	version	String	固定值：1.0.0
商户代码	merchantId	String	商户代码必须为整数,且长度须在 1-24 之间
商户订单号	merchantOrderId	String	商户订单号
交易时间	transTime	String	裕福平台记录的交易时间
交易状态	transStatus	String	01 受理失败 02 受理成功 03 支付中 04 交易失败 05 交易成功
业务流水号	bpSerialNum	String	裕福支付平台为本次交易生成的唯一订单流水标识

响应码	respCode	String	
响应描述	respDesc	String	

4.2 代扣查询

针对已发起代扣的交易，可以通过本接口查询该交易的代扣信息。

4.2.1 查询请求报文

名称	KEY	数据类型	必填	说明
接口版本号	version	String	是	固定值：1.0.0
商户代码	merchantId	String	是	商户代码必须为整数，且长度须在1-24之间
请求序列 TOKEN	token	String	是	置单请求序列标识
商户保留域	msgExt	String	否	
自定义保留域	misc	String	否	

4.2.2 查询应答报文

名称	KEY	数据类型	说明
接口版本号	version	String	固定值：1.0.0
商户代码	merchantId	String	商户代码必须为整数，且长度须在1-24之间
代扣金额	amt	String	代扣金额
交易时间	transTime	String	代扣交易时间
交易状态	transStatus	String	01 受理失败 02 受理成功 03 支付中 04 交易失败 05 交易成功

商户订单号	merchantOrderId	String	商户订单号
商户保留域	msgExt	String	同上送
业务流水号	bpSerialNum	String	裕福支付平台为本次交易生成的唯一订单流水标识
响应码	respCode	String	
响应描述	respDesc	String	

4.3 代扣通知

4.3.1 代付通知报文

名称	KEY	数据类型	说明
接口版本号	version	String	固定值：1.0.0
商户代码	merchantId	String	商户代码必须为整数,且长度须在 1-24 之间
商户订单号	merchantOrderId	String	同上送
商户订单时间	merchantOrderTime	String	同上送
交易时间	transTime	String	裕福平台记录的交易时间
交易状态	transStatus	String	04 交易失败 05 交易成功
业务流水号	bpSerialNum	String	裕福支付平台为本次交易生成的唯一订单流水标识
商户保留域	msgExt	String	同上送
响应码	respCode	String	
响应描述	respDesc	String	

五. 联调资源

5.1 接口地址

代扣申请	http://malltest.yfpayment.com/batchpay/withhold_apply.do
代扣查询	http://malltest.yfpayment.com/batchpay/withhold_query.do

5.2 测试证书

请联系商务代表索取。

5.3 软件开发包

请联系商务代表索取

六. 联系我们

6.1 公司相关信息

公司名称	裕福支付有限公司
公司网站	https://www.yfpayment.com
公司地址	北京市朝阳区光华里丙 17 号
公司邮编	

6.2 客服联系方式

客户邮箱	请联系商务代表索取
客户电话	请联系商务代表索取
客户 QQ	请联系商务代表索取
客户工作时间	工作日 9:00~12:00, 13:30~5:30

七. 附录

7.1 响应码表

安全通信响应码表	
响应码	释义
S0100	验签失败
S0200	AES 加密密文解密失败
S0300	业务报文解密失败

接口业务响应码表	
响应码	释义
0000	操作成功
902004	代扣申请失败
902005	系统常规异常
902006	代扣查询失败
902007	此订单不存在
902011	未接入此类型代扣
902012	已接入此类型代扣,需签约
1080401001	接口版本号字段必填
1080401002	商户订单号字段必填
1080401004	商户订单时间字段必填
1080401007	后台通知地址字段必填
1080401014	银行账号属性字段必填
1080401015	银行卡号字段必填
1080401016	金额字段必填
1080401017	银行名称字段必填
1080401021	金额格式不正确必须是正整数
1080401031	用户信息字段必填
1080401032	备注字段必填
1080401033	代扣类型字段必填
1080401034	附言字段限制 38 个字符内
1080401035	银行账户名称字段必填
1080401036	银行编号字段必填
1080401037	卡类型字段必填
1080401038	身份证号字段必填
1080401039	CVN2 码字段必填
1080401040	信用卡有效期字段必填"
1080401041	银行预留手机号字段必填
1080401042	证件类型字段必填
1080401043	预留手机号格式有误,支持 11 位数字
1080401044	银行卡格式有误,最多支持 64 位数字
1080401045	姓名格式错误,最少 2 个字符最多 64 个字符,不支持特殊符号
1080401046	身份证号码有误,支持 15 或 18 位字符
1080401047	信用卡有效期,格式:MMYY
1080401048	请求序列 TOKEN 字段必填
1080401054	商户订单号非法格式,正确格式:长度必须在 8-32 字符之间
0090015	商户支付授权地址异常

7.2 省市码表

7.3 银行码表

7.4 异步通知

裕福支付平台为尽最大努力保证批量代扣结果能及时知悉商户平台，设计了异步通知接口的状态补偿机制。本文档涉及代扣申请和代扣交易完成的异步通知。

当裕福支付平台向商户平台发起异步通知请求时，商户的回调接口应返回“**success**”字符串。否则，裕福支付平台将认为本次异步通知请求不成功，针对本笔交易的通知任务将被标记为需重复通知状态。裕福平台会依此对商户发起重复通知。通知次数和时点如下：

异步通知次数序列	通知时点
1	T
2	T + 30 秒
3	T + 5 分钟
4	T + 50 分钟
5	T + 2 小时
6	T + 24 小时

7.5 规范说明

- 商户在批量代扣申请中的回调接口（后台 URL）应能够处理针对同一笔商户订单多次重复通知的能力（重复通知的原因见 7.4 章节）。
- 支付平台对商户的异步通知接口负有尽力通知的义务，但从实践中得到的结论是由于公开网络等不可靠因素，支付平台无法完全保证通知的及时性。因此，商户平台应有自己独立的补偿体系。比如定期定时的轮询商户系统中的订单，并对这些订单向裕福支付平台发起代扣交易查询，同步订单的处理结果。
- 报文发送/接收过程中，由于报文多采用 Base64 做转码后通过网络传输，因平台不同，可能会将 Base64 编码中的加号“+”自动转换为空格“ ”，造成接收方解码失败，因此，发送方应将 Base64 格式的报文应首先通过 URLEncode 编码，然后上送。
- 应对文件的摘要值进行签名验证操作。如果校验不通过应立即放弃该文件并删除，避免安全风险。
- 同商户号下所有的代扣文件名应具有唯一性。
- 接口中的文件以标准的 ZIP 格式传输。一次代扣请求应上传一个代扣文件压缩包，压缩包中有且仅有一个代扣文件。文件摘要值应对压缩包进行计算，而非代扣文件本身。

- 为了确保交易场景的可靠性，商户可联系裕福运营人员进行商户 IP 的绑定配置，若交易入口为非此绑定 IP，则拒绝交易。